ISO/IEC 27001 • SECURE PURSUITS • OPERATING EVIDENCE

BID SECURITY BY DESIGN

A BRITISH FIELD MANUAL FOR BUILDING ISO/IEC 27001 INTO END-TO-END BID MANAGEMENT, BID WRITING AND APMP-ALIGNED PRACTICE

HAYDEN FAY

BID CHAMPIONS LTD

BID SECURITY BY DESIGN

ISO/IEC 27001 • SECURE PURSUITS • OPERATING EVIDENCE

BID SECURITY BY DESIGN

A British Field Manual for Building ISO/IEC 27001 into End-to-End Bid Management, Bid Writing and APMP-Aligned Practice

Hayden Fay

Published by Bid Champions Ltd
United Kingdom • 2026

COPYRIGHT AND PUBLICATION INFORMATION

First published in the United Kingdom in 2026 by Bid Champions Ltd.

Original UK edition.

Author: Hayden Fay

ISBN: 978-1-916752-12-2

Printed in the United Kingdom.

LEGAL, SECURITY AND PROFESSIONAL DISCLAIMER

This book is practical educational commentary about information security management, bid management, proposal development and organisational improvement. It is not a replacement for ISO/IEC 27001, ISO/IEC 27000, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27007, APMP's Body of Knowledge, an authorised standard, specialist cyber-security advice, legal advice, data-protection advice or certification advice.

The principal certifiable requirements used for this edition are ISO/IEC 27001:2022 together with ISO/IEC 27001:2022/Amd 1:2024 on climate action. The supporting standards and public guidance discussed include ISO/IEC 27000:2026, ISO/IEC 27002:2022, ISO/IEC 27005:2022 and ISO/IEC 27006-1:2024. Standards, regulatory guidance, technology and threats change. Readers should check the current position before relying on a clause reference, control decision, implementation plan or certification timetable.

The book paraphrases management-system requirements and security-control concepts. It does not reproduce the copyrighted text of ISO or IEC standards. Readers intending to implement or certify an information security management system should obtain authorised copies of the applicable standards and use appropriately competent advisers where needed.

APMP provides professional guidance and learning for bid, proposal, tender, capture and business-development practitioners. References to APMP-aligned practice in this book mean alignment with the broad pursuit stages and practices described in APMP's current Winning Business Ecosystem and related public resources. They do not mean that APMP has approved, certified or endorsed the system described here.

Every organisation is different. Its scope, interested parties, information assets, technologies, legal duties, contractual requirements, risk criteria, suppliers, threat environment and certification arrangements must be determined from its own facts. Examples in this book are fictional or composite. Names, businesses, procurements, incidents and dialogue have been created for learning purposes.

No process described here guarantees a tender award, a particular score, ISO/IEC 27001 certification, immunity from an incident, lawful processing in every circumstance or freedom from error. The author, contributor and publisher accept no responsibility for decisions taken without proper review of the applicable tender documents, contractual terms, laws, standards, technical evidence and professional advice.

The tender documents outrank this book. The authorised standard outranks this book. A certificate does not replace evidence. Security claims still have to be true.

STANDARDS STATUS AT PUBLICATION

This edition was completed on 21 August 2026. ISO/IEC 27001:2022 remained the current published requirements standard for information security management systems and had one published amendment, ISO/IEC 27001:2022/Amd 1:2024. The amendment adds an explicit climate-change consideration to the context and interested-party requirements.

ISO/IEC 27000:2026 had replaced the 2018 overview and vocabulary edition. ISO/IEC 27002:2022 remained the current guidance standard for information security controls, while ISO/IEC 27005:2022 provided current guidance on managing information security risk. ISO/IEC 27006-1:2024 contained requirements relevant to bodies auditing and certifying information security management systems.

The book therefore treats ISO/IEC 27001:2022 with Amendment 1:2024 as the certification baseline. It uses ISO/IEC 27002 concepts to explain controls, but does not imply that ISO/IEC 27002 is itself a certifiable requirements standard.

All requirements in clauses 4 to 10 apply to an organisation implementing ISO/IEC 27001. Annex A is different. It is a reference set used during risk treatment to help the organisation check that necessary controls have not been missed. The organisation may need controls that are not in Annex A. It may also determine that a particular Annex A control is unnecessary, provided the decision is justified through the required risk-treatment and Statement of Applicability process.

That distinction runs through the entire book. Annex A is not a shopping list to tick from top to bottom. The risk belongs to the organisation. So does the decision.

CONTENTS

THE FIELD MANUAL

CONTENTS - CONTINUED

THE FIELD MANUAL

CONTENTS - FIELD TOOLKITS

IMPLEMENTATION TOOLKIT

AUTHOR'S NOTE

Bid teams often meet ISO/IEC 27001 in the least useful way. A buyer asks for a certificate. Someone sends a PDF. The writer copies the scope into a security answer and the team moves on, while the tender documents are being shared through personal email, an external consultant still has access to last month's workspace and a draft containing staff CVs has been pasted into an online tool nobody has assessed.

The contradiction is not rare. That is the reason for this book.

Information security in bidding is easily mistaken for an IT task. IT matters, clearly. So do people, contracts, office doors, cloud suppliers, file names, access decisions, recruitment, remote work, disposal, incident response and the very ordinary moment when a director forwards a confidential pricing model to the wrong address because both contacts are called Martin.

ISO/IEC 27001 gives an organisation a way to manage those risks as a system. APMP practice gives the pursuit a professional lifecycle. Used together, they can make security part of how opportunities are qualified, captured, designed, written, reviewed, submitted, handed over and learned from. Used badly, they produce two parallel worlds: a security folder prepared for audit and a bid room operating by urgency.

The pages that follow treat information as something the pursuit uses, changes and creates. Customer documents arrive. People interpret them. Solutions reveal architecture. Pricing exposes commercial assumptions. CVs contain personal data. Partners bring their own systems. Artificial intelligence can accelerate work and multiply one unsupported statement across twelve answers before lunch.

Security is not the absence of movement. It is controlled movement.

Use the book with a live process beside you. Do not begin by writing thirty policies. Begin with the tender pack that arrived this morning. Ask who can see it, why they can see it, what they are allowed to do with it, which risks matter, what evidence remains and what happens when somebody makes the wrong decision at 17:42.

HOW TO USE THIS FIELD MANUAL

Read Chapters 1 to 7 first if the organisation has no defined information security management system around its pursuit process. They establish the ISMS logic, clause structure, APMP alignment, scope, leadership, risk and support controls.

Use Chapters 8 to 16 while building or rebuilding secure end-to-end bid operations. These chapters follow information from opportunity identification through capture, intake, risk assessment, design, writing, supplier use, review, submission, post-bid activity and handover.

Use Chapters 17 to 20 to understand every Annex A control in the current standard through the lens of bid and proposal work. The control labels are paraphrased. Use the authorised standards for exact wording and full guidance.

Use Chapters 21 and 22 when the system is running. Monitoring, internal audit, management review, corrective action, continual improvement and certification readiness turn a collection of security measures into an ISMS.

Do not implement every suggested record at once. Risk decides depth. A five-person consultancy handling ordinary commercial proposals does not need the same controls as a national supplier processing government-restricted information across a consortium. Both need to know their scope, information, access, risks, suppliers, incidents and decision authority.

Throughout the book, 'customer' may mean a contracting authority, private buyer, framework customer or internal business unit receiving the bid service. 'Bid' includes tenders, proposals, framework applications, call-off competitions and related competitive submissions. 'ISMS' means information security management system. 'Control' means a measure that changes risk; it may be organisational, contractual, human, physical or technological.

The APMP alignment used here follows four broad stages:

- pre-bid and capture;
- bid and proposal;
- post-bid and proposal;
- implementation and contract learning.

The ISMS runs across all four. It does not appear at final review to ask whether the password was strong enough.

THE INTEGRATED SECURE PURSUIT MAP

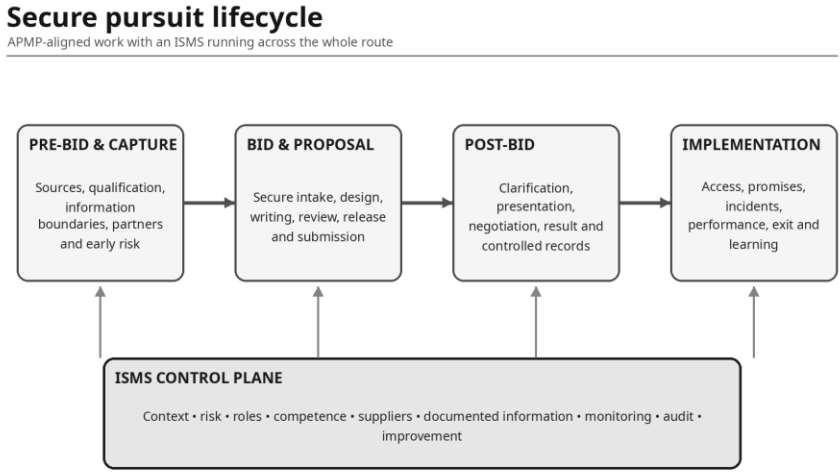

Figure 1 - The APMP-aligned secure pursuit lifecycle with ISMS control across every stage.

Pre-bid and capture - opportunity identification, lawful customer understanding, qualification, security requirements, information boundaries, partners, resources and early risk decisions.

Bid and proposal - controlled receipt, classification, access, requirements analysis, risk assessment, solution design, pricing, evidence, writing, review, release and secure submission.

Post-bid and proposal - clarifications, presentations, negotiation, incident handling, award or loss, retained records and controlled changes to the submitted position.

Implementation - mobilisation, transfer of security promises, access provisioning, supplier control, incident readiness, performance, customer feedback, improvement and future evidence.

Across the entire map, the ISMS asks awkward but useful questions. What information is involved? What would harm confidentiality, integrity or availability? Who owns the risk? Which treatment is necessary? What must be true before access is granted? How will a control be shown to work? What happens when the answer is no?

THE STANDARD AND THE CONTROL REFERENCE

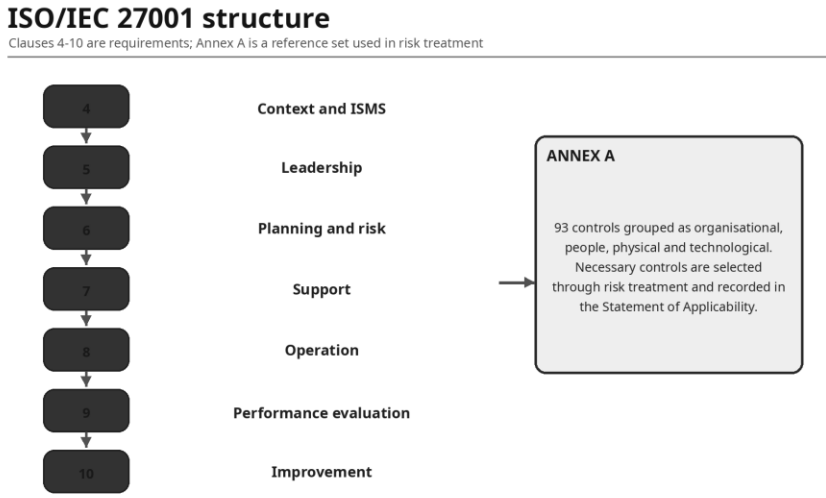

Figure 2 - Clauses 4-10 contain the certifiable ISMS requirements; Annex A is the reference set used during risk treatment.

All requirements in clauses 4 to 10 apply to an organisation claiming conformity. Annex A is used to check control completeness during risk treatment. Necessary controls may come from Annex A, another source or the organisation's own design, and the resulting position belongs in the Statement of Applicability.

CHAPTER 1

The Bid Security System You Already Have

CASE FILE

At 18:07, fifteen minutes after the external writer left the project, Priya asked IT to remove his access.

IT could not find the account.

He had been invited as a guest through a link created by the sales director. The link had no expiry. It opened the full opportunity workspace: customer documents, pricing drafts, staff CVs, partner agreements, review comments and the folder marked SUBMITTED. The writer had needed three questions and one case study. He could see almost everything.

Nobody had intended to give him permanent access. Nobody had designed a control that made the intention matter.

The organisation already had an information security system. It consisted of habits, platform defaults, personal judgement, hurried approvals and whatever the team did when a deadline became uncomfortable. Some of it worked. Some of it worked only because Priya remembered which link had been sent.

ISO/IEC 27001 begins there. Not with a policy template. With the system that exists when people are busy.

A bid is an information-processing operation

A bid team receives information, interprets it, combines it with internal knowledge and releases a controlled representation of the organisation to a customer. That sounds formal because the work is formal, even when it happens in a chat window.

Inputs may include notices, specifications, contracts, pricing schedules, customer data, site information, security questionnaires, incumbent assumptions, staff details, certifications, financial information, technical architecture, source material from partners and previous delivery evidence.

The team creates more information as it works: qualification decisions, customer insight, risk assessments, solution diagrams, commercial models, draft answers, reviewer comments, promises, clarification questions, approvals, submission files and handover records.

Some information is public. Some is commercially sensitive. Some contains personal data. Some may reveal security weaknesses or privileged architecture. Some arrives under a non-disclosure agreement. Some is supplied by a public buyer who expects it to remain inside a defined portal or team.

The security question is not simply whether files are encrypted.

It is whether information remains appropriately confidential, accurate, complete and available throughout the pursuit, and whether people can show how important decisions were made.

Confidentiality, integrity and availability in the bid room

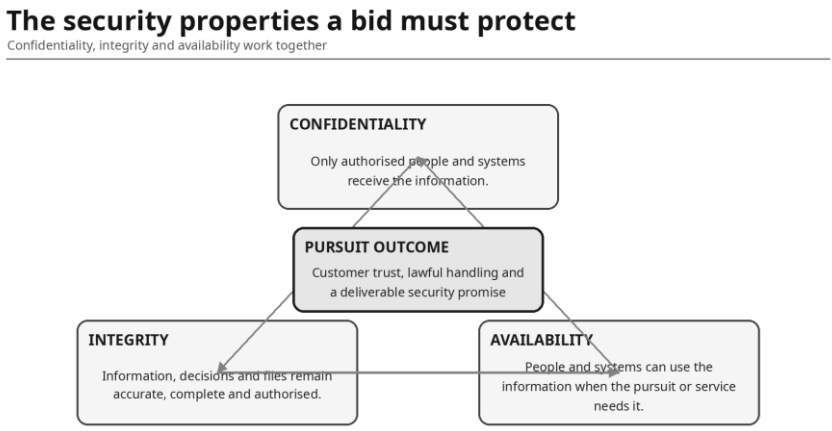

Figure 3 - Confidentiality, integrity and availability applied to bid information and operating promises.

The three familiar information-security properties become practical very quickly.

Confidentiality means that information is available only to authorised people and used only through permitted routes. A pricing analyst may need the complete cost model. A freelance editor probably does not. A consortium partner may need its work package and the buyer's relevant requirements, not every competitor assumption or another partner's margin.

Integrity means that information remains accurate, complete and protected from unauthorised or accidental change. The correct pricing workbook must remain the correct workbook. A clarification should update every affected answer. A reviewer must not unknowingly comment on a draft that has been superseded. The submitted security schedule must describe the same hosting model that was approved.

Availability means that information and systems are accessible when required. A secure repository that nobody can reach during the final upload is not an effective control. Nor is a portal account held by one person who is on a flight. Security includes resilience, deputies, backup access and recovery.

Other properties matter as well. Authenticity asks whether a file, person or instruction is what it claims to be. Accountability asks who performed an action. Non-repudiation, where relevant, helps demonstrate that an event or approval occurred. These do not replace the central three. They sharpen them.

The ordinary Wednesday test

Choose one live opportunity. Follow its information, not its meetings.

Who discovered the opportunity? Which source was trusted? Where were the original files stored? Who decided the classification? Which people received access, and why? Did the customer impose particular restrictions? Were personal data or security-sensitive diagrams present? What information entered a supplier platform, transcription service or AI tool?

Continue.

Who can alter the commercial model? How is an approved evidence item distinguished from an old one? What happens when a partner sends an attachment from a personal account? Which version is released? How are hidden comments and metadata checked? Who can submit? Where is the receipt retained? When is access removed? How long are unsuccessful drafts kept?

If the answer is, 'Sam knows', remove Sam from the room for ten minutes and ask again.

At Bracken Systems, Sam knew every portal, every folder and every customer restriction. He also knew that the chief executive disliked multi-factor authentication on his mobile because it slowed him down. Sam quietly approved sign-ins when the executive telephoned.

Then Sam became ill during a strategic tender.

The team could access the collaboration space, but not the customer's secure portal. A colleague found the password in an old notebook. The second authentication factor still went to Sam's phone. Four hours disappeared before the buyer's support desk reset the account.

The problem was not that Sam was indispensable. The problem was that the organisation had accepted indispensability as a control.

Security exists at the handovers

Many information failures occur between familiar tasks.

Sales sends account notes to bidding without explaining which statements came from public engagement and which were personal inference. The bid manager sends the full tender pack to an external consultant because separating the relevant files takes time. The solution architect exports a diagram to a design agency without removing internal IP addresses. Finance sends the pricing model by email because the guest user cannot open the protected workspace. The production lead converts the final document and accidentally retains tracked changes.

Each person may perform their own task competently. The failure appears where information changes owner, system, format, status or purpose.

Map those handovers. For each one ask:

- what information moves;
- who sends and receives it;
- why the recipient needs it;
- what classification and restrictions apply;
- which secure route is approved;
- how integrity is checked;
- what record remains;
- when access or copies should end.

A control that depends on everybody remembering to be sensible is not entirely useless. It is simply weaker than people often admit.

Assets are more than laptops

An information asset is anything with value to the organisation or its interested parties that needs protection. In a pursuit, this may include information, software, services, devices, people, relationships and physical records.

A practical asset view might include:

- customer tender documents and portal messages;
- bid strategy and competitor analysis;
- solution architecture and technical designs;
- commercial models, rates and margins;
- staff CVs, qualifications and personal details;
- contracts, non-disclosure agreements and legal advice;
- partner information and due-diligence material;
- approved evidence, case studies and customer permissions;
- collaboration platforms, CRM, email, AI tools and pricing systems;
- portal accounts, authentication methods and cryptographic keys;
- knowledge held by specialists;
- the submitted baseline, receipts and handover records.

Do not create an asset register that lists every mouse and forgets the customer dataset. Asset detail should support risk decisions, ownership and control.

For a small bid consultancy, one record may group similar assets: client tender packs, client credentials, draft responses, evidence and commercial files. A national supplier may need finer separation by platform, business unit, data type and owner.

The test is whether the register helps the organisation understand what could be harmed and who is responsible.

The threat is not always a criminal

Bid teams often picture information security as an external attack. External threats are real: phishing, credential theft, malware, extortion, hostile intelligence, supply-chain compromise and deliberate theft of commercial material.

Ordinary work creates risks too.

A well-meaning director forwards a confidential schedule. An exhausted writer pastes restricted content into the wrong browser window. A consultant retains local copies after the project. A formula is altered accidentally. A departed employee's account remains active. A cloud service changes its terms. An automatic transcription platform stores meeting content outside the expected region. A shared link is indexed or forwarded.

Threat, vulnerability and consequence belong together. 'Phishing' alone is not a useful risk statement. A more useful scenario might be:

> **WORKING WORDS**
>
> A bid team member is deceived into approving a fraudulent sign-in because the collaboration account lacks resistant authentication and the team is expecting an urgent supplier request, leading to unauthorised access to customer documents, commercial models and personal data.

Now the organisation can discuss likelihood, consequence, existing controls and treatment.

Controls should sit near the decision

Security checks placed only at the end create the same problem as final quality checks. One person is expected to find every access error, unsupported claim, infected file, exposed metadata, incorrect recipient and missing approval during the last hour.

That is not assurance. It is a crowded emergency.

Controls belong near the risk.

Opportunity qualification identifies unusual security obligations before the organisation commits. Workspace design controls access before documents spread. Classification controls handling before people choose tools. Supplier due diligence occurs before data is shared. Source approval protects integrity before writing. Design review tests security architecture before the narrative hardens. Release checks remove comments and verify files before submission. Handover transfers security commitments before delivery begins.

The final check still matters. It confirms that the system worked. It should not rebuild the system at 11:36.

The process has security customers

The contracting authority is an obvious interested party. It expects the bidder to protect information supplied through the procurement and to make accurate statements about the offered service.

There are others.

Staff expect their personal data to be handled lawfully and securely. Delivery teams need to know which security obligations they inherit. Partners need clear boundaries and safe communication routes. Finance needs commercial information protected from unnecessary access. Legal and data-protection specialists need material issues escalated. Certification auditors need objective evidence that the ISMS operates within scope. Leadership needs enough information to accept risk deliberately.

A bid process that protects the customer file but sends delivery an inaccurate security promise has not succeeded.

Security is not only about keeping information secret. It is also about ensuring that the information passed onward is trustworthy and usable.

The first secure-pursuit process card

Start with one page. Name the process in language the organisation uses, perhaps 'Secure End-to-End Bid Management'. Record:

- purpose and intended results;
- start and end points;
- information assets and main inputs;
- stages, decisions and outputs;
- process and information owners;
- interested parties and relevant requirements;
- classification and access principles;
- systems, suppliers and physical locations used;
- security risks and treatment routes;
- acceptance and release criteria;
- records and retention;

• measures and incident routes;
• interactions with sales, IT, security, legal, finance, HR, delivery and contract management.

The card is not an ISMS. It is a map that lets people find the real work.

Walk it with a live bid. Ask where it lies.

At Bracken Systems, the process card claimed that access was role-based. The live workspace showed twenty-seven people, including two former employees and an agency designer. The card claimed that external transfers used the secure portal. Finance was using email because the portal blocked macros. The card claimed access was removed at close. Nobody owned close.

The workshop became useful when the team stopped defending the document.

A maturity check without performance

Score each statement from zero to three. Zero means absent. One means dependent on individual memory. Two means defined but inconsistently applied. Three means routinely applied and supported by evidence.

• Information assets and owners are understood.
• Customer restrictions and legal requirements are identified early.
• Opportunity risk influences pursuit depth and tool choice.
• Workspaces use approved systems and least-necessary access.
• External contributors receive only the information they need.
• Classification, transfer and retention rules are understood.
• Risk assessment and treatment produce usable decisions.
• The Statement of Applicability reflects the organisation's real controls.
• Security claims trace to approved evidence.
• Solution, price and security commitments remain aligned.
• Incidents and near misses are reported without concealment.
• Release includes file, metadata and recipient checks.
• Access and promises transfer cleanly after the result.
• Monitoring, audit and corrective action change the system.
• The process can operate when its strongest individual is absent.

Do not add the scores too quickly. A total can conceal a zero where the damage sits.

Strong endpoint protection does not compensate for uncontrolled guest access. A complete policy library does not compensate for a false security answer. An excellent incident procedure does not compensate for nobody recognising an event.

Look at the pattern.

What to do this week

Choose one recent or live bid and reconstruct the information path. Use access logs, sharing links, emails, portal records, file histories, supplier accounts, interviews and final submission evidence. Do not improve the story while recording it.

Mark every point where:

• information entered or left an approved system;
• access was granted, widened or removed;
• classification was assumed;
• a person copied data for convenience;
• a supplier or AI service processed information;

- a material file changed;
- an approval affected integrity;
- an incident or near miss occurred;
- the final files were released;
- security promises became delivery obligations.

Then choose three controls. Give each an owner, trigger, method, evidence and review date. Three is enough for the first week.

The objective is not to make bidding slower. Uncontrolled bidding is already slow. People search for the right file, repair permissions, repeat explanations, recreate approvals and discover risk when choices have disappeared.

A working ISMS protects information and preserves options.

The system exists now. Your first job is to see it.

CHAPTER 2

ISO/IEC 27001 Without the Fortress Theatre

CASE FILE

Northmere Analytics held an ISO/IEC 27001 certificate.

The certificate sat on the website beside a padlock icon. In a live bid, the security answer said the company operated 'military-grade protection across all information assets'. Nobody could explain what military grade meant. The tender pack was open through an anonymous sharing link because one reviewer had struggled with guest access.

The certification had not failed Northmere. The organisation had allowed the certificate to become a substitute for an explanation.

What the standard is trying to do

ISO/IEC 27001 specifies requirements for an information security management system. The system is intended to help an organisation establish, implement, maintain and continually improve a structured approach to information security risk.

It is not a catalogue of products. It does not prescribe one firewall, one cloud, one risk matrix or one way of organising a bid room. A software company, law firm, manufacturer, charity, local supplier and proposal consultancy can use the same requirements while operating very different controls.

The standard is deliberately generic. That is useful, and sometimes irritating. It will not tell the bid director how many people should have access to a pricing model, whether transcription is allowed, which review should inspect security architecture or how long an unsuccessful draft should be kept.

The organisation has to decide what is necessary, based on context, interested parties, scope, information-security risks and obligations.

That decision must survive evidence.

Use the full name

The correct reference is ISO/IEC 27001 because the standard is jointly published by the International Organization for Standardization and the International Electrotechnical Commission.

In ordinary conversation, people shorten it. On a certificate, tender response, contract schedule or formal assurance statement, use the full reference and edition accurately: ISO/IEC 27001:2022, with Amendment 1:2024 where relevant to the stated basis.

Do not say the organisation is 'ISO certified'. ISO does not certify organisations. Certification is performed by certification bodies. Accreditation bodies assess the competence of certification bodies within their schemes.

In the United Kingdom, UKAS accredits bodies for management-system certification, including information-security management systems. A tenderer should check the certificate, issuing body, accreditation, scope, sites, edition, status and dates rather than treating the logo as complete proof.

Clauses 1 to 3 set the frame

Clause 1 defines the purpose and broad applicability of the requirements. The standard is intended for organisations of any type and size. It focuses on an ISMS that protects information through risk management.

Clause 2 identifies the normative reference. ISO/IEC 27000 provides the overview and core vocabulary used across the family. Because the reference is not a decorative reading list, definitions matter when organisations use terms such as risk, control, incident, interested party, process and information security.

The current overview edition at publication of this book is ISO/IEC 27000:2026. An organisation should use current authorised material rather than an old glossary copied into a policy in 2019.

Clause 3 points users to the applicable terms and definitions. This sounds small until two departments use the same word differently.

Security calls an event something that may indicate a breach or control failure. Operations calls every service interruption an incident. Legal reserves 'breach' for a confirmed legal conclusion. The bid team writes 'no incidents in five years' without deciding which definition supports the statement.

Definitions are controls when they change meaning.

Clauses 4 to 10 form the management system

The main requirements sit in clauses 4 to 10.

Clause 4 - Context of the organisation. Understand internal and external issues, relevant interested parties and requirements, define the ISMS scope and establish the necessary processes.

Clause 5 - Leadership. Top management remains accountable, establishes policy, integrates security into business processes and assigns responsibilities and authority.

Clause 6 - Planning. Address risks and opportunities affecting the ISMS, establish a repeatable information-security risk assessment, determine risk treatment, prepare the Statement of Applicability, set objectives and plan changes.

Clause 7 - Support. Provide resources, competence, awareness, communication and controlled documented information.

Clause 8 - Operation. Plan and control the work, perform information-security risk assessments at planned intervals and when significant changes occur, and implement the risk-treatment plan.

Clause 9 - Performance evaluation. Monitor and evaluate information-security performance and ISMS effectiveness, conduct internal audits and hold management reviews.

Clause 10 - Improvement. Improve continually and respond to nonconformity through correction, cause-based action and effectiveness review.

For a secure bid operation, clause 4 shapes boundaries and interested-party requirements. Clause 6 decides security risk and treatment. Clause 7 makes the people and workspace capable. Clause 8 is the work happening. Clause 9 asks whether it works. Clause 10 changes what did not.

The clauses are not departments. They are connected questions about one system.

Annex A is a reference set, not a complete shopping list

Annex A contains 93 information-security controls arranged in four themes: organisational, people, physical and technological.

The numbers are useful. The myth around them is not.

The organisation first determines the controls it needs through risk treatment and other requirements. It then compares those necessary controls with Annex A to check whether something necessary has been missed. The Statement of Applicability records the necessary controls, why they are included, whether they are implemented and why any Annex A controls are excluded as unnecessary.

A control may be necessary even though it does not appear in Annex A. A sector regulator, customer contract, national framework, internal architecture or specialist control set may create a different requirement. That control still belongs in the Statement of Applicability if it is necessary for the ISMS.

Equally, an Annex A control does not become mandatory simply because it is printed in the reference set. The organisation must justify why it is unnecessary if excluded.

All clauses 4 to 10 apply. Annex A controls are selected and justified through risk treatment. Mixing those two ideas creates weak systems and unnecessary paperwork.

ISO/IEC 27002 explains controls in more depth

ISO/IEC 27002:2022 provides guidance on information-security controls. It expands the control concepts and offers implementation guidance and related attributes. It is valuable when designing controls and assessing whether a short Annex A label has been understood properly.

ISO/IEC 27002 is not the certifiable requirements standard. An organisation is certified against ISO/IEC 27001 within a defined scope.

This matters in bids. A supplier may write 'certified to ISO 27002'. That statement is normally incorrect. It may use ISO/IEC 27002 guidance. It may be certified to ISO/IEC 27001. The difference should not be hidden by a missing slash and a confident sentence.

Risk management is the centre, not the register

ISO/IEC 27001 preserves confidentiality, integrity and availability through a risk-management process. The risk register is evidence of part of that process. It is not the purpose.

A useful risk process establishes context and criteria, identifies risks, analyses and evaluates them, selects treatment, determines necessary controls, gains risk-owner approval, accepts residual risk through authority and checks whether treatment works.

The standard does not force one scoring model. A three-by-three matrix may suit a small consultancy. A complex critical-service provider may need richer consequence and likelihood analysis. Both require consistency and decisions that match the stated criteria.

Risk should alter behaviour.

If the tender contains personal data, guest access and retention may change. If the solution uses a new cloud region, legal and architectural review may deepen. If a bid requires source code to be shared, the organisation may need a controlled disclosure environment. If an external writer needs one answer, access should not default to the whole pursuit.

A risk recorded in red while the work proceeds unchanged is colour management.

The 2024 climate amendment

Amendment 1:2024 added an explicit requirement to determine whether climate change is a relevant issue within organisational context, and reminded organisations that relevant interested parties may have climate-related requirements.

For a bid ISMS, the answer is not automatically a carbon policy.

Climate change may affect office access, travel, power, connectivity, data-centre resilience, supplier continuity, physical records, remote working, staff availability and the security obligations of proposed services. Customers may also require climate-resilient technology, reporting or supply-chain evidence.

A cloud-based consultancy may conclude that direct exposure is limited but that provider resilience and customer requirements are relevant. A print, logistics or field-service bidder may face more immediate physical and supply-chain effects.

The determination should be reasoned, reviewed and connected to action where relevant.

'Climate change is relevant because it is important' is not an analysis.

Implementation is different from certification

An organisation may implement an ISMS without seeking certification. Certification adds independent assessment within a defined scope. It may support tender access, customer assurance, governance and market credibility.

Certification does not prove that every system is secure, every Annex A control is implemented, every supplier is safe or every answer in a tender is accurate. It shows that an accredited certification process has assessed the organisation's ISMS against the standard within the stated scope and certification arrangements.

The scope matters.

A certificate covering 'development and support of the hosted analytics platform from the London office' may not cover a recently acquired consultancy, overseas delivery centre or unrelated managed service. A bid team should not expand the certificate through language.

The customer may ask for the certificate, the scope, the Statement of Applicability, a bridge letter, recent audit evidence, security test summaries or opportunity-specific answers. Each item performs a different job.

The scope trap in bidding

Some companies seek ISO/IEC 27001 certification because tenders ask for it. The commercial reason is understandable. The scope must still reflect real, controlled activities.

A bid consultancy could define a scope around the provision of bid management, tender writing, review and related services, including the information systems and suppliers used to handle client material.

A wider supplier may include information systems and business processes supporting the design, delivery and support of its services. The bid process then sits inside a broader ISMS.

A narrow scope is not automatically weak. A misleading scope is.

Ask whether the boundaries cover the information, people, locations, systems and external services that produce the assured outcome. If pricing files are processed by a separate shared-service centre outside scope, the interface still matters. If a parent company provides identity management, that externally provided process needs control.

The certificate line should not be written to impress one procurement and confuse the next auditor.

Security documentation is not the objective

The standard requires documented information necessary for the effectiveness of the ISMS and particular records required by its clauses. Information may exist in workflows, databases, tickets, dashboards, logs, policies, diagrams, registers, approvals and conventional documents.

A two-page secure-bid process with working controls can be stronger than a seventy-page manual nobody uses.

Ask what confidence is needed.

A risk assessment needs criteria, results and approval. A Statement of Applicability needs control decisions. A workspace needs access records. A security claim needs evidence. An incident needs a timeline and actions. A released file needs identity and approval. The form can vary. The evidence cannot simply vanish because the team prefers agility.

Northmere reduced its security manual by half. That was not the improvement.

The improvement was that anonymous links were disabled, guest access gained owners and expiry, the certificate scope was checked before use, security answers cited controlled evidence and the chief executive stopped describing encryption as military grade.

The next tender did not praise the shorter manual.

It asked who could access customer data.

Northmere could answer.

The anti-fortress test

Take any security policy, control or technology and ask:

1. Which information-security risk or requirement does it address?
2. Who uses or operates it during ordinary work?
3. What evidence shows it functions?
4. What happens when people need an exception?
5. How does failure become visible?
6. When was the control last changed because evidence required it?

If the answers depend on a logo, a product brochure or the phrase 'industry standard', the control may be theatre.

Security should make authorised work safer and more reliable. A fortress nobody can enter will be bypassed. A door that never locks is not user-friendly.

The work is to design the route people can actually use.

CHAPTER 3

APMP and ISO/IEC 27001: Two Views of the Same Pursuit

CASE FILE

At Westmoor Digital, the information-security manager and proposal director agreed on almost nothing except that the other one arrived too late.

The security manager said the bid team shared information without control. The proposal director said security blocked tools after work had already started. Security used asset registers, risk treatment, incident procedures and statements of applicability. The bid team used capture plans, compliance matrices, colour reviews and submission schedules.

Both sides had a process.

Neither could follow customer information from opportunity discovery to contract mobilisation without crossing an argument.

Then an external reviewer downloaded a complete tender pack to a personal laptop. The customer discovered the transfer through its own monitoring. The discussion became more specific.

Different disciplines, different questions

APMP is a professional association for people involved in winning business through capture, bids, proposals, tenders and related work. Its public Winning Business Ecosystem describes a pursuit from pre-bid and capture through proposal, post-bid activity and implementation.

ISO/IEC 27001 is a management-system requirements standard. It asks the organisation to establish, operate, evaluate and improve an ISMS based on risk.

APMP practice helps answer pursuit questions. Which opportunity should be chased? What should capture discover? How should requirements be analysed? What belongs in the plan? When should reviews occur? How do price, strategy and content stay aligned? What happens after the result?

ISO/IEC 27001 asks how information used in those activities remains appropriately protected. What is inside scope? Which interested-party and legal requirements apply? What information assets are involved? Who has access? Which risks are accepted? How are suppliers controlled? What evidence shows the controls work? How are incidents and failures corrected?

One is not a substitute for the other.

A proposal team can follow recognisable APMP practices while using uncontrolled information. An organisation can hold ISO/IEC 27001 certification and still run a strategically weak or poorly written bid. The useful system combines pursuit craft with security discipline.

The four pursuit stages and their security questions

Pre-bid and capture includes opportunity identification, customer understanding, qualification, competitive positioning, partners, resources and strategy.

The security questions begin immediately. What customer or market information is being collected? Is it public, permissioned, confidential or speculative? What legal or contractual restrictions apply? Does the opportunity require clearances, hosting conditions, certifications, privacy controls or unusual supplier assurance? Which early security gap could make the opportunity unwinnable or undeliverable?

Bid and proposal includes solicitation review, planning, solution development, pricing, evidence, writing, reviews, production, release and submission.

Now information volume rises. Customer files arrive. Guest users join. Security schedules expose architecture. CVs and financial data move. External tools process content. The ISMS needs classification, access, secure workspaces, supplier control, version integrity, risk treatment, release criteria and incident routes.

Post-bid and proposal includes evaluation support, clarification, presentation, negotiation, award or debrief and transition.

The submitted baseline becomes important. A two-line clarification can create a new security commitment. A presentation may reveal an architectural detail not approved for disclosure. Negotiation can change liability, incident notification, data location or audit rights. Customer communication needs authority and a record.

Implementation includes mobilisation, contract administration, deliverables, change, closeout, learning and continued relationship.

Security promises become operational. Access is provisioned. Suppliers process data. Logging, backup, incident response and continuity are tested. The bid's evidence may become inaccurate or stronger. The ISMS has to carry information and risk beyond the award email.

A compliance matrix is also a security control

A compliance matrix is usually described as a way to track tender requirements. It also protects integrity.

Security requirements rarely sit in one schedule. They may appear in the invitation, specification, contract, data-processing terms, security policy, architecture appendix, pricing notes, clarification responses and portal fields.

The matrix gives each requirement a source, owner, response location, evidence and status. If a clarification changes a data-retention period, the affected design, price, contract position and answer can be identified.

ISO/IEC 27001 does not require a compliance matrix by name. It requires the organisation to determine relevant requirements, control documented information and operate its processes. APMP practice supplies a useful artefact. The ISMS supplies the security and governance questions around it.

That is alignment without forcing one discipline to pretend it invented the other.

Capture intelligence needs boundaries

Capture teams collect valuable information. They also create risk when source, permission and sensitivity are unclear.

APMP-aligned capture may examine customer objectives, incumbent position, competitors, likely route, stakeholders and win themes. The ISMS asks whether the information was

obtained lawfully, whether it contains personal data or customer confidence, which system may store it, who can use it and when it should be corrected or removed.

Westmoor introduced three labels into capture records:

- known and source-backed;
- reasoned inference;
- unresolved or unknown.

It added a handling label where information was not public.

The change did not make capture timid. It stopped one account director's private opinion being repeated as the buyer's confirmed security concern in six answer plans.

Colour reviews need security maturity

APMP's public lifecycle refers to colour-team reviews such as Pink, Red and Gold. Organisations use the names differently. The colour is not the control. The review question is.

A strategy review may test whether security requirements and customer risk are understood. A solution review may examine data flows, access, suppliers, logging, continuity and price. A Pink review may test whether answer plans contain the right evidence. A Red review may score the near-complete response and inspect unsupported security claims. A Gold review may confirm residual risk, commitments and release.

Each review needs entry criteria.

A Red review cannot evaluate architecture if the data-flow diagram is illustrative, the cloud supplier is undecided and the incident model has not been costed. Reviewers will mark prose around a missing design.

Define:

- review purpose;
- expected maturity;
- inputs;
- reviewer competence and independence;
- criteria;
- security information they may access;
- finding severity;
- closure and verification;
- authority to proceed or stop.

Security specialists should not arrive only to comment on password policy. Proposal reviewers should not score a technical claim they cannot assess. Both can contribute when the review has a job.

The integrated gate model

A practical secure-pursuit system can use six gates.

Gate 0 - Market and route relevance. Is this customer, framework, dynamic market or sector consistent with strategy, security capability and risk appetite?

Gate 1 - Opportunity qualification. Can the organisation meet mandatory security, privacy, data, clearance, hosting, supplier and contractual requirements at an acceptable risk and cost?

Gate 2 - Strategy and secure-solution commitment. Do leadership, operations, technology, security, privacy, commercial and partners support the proposed design and boundaries?

Gate 3 - Response readiness. Are documents controlled, requirements mapped, access appropriate, sources approved, workspaces secure and people competent to develop the response?

Gate 4 - Release. Does the final submission meet requirements, contain approved security claims, use the correct files and retain no unintended content or metadata?

Gate 5 - Result and transition. What access, records, incidents, obligations, risks and improvements follow award, loss, clarification or delay?

The gate depth changes with risk. A low-value repeat quotation may use a brief recorded check. A sensitive national service may require independent architecture assurance, formal risk acceptance and a mobilisation exercise.

The logic remains. A decision is made by authority, using evidence, before the next irreversible commitment.

Security artefacts need one job

Combining APMP and ISO can produce template growth if nobody resists.

The team creates an opportunity security questionnaire, bid risk register, ISMS risk register, data-protection checklist, supplier form, AI form, access log, decision log, security schedule tracker, evidence register and Statement of Applicability extract. Some are necessary. Several may repeat the same fact.

Before creating another record, ask:

1. Which decision, risk or requirement does it support?
2. Who uses it, and when?
3. Is the information already controlled elsewhere?
4. Does combining records reduce clarity or improve it?
5. What evidence must remain after the bid?

A small organisation may combine opportunity security qualification, data classification, key risks and required approvals in one gate record. A large consortium may need separate records with defined links and access restrictions.

Do not force every Annex A control into a bid checklist. Do not compress the entire ISMS into a spreadsheet only the security manager understands.

The secure pursuit charter

For Enhanced and Strategic bids, create a short charter. It may include:

- opportunity and customer;
- security classification and information types;
- applicable customer, legal and contractual requirements;
- approved systems and prohibited routes;
- key roles and decision authority;
- supplier and AI boundaries;
- risk-assessment method and escalation;
- security review points;
- incident reporting route;
- release and retention rules;

• handover expectations.

The charter should not repeat every policy. It tells the live team which parts of the system matter now.

Westmoor's first charter prohibited customer-confidential information in consumer AI services, required guest access to expire seven days after submission and named the information owner for the solution architecture. It also stated that urgent exceptions could be approved by the security director and bid director together.

During the bid, an external designer needed a diagram. The team did not spend two days debating policy. It created a redacted design extract, granted time-limited access and recorded the approval.

Control made the work possible.

Security belongs before the tender arrives

An ISMS that begins when the formal documents arrive is already late.

The organisation may have chosen an insecure sales tool, retained account notes without purpose, promised a cloud provider, agreed a partner, advertised a certification scope or shared customer information during capture. Those choices shape the pursuit.

Pre-bid security controls can be lighter, but they should exist. Establish approved systems, source and handling discipline, risk triggers, supplier boundaries and clear rules for live-procurement communication.

Customer understanding should improve the offer without turning professional contact into uncontrolled surveillance.

Security belongs after submission

Westmoor used to archive the final PDF and close guest access when somebody remembered. Delivery received a slide deck. The ISMS held no route from submitted security promises into operational control.

The integrated lifecycle changed the endpoint.

On submission, the team retained the exact files, release decision, risk position, security evidence, clarification log, supplier commitments and promise register. On award, delivery accepted the obligations and raised open issues. On loss, access was removed according to purpose, records were retained according to policy and feedback altered controls where justified.

Security had stopped being an attachment to the bid.

It became part of the pursuit's memory.

A thirty-day integration exercise

Select one live opportunity. Do not redesign both systems at once.

Week one: map APMP-style pursuit activities, information inputs, outputs, people, systems and suppliers.

Week two: connect each stage to existing ISMS controls: classification, access, risk, supplier management, incident reporting, documented information and retention.

Week three: remove duplicate records, define security review criteria and establish the submitted-baseline handover.

Week four: conduct a short internal audit following one sensitive information item from source to current state. Record what happened, not what policy expected.

Westmoor found three anonymous links, nine duplicate risk fields and a good joiner-leaver process that had never been extended to bid guests. It also discovered that the proposal director's release checklist already performed several integrity controls security had planned to recreate.

The security manager stopped sending generic awareness slides to the bid team.

The proposal director stopped describing the ISMS as a certificate-maintenance project.

They were not finished.

They were finally working on the same pursuit.

CHAPTER 4

Context, Interested Parties, Scope and the ISMS

CASE FILE

Hartwell Advisory's first context workshop produced four risks.

Cyber attacks. Data breach. Staff error. Supplier failure.

All four were true. None explained what the organisation should do differently on Monday.

Then a bid manager mentioned that one client prohibited overseas processing. The finance director said pricing models were being shared with a subcontractor through personal email. IT admitted the proposal platform was administered by a former employee's account because changing ownership might disrupt access. HR said CVs contained more personal information than tenders required.

The context became less dramatic and more useful.

Clause 4.1 - Understand the organisation and its context

The organisation must determine internal and external issues relevant to its purpose and affecting the intended outcomes of the ISMS. It must also determine whether climate change is a relevant issue.

The standard does not require one analysis method. SWOT, PESTLE, risk workshops, threat reports, audits, customer feedback, legal registers and management discussions may all contribute.

A useful context issue has a consequence.

'Cyber threats are increasing' is background.

'Bid teams receive realistic credential-theft messages during supplier onboarding; therefore external invitations require a verified contact route, strong authentication and a reporting path' is context influencing control.

'Remote work is common' is background.

'Proposal teams use home networks and travel during final review; therefore sensitive work requires managed devices, encrypted storage, approved connectivity and a tested route when remote access fails' is managed context.

For secure bid operations, external issues may include:

- customer security expectations and procurement schedules;
- cyber threats and fraud methods;
- legal, regulatory and contractual obligations;
- cloud, AI and collaboration technology;
- supplier concentration and service dependency;
- market expectations for certification;

- sector-specific assurance frameworks;
- geopolitical, economic and supply-chain conditions;
- climate-related disruption;
- skills availability and changing work patterns.

Internal issues may include:

- strategy and risk appetite;
- service and technology architecture;
- information assets and data flows;
- leadership behaviour;
- culture and reporting confidence;
- competence and capacity;
- legacy systems;
- evidence maturity;
- remote and hybrid working;
- acquisition, restructuring or outsourcing;
- prior incidents, audit findings and delivery failures.

Do not list the entire world. Identify the issues that affect information-security decisions, controls, objectives, resources or risks.

Climate relevance needs a real answer

The 2024 amendment makes the climate question explicit. The answer may differ by organisation and scope.

Hartwell's main work was digital and remote. The team initially concluded that climate change was irrelevant. The business-continuity lead challenged that conclusion. The primary office sat in a flood-prone area. Two key cloud suppliers operated across regions. Severe weather had previously caused power and connectivity loss during a deadline. Several target customers now asked for climate-resilient service and supplier emissions information.

Climate change did not create a new cyber policy.

It affected resilience, supplier monitoring, remote working, information availability and customer requirements. Those issues entered the context register, continuity testing and qualification process.

A different organisation may reach a narrower conclusion. 'Not relevant' remains possible. It needs a reason and review, not a pre-written sentence.

Clause 4.2 - Interested parties and relevant requirements

An interested party matters when it can affect, be affected by or perceive itself to be affected by the ISMS, and when its requirements are relevant to information security.

The organisation identifies relevant parties and relevant requirements. It also determines which requirements will be addressed through the ISMS.

Possible parties in bid work include:

- contracting authorities and private buyers;
- service users and data subjects;
- employees and contractors;
- delivery and mobilisation teams;
- regulators and supervisory authorities;

- shareholders, insurers and lenders;
- partners, subcontractors and cloud providers;
- professional and certification bodies;
- internal sales, finance, legal, HR and IT functions;
- framework managers and prime contractors.

Do not create a Christmas-card list.

For each party, record the requirement, source, ISMS relevance, process affected and monitoring route.

A buyer may require ISO/IEC 27001 certification, incident notification within a stated period, UK-based hosting, staff screening, secure development, access to audit evidence or restrictions on subcontracting. Staff may require lawful, proportionate handling of CV and vetting information. Delivery may require complete transfer of security obligations. A cloud provider imposes technical and contractual boundaries that the organisation must understand.

'Regulator - compliance' is not enough.

Which regulator? Which obligation? Which processing or service? Who monitors change? What control or evidence follows?

Customer requirements do not begin at the security questionnaire

Security requirements are scattered across the pursuit.

A security schedule may ask about encryption. The contract may define breach notification. The data-processing terms may restrict location and subprocessors. A mobilisation schedule may require access controls before service start. The evaluation questions may ask for resilience and incident evidence. A clarification may alter retention.

Context and interested-party analysis help the organisation recognise requirements before they become one more spreadsheet.

They do not authorise invention.

A capture team may know that the buyer suffered a previous supplier incident because it was reported publicly. That context can shape evidence and design. A colleague's claim that 'the CISO hates cloud' remains inference until supported.

Keep facts, inference and unknowns separate.

Clause 4.3 - Define the ISMS scope

Scope sets the boundaries and applicability of the ISMS. It considers context, interested-party requirements and interfaces or dependencies between the organisation's own activities and those performed by others.

A useful scope states the organisational units, locations, services, processes, technologies and boundaries covered. It should be available as documented information.

A bid consultancy might use:

> **WORKING WORDS**
>
> Provision of bid management, tender writing, proposal review and related advisory services, including the information systems, remote-working arrangements and approved external providers used to process client information from the Manchester and London operations.

A technology supplier might use:

> **WORKING WORDS**
>
> Design, development, hosting, support and commercial pursuit of the Northstar service, including associated customer onboarding, bid management and supplier-management processes operated from the United Kingdom.

These are illustrations, not recommended wording.

Scope must follow control. If an offshore support centre processes customer tender data, the boundary cannot be made safe by leaving the location out of the sentence. If a parent company provides identity, security operations or HR screening, the dependency must be understood and controlled.

Certification scope and bid claims

The ISMS scope and the certificate scope are related but not always identical in presentation. Bidders should use the exact certificate information and avoid expanding it through implication.

Check:

- legal entity;
- sites and organisational units;
- products and services;
- standard edition and amendment basis;
- certification body and accreditation;
- issue, expiry and surveillance status;
- exclusions or boundaries evident from the wording;
- current Statement of Applicability reference where relevant.

A certificate covering corporate IT does not automatically assure the security of a newly acquired software service. A certificate covering one development site does not automatically cover every subcontractor. A certificate may still be useful evidence. It must be described honestly.

A buyer may reject a certificate because the scope does not cover the offered service. That is not an argument about branding. It is a requirements issue that should have been found at qualification.

Scope the pursuit process

Define where secure end-to-end bid management begins and ends.

Does it begin when a lead appears in the CRM, when capture starts or when formal documents arrive? Does it end at submission, result, handover, retention review or contract close-out?

A narrow boundary leaves risk outside control.

If the process begins only at tender receipt, customer information collected during capture may use unapproved systems. If it ends at submission, guest access may remain open and security commitments may never reach delivery.

A practical boundary may be:

> **WORKING WORDS**
>
> From identification of a potential opportunity through qualification, lawful capture, solicitation receipt, security and contractual requirements review, controlled collaboration, solution and commercial development, writing, assurance, release, submission and post-submission activity, to award handover or unsuccessful closure, access removal, retention and learning.

Long, yes.

It reflects the work.

Clause 4.4 - Establish, operate and improve the ISMS

The organisation must establish, implement, maintain and continually improve the ISMS, including the processes needed and their interactions.

Do not build one process for every clause.

People do not perform 'Clause 7.5' at 10:00 and 'Clause 8.2' after lunch. They classify a tender pack, grant access, assess a risk, approve a supplier, release a file and respond to an incident. The requirements live through those processes.

A bid-related ISMS process architecture might include:

Core pursuit processes: opportunity qualification, capture, tender intake, requirements review, solution design, pricing, writing, review, release, submission and handover.

Security-support processes: asset management, identity and access, supplier assurance, incident management, vulnerability management, secure configuration, backup, continuity, privacy, legal compliance, training and document control.

Management processes: context, risk, objectives, monitoring, internal audit, management review, corrective action and improvement.

Map interactions. The bid process consumes identity management, supplier security, knowledge and incident routes. It produces new assets, risks, supplier relationships and customer commitments that the ISMS must absorb.

Externally provided processes remain your problem

Hartwell's cloud platform, payroll team, external writers, managed IT provider and parent-company security operations all affected the ISMS. Some sat outside the scoped legal entity.

Outsourcing work does not outsource accountability.

Define which external or group services the scoped organisation relies upon, what requirements apply, how performance is monitored and what happens when the service changes or fails.

A parent-company identity service may be well controlled. The bid team still needs a route to request, approve and remove access. A secure cloud platform may meet recognised standards. The organisation still needs correct configuration and user behaviour.

'Provided by corporate' is not an audit trail.

Context monitoring without another ceremonial meeting

Context, interested parties and scope require review. They do not require a monthly workshop with coloured notes.

Use existing routes:

- pipeline and market reviews;
- legal and compliance monitoring;
- supplier reviews;
- threat intelligence;
- incident and near-miss analysis;
- customer feedback;
- audits;
- business-continuity exercises;
- technology change;
- management review.

Create triggers for material reassessment:

- new service, sector, country or customer type;
- acquisition or restructuring;
- major supplier or platform change;
- significant incident;
- new legal or contractual obligation;
- new AI use;
- change in working location;
- repeated tender security requirement;
- climate event affecting availability;
- change in certification scope.

When a trigger occurs, assess effect. Updating the date on the context register is not an effect.

A two-hour context and scope workshop

Invite top management, bidding, delivery, IT/security, finance, legal or privacy, HR and one person who performs ordinary bid work. Keep the room small enough for disagreement.

First thirty minutes: list changes that affected information, bids or delivery during the past twelve months. Use actual incidents and near misses.

Second thirty minutes: identify relevant parties, requirements and sources. Remove generic entries.

Third thirty minutes: test the ISMS and secure-pursuit boundaries against systems, sites, suppliers and data flows.

Final thirty minutes: decide actions, owners, dates and monitoring routes. Include the climate relevance decision.

Hartwell finished with eleven material context issues, nine relevant interested-party groups, one revised scope and six actions. The most important action was not a new policy.

The organisation moved external bid collaborators into the corporate joiner-and-leaver process and made the bid owner responsible for their end date.

The context had reached the workspace.

CHAPTER 5

Leadership, Policy, Roles and Accountability

CASE FILE

The chief executive at Arden Response disliked the secure file-transfer service.

It required a second sign-in and the link expired. At 22:16, during final review, he attached the commercial model to an ordinary email and sent it to his home account so he could work from a tablet.

The next morning he opened the leadership meeting by saying information security remained a board priority.

The policy was not false. It was simply weaker than the lesson he had delivered overnight.

Clause 5.1 - Leadership and commitment

Top management remains accountable for the effectiveness of the ISMS. Security can be coordinated by an ISMS manager, CISO or information-security lead. Accountability for integration, direction, resources and results cannot be deposited in that role and forgotten.

Leadership should ensure that information-security policy and objectives align with strategic direction, that ISMS requirements are integrated into business processes, that resources are available, that risk-based thinking is supported, that people contribute and that continual improvement occurs.

In secure bidding, leadership influence is immediate.

Executives approve opportunities, suppliers, technologies, exceptional data access, contract positions, disclosure, residual risk and final submissions. They decide whether a deadline justifies additional resource or an unsafe shortcut. They can protect a control in one sentence or remove it with the same speed.

A leader who asks the team to follow policy and then bypasses it under pressure communicates the actual policy very clearly.

Security must support the business objective

An ISMS exists to help the organisation achieve its purpose while managing information-security risk. It is not a separate security kingdom.

The bid process needs to move quickly. It also needs trustworthy information, controlled access, secure collaboration and accurate commitments. A security control that blocks all external collaboration may damage the pursuit and encourage bypass. A process that grants universal guest access may move quickly until information is lost.

Leadership has to resolve the trade-off. The answer is often better design: approved external workspaces, time-limited access, role templates, secure transfer, deputies and fast exception decisions.

Security should not be described as the department that says no. Leadership gives it authority to say not like that, not without evidence or not at this level of risk.

Sometimes the correct answer remains no.

Integrate security into pursuit decisions

Leadership commitment becomes visible when security is part of ordinary commercial governance.

At qualification, the gate considers information sensitivity, customer obligations, hosting, supplier reliance, security evidence, certification scope, incident history and the cost of required controls.

At solution commitment, leadership asks whether the proposed architecture and security model can be delivered, assured and priced.

At release, authority confirms that claims are accurate and risks are accepted.

At handover, delivery receives the security obligations it must operate.

At management review, leadership examines objectives, incidents, audit findings, supplier performance, resources, change and improvement.

If security appears only in an annual committee and a tender questionnaire, it is not integrated.

Clause 5.2 - Information-security policy

The organisation establishes an information-security policy appropriate to its purpose, providing a framework for objectives and including commitments to satisfy applicable requirements and continually improve the ISMS.

The policy should be available as documented information, communicated, understood and available to relevant interested parties where appropriate.

It does not need to sound ceremonial.

Arden replaced a generic policy with a short set of working commitments:

> **WORKING WORDS**
>
> We protect information according to its value, sensitivity, legal duties and customer requirements.

> **WORKING WORDS**
>
> We grant access for defined business need, through approved systems, for no longer than necessary.

> **WORKING WORDS**
>
> We assess information-security risk before making material commitments or introducing significant change.

> **WORKING WORDS**
>
> We report events early, correct failures and improve controls using evidence rather than blame.

The formal policy contained the necessary management-system commitments. The language remained close to decisions people made.

A useful test is to place the policy beside a difficult pursuit.

Does it help decide whether to use an external AI service? Does it support refusing an anonymous link? Does it require risk acceptance before promising a new hosting region? If the policy cannot reach the work, it may still satisfy a format. It will not lead.

Policies are a hierarchy, not one enormous document

The top-level policy sets direction. Supporting policies and standards may cover access control, acceptable use, classification, cryptography, suppliers, incidents, business continuity, privacy, remote working, secure development, logging and other necessary controls.

Do not create a separate policy for each Annex A control. Group requirements in a way people can use.

A secure-bid standard may explain:

- approved collaboration and storage;
- classification and information handling;
- guest and supplier access;
- personal data and CV handling;
- permitted AI and transcription use;
- customer communication;
- file transfer and release;
- incident and near-miss reporting;
- retention, archive and disposal;
- exception authority.

This is a local operating control under the policy, not a second ISMS.

Clause 5.3 - Roles, responsibilities and authorities

Security responsibilities and authorities must be assigned and communicated. Top management also assigns responsibility for ensuring the ISMS conforms and for reporting on performance.

A RACI table may help. It often fails where authority matters most.

For each material role, define what the person must do, what they may decide, what they may not decide and where they escalate.

Top management: sets scope, policy, objectives, risk appetite and resources. Accepts material residual risk. Cannot describe a policy exception as 'just this once' without using the exception route.

ISMS or information-security manager: maintains the management system, coordinates risk, control, audit and review. Does not own every information asset or business risk.

Bid process owner: ensures secure end-to-end pursuit controls operate and improve. Connects the ISMS to APMP-aligned practice.

Bid manager: controls the live workspace, access requests, information flow, requirements, risks, changes, reviews, release and closure. Does not become the sole technical security authority.
Information or asset owner: determines business value, handling, access need, retention and risk decisions for defined information.
System owner: ensures the platform or tool is configured, maintained, monitored and supported.
Security architect or technical lead: owns the truth of security design and its validation.
Commercial lead: ensures controls, assurance and security obligations are priced and approved.
Legal and privacy advisers: interpret relevant obligations within competence and authority.
External-provider owner: selects, briefs, monitors and ends supplier access and service.
Delivery owner: accepts the security commitments and risks that continue after award.

One person may perform several roles. The authorities should not dissolve into one name.

Information ownership has edges

Organisations frequently say the bid manager owns the tender. That phrase hides several kinds of ownership.

The customer owns information it supplies. The organisation may be a custodian under contract. HR owns authoritative employment information. Finance owns the approved commercial model. The solution lead owns the proposed design. The bid manager owns process integration and the controlled working environment. Delivery owns the service after handover.

Define ownership at the level needed for decisions.

Who decides whether a customer dataset may be shared with a subcontractor? Who approves an architecture diagram for an evaluator? Who determines retention? Who can accept residual risk from a cloud service? Who can release a security claim?

'Bid team' is not a person with authority.

Segregation of duties without enterprise theatre

Some activities benefit from separation so that one individual cannot create, approve and release a high-risk output without challenge.

Examples include:

- requesting and approving privileged access;
- developing and approving a pricing model;
- writing and independently verifying a material security claim;
- preparing and releasing final files;
- operating a control and auditing its effectiveness;
- investigating an incident and accepting its closure.

A small firm may not have separate departments. It can still create proportionate challenge. A director may approve access requested by the bid manager. A competent external reviewer may test the security answer. Finance may verify commercial commitments. Another authorised user may compare portal files with the manifest.

Segregation should reduce risk, not create a ceremonial queue.

The authority matrix

Arden created an authority matrix for decisions that had previously travelled through seniority and urgency.

The bid manager could approve ordinary internal access based on role. The information owner approved external guest access and sensitive-data sharing. IT administered accounts. The security director approved non-standard tools and significant exceptions. The commercial director approved the cost of controls and security liabilities. The executive sponsor accepted residual risk above the stated threshold. The release authority could stop submission when mandatory security evidence or approval was absent.

Emergency authority existed. It required:

- a stated business need;
- risk and affected information;
- compensating controls;
- start and expiry;
- named approver;
- review after use.

The matrix did not make exceptions impossible.

It stopped exceptions becoming invisible permanent design.

Objectives need leadership and resources

Security objectives are planned in clause 6, but leadership makes them credible.

A target to remove external bid access within one working day of closure requires ownership, system capability and reporting. A target to verify all high-impact security claims requires evidence and reviewer capacity. A target to reduce unsupported AI use requires approved tools and practical alternatives.

Leadership should ask what resource the objective needs and what behaviour it may create.

A target of zero reported events may reward silence. A target to close every vulnerability within seven days may cause inaccurate status. A target for 100 per cent training completion may produce attendance without competence.

Objectives need consequence, not only green cells.

Culture is what happens after an event is reported

Leaders often say they want early reporting. People watch what happens to the first person who reports an uncomfortable event.

A junior writer at Arden realised she had pasted a paragraph from a restricted customer schedule into an unapproved translation tool. She reported it within eight minutes. The security team assessed the provider terms, information involved and possible retention. The customer was informed through the agreed route because the contract required it. The event was contained and investigated.

The writer was not publicly blamed. She helped redesign the approved translation process.

Two weeks later, a director reported his own mistaken email recipient before recall had completed.

People had noticed the earlier response.

A reporting culture is not soft. It is fast information.

Leadership evidence is behaviour

An auditor may ask how top management demonstrates commitment. Policy signatures and meeting attendance are part of the answer. Stronger evidence sits in decisions.

Show:

- resources approved because risk required them;
- a pursuit declined because security obligations could not be met;
- an insecure tool replaced with a usable approved route;
- a serious incident reviewed without concealment;
- objectives monitored and corrected;
- supplier risk escalated;
- management review actions completed;
- a senior exception recorded with expiry;
- a security promise removed because evidence was insufficient.

One of Arden's strongest leadership records was a no-bid.

The opportunity required a segregated hosting environment and twenty-four-hour incident response within six weeks. The service could eventually provide both. The mobilisation route could not. Leadership declined the bid and funded the capability for the next cycle.

Customer focus did not mean saying yes.

A monthly secure-pursuit review

Keep the meeting short and decision-focused. Review:

- current high-risk pursuits and sensitive information;
- objectives and trends;
- access exceptions and aged guest accounts;
- incidents and near misses;
- material supplier or tool changes;
- unsupported security evidence;
- capacity and competence;
- forthcoming irreversible dates;
- corrective actions needing leadership support.

This does not replace formal management review. It provides operational leadership.

Arden's first dashboard showed that access was usually removed after submission but often remained open during delayed evaluation. The original objective used submission as the trigger. The information need continued, but the access population did not.

Leadership changed the rule. Access was reviewed at submission, result, every thirty days during delay and at closure.

No new policy was required.

A decision was.

CHAPTER 6

Risk, Objectives and Planned Change

CASE FILE

At 09:40, the leadership team at Pelham Services approved a new generative-AI platform for bid writing.

At 10:05, the first user uploaded a complete tender pack.

The data-protection review was scheduled for next Tuesday. The supplier contract was with legal. Single sign-on had not been configured. The platform's training and retention settings were still at their default.

The change had been announced as a pilot.

The information had not heard that word.

Clause 6.1.1 - Address risks and opportunities to the ISMS

The organisation considers context and interested-party requirements, then determines the risks and opportunities that need action so the ISMS can achieve intended outcomes, reduce unwanted effects and improve.

This requirement concerns the ISMS itself, not only individual cyber risks.

ISMS risks may include unclear scope, weak leadership, insufficient competence, poor reporting, unmanaged suppliers, unreliable data, ineffective audit or a risk method nobody uses. Opportunities may include better access automation, secure collaboration that reduces email, evidence reuse, stronger customer confidence and a simplified control architecture.

Actions should be integrated into ISMS processes and evaluated for effectiveness.

A register that says 'risk: human error; treatment: training' does not yet show integration or effectiveness.

Clause 6.1.2 - Establish the information-security risk-assessment process

The organisation defines and applies a risk-assessment process that produces consistent, valid and comparable results. It establishes risk criteria, including risk-acceptance criteria and criteria for performing assessments.

The process identifies information-security risks associated with loss of confidentiality, integrity and availability within the ISMS scope. It identifies risk owners, analyses consequences and realistic likelihood, determines levels and evaluates them against the criteria.

The organisation retains documented information about the process and results.

The standard does not prescribe one formula. It does require a repeatable decision method.

Define risk criteria before the room becomes excited

Risk criteria answer questions such as:

- which impact dimensions matter;
- how impact is rated;
- how likelihood is assessed;
- what existing controls mean for the rating;
- how risk levels are calculated or expressed;
- which levels require treatment or escalation;
- who may accept residual risk;
- when assessment is repeated;
- how uncertainty is recorded.

Impact may include customer harm, contractual breach, personal-data consequences, service interruption, financial loss, regulatory action, loss of competitive position, safety, reputation and strategic effect.

Likelihood should not be guessed from anxiety. Consider threat capability and intent, exposure, vulnerability, control strength, history, sector information and change.

A three-level qualitative method may be enough. A larger organisation may use detailed matrices and scenario analysis. False precision is not maturity.

Write risk scenarios people can act upon

'Cyber attack' is a topic. A risk scenario connects cause, weakness, event and consequence.

A useful structure is:

> **WORKING WORDS**
>
> Because [threat or source] can exploit [vulnerability or condition], [event] may occur, leading to [consequence for information, customer or business].

Example:

> **WORKING WORDS**
>
> Because external reviewers receive broad guest access without automatic expiry, a former contributor may retain access to customer-confidential tender material and commercial models after their role ends, leading to unauthorised disclosure, contractual breach and loss of customer confidence.

The scenario supports ownership and treatment.

Do not write a novel. Include enough specificity to choose action.

Risk ownership is not task ownership

The risk owner has authority and accountability to manage the risk. The person performing a treatment action may be different.

The bid director may own risk arising from pursuit collaboration. IT configures expiry. The information owner approves access. HR manages leavers. The system owner monitors accounts.

If the risk owner cannot fund, accept, escalate or change the process, ownership may be nominal.

Pelham initially assigned every cyber risk to the IT manager. The managing director accepted sales exceptions. HR controlled joiners and leavers. Procurement selected cloud suppliers. The IT manager owned a collection of consequences without authority.

Ownership was redistributed to business and system owners. Security remained advisory and coordinating.

Analyse the controls that exist, not the controls in the policy

Risk analysis should consider real controls and their effectiveness.

A policy requires multi-factor authentication. Is it enabled for guest users? A contract requires deletion within thirty days. Does the provider offer verifiable deletion? The incident plan names a response team. Can it be reached outside working hours? Access reviews occur quarterly. Are failed accounts removed between reviews?

Assess design, implementation and operation separately where useful.

A control may be well designed and not implemented. It may be implemented and routinely bypassed. It may operate but fail to reduce the intended risk.

The residual-risk decision depends on reality.

Clause 6.1.3 - Treat information-security risk

Risk treatment follows assessment. The organisation selects appropriate treatment options, determines the controls necessary to implement those options, compares necessary controls with Annex A to check for omission, produces the Statement of Applicability, prepares a risk-treatment plan and obtains risk-owner approval of the plan and residual risk.

Treatment options commonly include avoiding the activity, changing likelihood, changing consequence, sharing or transferring aspects of risk, and retaining risk through authorised acceptance. Controls may combine technical, organisational, people, physical and contractual measures.

The organisation should choose treatment because it addresses risk and requirements, not because a template already contains it.

Necessary controls come before Annex A comparison

The risk-treatment process determines what controls are necessary.

For broad guest access, necessary controls may include role-based access, approval, expiry, periodic review, monitoring, confidentiality terms and a defined closure process.

Then compare those controls with Annex A. The comparison may identify relevant reference controls around access, identity, supplier relationships, confidentiality, logging or documented procedures. It may also reveal that an organisation-specific control - such as a proposal-platform role template - has no one-to-one Annex A label but remains necessary.

Annex A is a completeness check and common reference. It is not the source of every risk.

Build a Statement of Applicability that can be used

The Statement of Applicability, or SoA, contains the organisation's necessary controls, reasons for inclusion, implementation status and reasons for excluding any Annex A control considered unnecessary.

The standard does not require one table layout. A practical SoA may contain:

- control identifier and description;
- source, including Annex A mapping where relevant;
- reason for necessity or exclusion;
- risks, obligations or business needs addressed;
- implementation status;
- control owner;
- evidence or linked procedure;
- review trigger;
- scope or boundary notes.

Do not reduce the SoA to 93 rows marked Yes.

Controls outside Annex A that are necessary belong in the SoA. Annex A controls excluded as unnecessary need justification. 'Not relevant' is a label, not a reason.

A mature SoA is a control-decision ledger. It helps leadership, auditors and process owners understand why controls exist and where they apply.

The risk-treatment plan is the work still to happen

The SoA says which controls are necessary and their status. The risk-treatment plan turns incomplete treatment into managed action.

Record:

- risk and treatment decision;
- control or action;
- owner;
- resources;
- target date;
- dependencies;
- acceptance criteria;
- residual risk;
- approval and status;
- effectiveness review.

Avoid treatment actions such as 'implement access control'. State what will change and how completion is known.

> **WORKING WORDS**
>
> Configure role-based guest groups for the proposal platform, require information-owner approval, set default expiry to thirty days, test on one live bid and review access-removal evidence across the next five closures by 30 November.

That can be managed.

Residual risk needs an informed owner

Controls rarely remove risk completely. The remaining risk should be understood and accepted by a person with appropriate authority.

Acceptance is not a signature added because the deadline arrived.

The owner needs the scenario, rating, treatment, control limits, remaining exposure and consequences. If information is uncertain, record that uncertainty.

Pelham's AI pilot retained a risk that approved users might include excessive customer information despite training. Treatment included data classification, workspace isolation, provider settings, logging, prompt guidance and output review. Leadership accepted a limited pilot with low-sensitivity internal content only. Customer tender packs remained prohibited until contract and technical reviews were complete.

The pilot started two weeks later.

Nothing commercially important was lost by waiting.

Clause 6.2 - Information-security objectives

Objectives should be consistent with policy, measurable where practicable, monitored, communicated, updated and supported by plans.

Plan what will be done, resources, responsibility, timing and evaluation.

Useful secure-pursuit objectives might include:

- remove or review all external bid access within one working day of result, closure or role end;
- reduce material security claims without approved evidence from a baseline of nine per quarter to fewer than two;
- complete opportunity security classification within four working hours of tender receipt for Enhanced and Strategic bids;
- achieve 100 per cent verified handover of material security commitments within two working days of award;
- reduce use of unapproved information-transfer routes by 60 per cent within six months;
- test recovery of the bid collaboration environment twice yearly and achieve the defined recovery time.

'Improve cyber security' is not an objective. It is a subject.

Measures can create unsafe behaviour

A target of immediate access removal may cause deletion before a legitimate clarification period ends. A target of no incidents may suppress reporting. A target of 100 per cent controls implemented may encourage meaningless SoA entries.

Define the intended result and guardrails.

For guest access, the objective may be timely review and removal of unnecessary access, not automatic destruction of necessary post-submission collaboration. The measure can distinguish justified retained access, overdue review and active role.

Security metrics need context.

Clause 6.3 - Plan changes to the ISMS

When changes to the ISMS are needed, they should be carried out in a planned manner.

Consider purpose, consequences, ISMS integrity, resources, responsibilities and timing.

Changes may include:

- a new proposal platform;
- AI or automated requirement extraction;
- acquisition or new office;
- outsourced writing;
- identity-provider migration;
- revised risk method;

- new security monitoring;
- change to certification scope;
- new customer sector;
- major corrective action.

Plan testing, communication, access, migration, fallback, competence and acceptance. Avoid introducing an untested security tool in the final week of a strategic tender unless the risk of not changing is greater and authority accepts it.

A change record for the AI platform

Pelham reconstructed the pilot as a planned change.

Purpose: reduce time spent on extraction, comparison and first-pass drafting while retaining information security and human accountability.

Scope: initially internal, non-customer-confidential material; named users; one business unit.

Risks: data retention, provider training use, unauthorised access, unsupported output, excessive input, cross-client retrieval, contractual disclosure, dependency and service availability.

Controls: enterprise agreement, provider assessment, single sign-on, multi-factor authentication, restricted tenant, retention settings, logging, approved use cases, source grounding, user competence, output verification and incident route.

Acceptance: technical and legal review complete; test data only; users pass practical exercise; logs reviewed; fallback available.

Pilot evidence: representative tasks, output defects, time saved, user behaviour, incident or near-miss records.

Decision: extend, change, restrict or stop.

The change became slower than the original announcement and faster than repairing a customer breach.

A risk workshop for a live pursuit

Use ninety minutes with the bid manager, information owner, solution, security, commercial, legal or privacy and delivery.

First twenty minutes: identify information assets, customer requirements, systems, people, suppliers and stages.

Next twenty: create risk scenarios around confidentiality, integrity and availability. Include ordinary mistakes, external threats and dependencies.

Next twenty: assess existing controls and rate risk using approved criteria. Record uncertainty.

Next twenty: choose treatment, necessary controls, owner and residual risk. Compare with relevant Annex A areas.

Final ten: identify gate impact, actions, approvals and review trigger.

Do not spend the meeting debating whether likelihood is exactly three or four while an anonymous link remains open.

Risk assessment is a decision service.

Its output should change the pursuit.

CHAPTER 7

Resources, Competence, Awareness, Communication and Records

CASE FILE

A security consultant joined the Fenwick Housing bid on Monday morning.

By 10:20 she had access to the proposal platform, customer security schedule, architecture folder and pricing assumptions. By 15:00 she had identified several good improvements. On Friday the assignment ended.

Her account remained active for eighty-three days.

The bid manager assumed IT would remove it. IT assumed the sponsor would request removal. The consultant assumed access had ended because she stopped using the link.

Everyone understood confidentiality.

Nobody owned the final click.

Clause 7.1 - Resources

The organisation determines and provides resources needed to establish, implement, maintain and continually improve the ISMS.

Resources include more than budget and headcount. They include competent people, time, infrastructure, monitoring capability, specialist advice, secure systems, workspace, tools, information, backup routes and leadership attention.

For a secure pursuit, ask:

- which roles are needed at each stage;
- when they are needed;
- whether deputies exist;
- which systems and accounts are required;
- what customer or technical information must be available;
- which suppliers are involved;
- what review and monitoring capacity exists;
- what happens if a resource fails.

A security architect available after solution freeze is not available for design. A deputy who lacks portal access is not a deputy. An approved file-transfer service nobody can use under deadline is not an effective resource.

People and capacity are security controls

Overload changes behaviour.

People reuse passwords, download local copies, approve without reading, share broad links and postpone access removal when the process has more work than capacity. Fatigue does not remove competence. It reduces the ability to apply it safely.

Resource planning should consider concurrent pursuits, time zones, holidays, operational duties, incident cover and critical decision dates.

Fenwick's bid plan showed the information-security manager at ten per cent allocation. The ten per cent sat on Thursday afternoon. The supplier-security review was required on Tuesday.

The resource existed on paper and failed in time.

The team moved provider identification earlier and trained a competent deputy for standard supplier reviews.

Infrastructure must support secure work

Bid infrastructure may include CRM, email, portals, document management, proposal systems, secure transfer, identity services, managed devices, VPN or zero-trust access, pricing models, AI services, backup connections, telephony and physical workspace.

Determine requirements for availability, confidentiality, integrity, support, maintenance and recovery.

Ask:

- is the platform approved for the information type;
- are access roles appropriate;
- is authentication strong enough;
- are logs available;
- are backup and recovery tested;
- can data be exported or deleted as required;
- does the supplier change terms or features without notice;
- can the team operate if the service fails;
- who owns configuration and support.

A secure cloud does not compensate for an open sharing link. A managed laptop does not compensate for sending the file to a personal account.

Infrastructure and user process meet at configuration.

Clause 7.2 - Competence

The organisation determines the competence required for people doing work under its control that affects information-security performance. It ensures competence through appropriate education, training or experience, takes action where needed and retains evidence.

Competence is the ability to apply knowledge and skill to the actual work.

A bid manager may need competence in:

- information classification and handling;
- secure workspace and access management;
- customer security requirements;
- risk and incident escalation;
- supplier and guest control;
- release and retention;
- APMP-aligned pursuit management under security constraints.

A writer needs to recognise personal data, security-sensitive content, unsupported assurance claims, permitted AI use, source limitations and hidden disclosure.

A technical reviewer needs current architecture and threat knowledge, not only proposal experience.

An uploader needs portal competence, file integrity, manifest and evidence handling.

A risk owner needs enough understanding to accept residual risk deliberately.

Training attendance is not competence

Fenwick required every bidder to complete an annual information-security course. Completion was 100 per cent. The external-access failure still happened because the training did not explain who requested removal, which system record proved it or how guest expiry worked.

Actions to build competence may include:

- practical training;
- supervised live work;
- simulations;
- coaching;
- professional qualifications;
- observed assessment;
- role authorisation;
- external specialist support;
- changed responsibility where a gap remains.

Evaluate effectiveness.

Ask a bid manager to set up a secure workspace from a scenario. Ask a writer to classify five information examples. Ask a reviewer to identify an unsupported security claim. Ask an incident lead to run a mistaken-recipient exercise.

The certificate of attendance is evidence that a person attended.

It does not prove the intended capability.

Clause 7.3 - Awareness

People doing work under the organisation's control need awareness of the information-security policy, their contribution to ISMS effectiveness and the implications of not conforming.

Make awareness local.

The bid manager should know why anonymous links create risk. The sales director should know that customer insight may have handling restrictions. The writer should know that a fabricated control claim can become contractual debt. The external reviewer should know where local copies may be stored and when they must be removed. The chief executive should know that forwarding a commercial model to personal email is an exception, not a convenience.

People also need awareness of event reporting. They should recognise and report suspicious sign-ins, wrong recipients, lost devices, unexpected access, malware, disclosure, integrity errors and unusual supplier behaviour.

A poster saying 'security is everyone's responsibility' does not state what anyone should do at 17:42.

Awareness has to survive the deadline

Use live bid kick-offs, short role briefings, prompts in workflows, near-miss discussions and leadership behaviour.

At Fenwick, every Enhanced bid began with a five-minute handling brief:

- information classification and customer restrictions;
- approved workspace and transfer routes;
- external participants and expiry;
- prohibited tools or data uses;
- event reporting;
- final release and closure.

The brief did not repeat the entire policy. It translated it for the pursuit.

When a customer clarification introduced personal data, the brief was updated. Awareness followed change.

Clause 7.4 - Communication

The organisation determines internal and external communications relevant to the ISMS: what, when, with whom, how and by whom.

Secure bidding needs communication control because a message can change risk, requirements or commitments.

Relevant communications include:

- customer security requirements and clarifications;
- classification and handling instructions;
- access approvals and removal;
- risk decisions and treatment actions;
- supplier requirements;
- security incidents and near misses;
- design and evidence approvals;
- review findings;
- release status;
- post-submission questions;
- handover and closure;
- audit and corrective action.

Do not let material decisions exist only in chat messages. Summarise them into the controlled record.

Customer communication needs authority

During a live procurement, follow the customer's stated route. An account director should not privately ask a friendly contact to interpret a security requirement. A technical expert should not answer a clarification directly because the question appears simple.

Define who may communicate, what approvals are required and where the record remains.

A short statement can change liability.

When a buyer asked whether all subcontractors were ISO/IEC 27001 certified, a delivery manager drafted 'yes' because the principal cloud providers were. One specialist subcontractor was not certified. The controlled communication route stopped the reply. The final answer described certification, contractual controls, due diligence and the exact boundary accurately.

Two letters had nearly created a false declaration.

Incident communication is not ordinary update

Incident plans should define internal escalation, leadership, legal or regulatory assessment, customer notification, law-enforcement or authority contact where relevant, supplier coordination and media handling.

Do not assume every security event becomes a reportable personal-data breach or contractual incident. Competent assessment decides. Do not delay reporting internally until certainty exists.

Time matters. Some contracts impose short notification periods. The organisation needs decision authority and contact information before an event.

A secure-pursuit charter can identify the opportunity-specific customer notification route and contractual deadline.

Clause 7.5.1 - Required and necessary documented information

The ISMS includes documented information required by the standard and information the organisation determines necessary for effectiveness.

For bid-related security, this may include:

- scope and policy;
- risk-assessment and treatment methods;
- risk results and treatment plans;
- Statement of Applicability;
- objectives;
- competence evidence;
- operational process and work instructions;
- asset and information records;
- access approvals and reviews;
- supplier assessments;
- incidents;
- monitoring and audit;
- management review;
- nonconformity and corrective action;
- controlled pursuit records.

Do not create records because a consultant has a template. Create enough information to operate, decide and demonstrate.

Clause 7.5.2 - Create and update information properly

When documented information is created or updated, ensure appropriate identification, format, review and approval.

In bid work, identification may include customer, opportunity, lot, information owner, classification, version, status and date.

Format should support use. A risk register in a locked spreadsheet with invisible columns may be controlled and unusable. A policy in a workflow may be effective if people can access and understand it.

Review and approval should match consequence.

An information-security policy needs top-management approval. A standard access-role template may need system and information-owner approval. A specific guest-access request needs the authorised decision defined by process.

'Approved' should refer to an identifiable version.

Clause 7.5.3 - Control documented information

Control availability, suitability, distribution, access, retrieval, use, storage, preservation, change, retention and disposal as needed. Protect information from loss of confidentiality, improper use or loss of integrity. Control relevant externally originated information.

This clause reaches the bid room directly.

Customer tender files are externally originated information. So are standards, supplier certificates, penetration-test reports, partner evidence, legal guidance and portal instructions.

Control:

- authoritative source;
- access and permissions;
- superseded status;
- version and change;
- secure storage and transfer;
- backup and recovery;
- retention and disposal;
- printing and physical copies;
- final archive;
- customer or legal holds.

A central folder is not automatically controlled. Fenwick's evidence library contained three security certificates called current. Two had expired. One covered another legal entity.

Centralisation had made the wrong evidence easier to find.

Retention should have a reason

Define retention based on customer terms, contract, law, limitation, certification, learning, dispute and business need. Apply data-minimisation and storage-limitation principles where personal data is involved.

Different records may have different periods.

The submitted baseline may need long retention. Unsuccessful working drafts may not. CVs may need redaction or deletion. Supplier due diligence may have a defined review cycle. Incident evidence may be subject to legal hold. AI logs may contain customer content and need specific treatment.

'Keep everything forever' is not safe preservation. It is unresolved risk with storage.

The joiner, mover and leaver process for bids

External and temporary pursuit participants need the same discipline as employees, adapted to their role.

Joiner: verify identity and contract, define role, classification, systems, access, expiry, confidentiality, device and handling requirements. Provide a practical briefing.

Mover: review access when role, lot, customer, sensitivity or employment changes. Remove old rights before assuming new ones are sufficient.

Leaver: revoke access, recover assets, confirm information return or disposal, preserve necessary records and assess unusual activity.

Use triggers beyond employment termination: submission, result, project end, inactivity, supplier change and customer instruction.

Fenwick configured guest expiry and a weekly owner report. Accounts did not vanish automatically where post-bid work remained. They became visible and required justification.

The consultant's next account closed on the planned date.

Nobody had to remember the final click.

A support-control audit

Choose one person, one system, one supplier and one record from a live pursuit.

For the person: what competence and awareness are required, and what evidence supports them?

For the system: what information may it process, who owns configuration, how is access controlled and what happens on failure?

For the supplier: what requirements were communicated, how was assurance obtained and when is access or service reviewed?

For the record: which version is authoritative, who approved it, who can access it, how long is it retained and how will it be disposed of?

If the answers are split across five people who assume the others have them, the support system needs work.

Security becomes real when ordinary people can perform ordinary controls without a translator.

CHAPTER 8

Opportunity Identification and Security Qualification

CASE FILE

The opportunity appeared in Kestrel Health's CRM at 07:28.

By 07:44 it was marked Must Win. The contract involved a national patient-support platform, sensitive personal data, twenty-four-hour service, offshore development restrictions and a requirement for security-cleared support staff.

Kestrel had an ISO/IEC 27001 certificate.

Its certificate covered the corporate network and one hosted product. The proposed service used a newly acquired platform outside the certified scope. Nobody had yet asked.

The opportunity was not being qualified. It was being comforted by a logo.

Security begins in the pipeline

Opportunity information may arrive through portals, framework alerts, account teams, market engagement, partners, consultants or automated services. Record the source, date, customer, route, likely information types, timing, value and owner.

Do not copy a framework ceiling into forecast revenue. Do not copy a buyer's statement that ISO/IEC 27001 is required into a conclusion that the organisation qualifies. The certificate scope, offered service and procurement wording still need review.

A secure opportunity record should identify early signals:

- information sensitivity and likely data types;
- buyer security, privacy and assurance expectations;
- certification, clearance or accreditation conditions;
- hosting, location and sovereignty requirements;
- critical suppliers and subcontractors;
- secure-development or technical-testing requirements;
- incident, continuity and recovery obligations;
- access to buyer systems or sites;
- likely audit, transparency and evidence demands;
- unusual contractual liability or notification periods.

At this stage, some information will be uncertain. Mark it.

Triage before the team downloads everything

Triage is a short check for conditions that can end or reshape the pursuit. It should occur before broad access and content production.

Within the first working hour, where practical, check:

- deadline, clarification date, procedure and lot;

- portal and file completeness;
- mandatory certificate and scope requirements;
- security clearance or personnel restrictions;
- data type, location and transfer conditions;
- prohibited suppliers, countries or technologies;
- cyber-insurance and financial thresholds;
- critical incident and continuity obligations;
- required security questionnaires or schedules;
- access to buyer systems, code, sites or sensitive data;
- obvious conflicts, exclusions or sanctions concerns;
- whether the information can be handled in current approved systems.

Triage does not replace the full gate. It finds the conditions that should influence the gate before thirty people receive the files.

Kestrel's triage identified that the certificate scope did not cover the proposed platform. That was not automatically fatal. The tender required the bidder to operate an ISMS covering the service by contract start, with certification evidence evaluated separately. The gap became a condition requiring legal, security and certification-body review.

The opportunity remained possible. It was no longer comfortably green.

Qualification dimensions

A security-aware gate should keep dimensions separate.

Strategic fit: Does the opportunity support the organisation's chosen services, sectors and security capability?

Customer and route: What is known about the buyer's risk, assurance process and permitted communication?

Mandatory requirements: Can certificate scope, clearance, data location, regulatory, technical and contract conditions be met?

Information handling: Can the bid and later service process the information lawfully and securely through approved systems?

Solution and evidence: Is there a credible security design and current proof?

Suppliers: Which external parties are essential, and can their security, capacity and terms be controlled?

Commercial case: Are security people, tools, testing, insurance, audits, incident cover and continuity priced?

Capacity and timing: Can the organisation close security gaps before the relevant commitment, not eventually?

Risk and ethics: Are residual information, customer, legal, safety and reputational risks acceptable?

Use minimum thresholds. A high overall score cannot average away a failed clearance condition or an impossible hosting location.

Evidence beside the score

'ISO position: strong' is not evidence.

A gate record might state:

WORKING WORDS

Current ISO/IEC 27001:2022 certificate held by Kestrel Health Ltd. Scope covers corporate IT and the Meridian platform from the Leeds site. Proposed service uses the acquired Helix platform, currently outside certificate scope. Certification body has confirmed that extension assessment is possible but not scheduled. Tender requires evidence of ISMS operation covering the service by mobilisation and awards separate marks for current accredited certification. Condition: obtain written interpretation through clarification and approved scope-extension plan by Gate 2.

That statement can be challenged and updated.

A green cell cannot.

Certification is one control signal

A current accredited certificate can reduce uncertainty. It does not answer every security question.

At qualification, examine:

- exact legal entity and scope;
- relevant sites and services;
- standard edition and amendment;
- certification body and accreditation;
- dates and status;
- current Statement of Applicability reference if available;
- changes since the last audit;
- known major incidents or nonconformities affecting the offer;
- customer-specific requirements beyond the certificate.

A certificate may be mandatory, scored or simply requested as evidence. Treat the wording accurately.

Do not promise certification by award date because a consultant believes it is achievable. Speak to suitable certification bodies, understand readiness and obtain authority.

Security due diligence on the customer requirement

Some tenders contain security requirements copied from another service, internally inconsistent schedules or controls disproportionate to the data involved. Suppliers may clarify through the formal route.

Challenge with evidence and respect.

A requirement for all staff to hold a high-level clearance may conflict with a service that never accesses classified information. A blanket prohibition on all cloud services may conflict with the specification's named cloud platform. A four-hour incident notification may need definition of the triggering event and reporting route.

Do not assume the buyer will change. Assess the requirement as written until clarified.

Do not privately ask a friendly contact for the answer.

Data protection and information security are connected, not identical

An opportunity involving personal data requires data-protection analysis alongside information security. Determine roles, purposes, data categories, data subjects, legal basis, processors, transfers, retention, individual rights, security and potential need for a data-protection impact assessment.

ISO/IEC 27001 can support security and accountability. It does not by itself establish lawful processing.

The gate should identify competent privacy input early. The bid writer should not answer a controller-processor question by copying the security policy.

Kestrel's proposed patient platform handled health information. The privacy lead identified that one analytics feature would use data for a purpose not required by the tender. The feature was removed from the base offer. Security had not failed. Product enthusiasm had crossed purpose.

Security capacity is time-specific

The organisation may possess the expertise to meet a requirement and still lack it during the pursuit or mobilisation.

Assess:

- security architecture and engineering time;
- privacy and legal review;
- supplier due diligence;
- penetration testing or independent assurance;
- evidence preparation;
- clearance lead times;
- incident-response coverage;
- implementation and monitoring capacity;
- certification or audit scheduling.

Kestrel's security architect had thirty available hours during the month. Twenty-eight were after solution freeze. The gate needed ten hours in the next four days.

External support was approved. The opportunity class moved from Standard to Strategic because the service and evidence were novel.

Capacity became a control decision, not a monthly average.

Security risk should change the pursuit route

Use opportunity classes or control levels.

A Standard pursuit may involve familiar information, existing approved services, low supplier novelty and ordinary contractual terms. Core controls may be enough.

An Enhanced pursuit may include personal data, new suppliers, significant security schedules, remote access to customer systems or important certification questions. Add specialist reviews, deeper risk assessment and stronger evidence.

A Strategic pursuit may involve critical services, sensitive or regulated data, novel architecture, high liability, national scale, many suppliers or severe customer consequence. Add independent assurance, leadership risk hearings, simulations, formal design baselines and mobilisation validation.

Risk should select the route. Headline value should not.

Conditional bid is a real decision

A gate may approve the pursuit subject to conditions:

- certificate-scope interpretation confirmed;
- named cloud provider passes due diligence;
- security architect available by a stated date;
- data-location requirement resolved;
- required assurance test scheduled;
- contract incident clause accepted or departed;
- partner signs security obligations;
- residual risk accepted by authority.

Record action, owner, due date, evidence and consequence if unmet.

'Proceed subject to security' is not a decision. It is a future argument.

Requalify after material change

Security position changes during a pursuit.

Re-gate when:

- a clarification changes data, scope or control;
- a supplier withdraws or fails due diligence;
- architecture changes;
- certification timing moves;
- legal or privacy review identifies new exposure;
- a security test fails;
- required evidence is unavailable;
- cost or capacity exceeds approved limits;
- an incident affects the proposed service;
- leadership proposes a new commitment.

Sunk cost does not reduce security risk.

Kestrel had spent 610 hours when the preferred hosting provider could not meet the stated UK-only support requirement. The team considered another provider, a modified support model and a formal clarification. The alternatives changed price and timetable. Leadership requalified the opportunity rather than hiding the issue behind existing effort.

The bid continued with a different architecture and a smaller margin.

At least the margin belonged to a service that could be delivered.

No-bid is a security output

Reasons may include:

- mandatory certification or clearance cannot be met;
- information cannot be handled through an approved route;
- customer requirements conflict with law or organisational policy;
- a critical supplier cannot be controlled;
- security design is not feasible in time;
- evidence would require overstatement;
- incident or continuity obligations exceed capability;
- residual risk exceeds appetite;
- security cost destroys the commercial case;

• the pursuit displaces a stronger, safer opportunity.

Record the reason in a taxonomy that can be analysed.

'No-bid: security' teaches little.

'No-bid: mandatory privileged-support clearance lead time exceeds mobilisation by fourteen weeks and no compliant partner route exists' can influence future capability and market engagement.

The security gate pack

For an Enhanced or Strategic opportunity, include:

• opportunity and customer summary;
• information types and handling restrictions;
• mandatory security and privacy requirements;
• certificate and assurance position;
• architecture and supplier assumptions;
• major risk scenarios;
• resource and competence;
• commercial impact;
• conditions and unknowns;
• recommendation and authority required.

Keep it decision-ready. Leadership does not need every line of the security schedule to decide whether the organisation can pursue it. It does need the red condition that could stop the service.

A Friday qualification drill

Choose the three largest opportunities in the pipeline. Hide the published values.

For each, write:

• the strongest security reason to pursue;
• the most dangerous information unknown;
• the certificate or assurance boundary;
• the critical supplier dependency;
• the scarce security resource;
• the risk that triggers no-bid;
• the next re-gate event.

Invite delivery, security, privacy and finance to challenge the answers.

Kestrel did this at 15:30. One opportunity became stronger. One moved to conditional. One left the pipeline because the proposed subcontract chain could not meet the buyer's incident and data-location terms.

On Monday, the team had time to work on the bids it could secure and deliver.

CHAPTER 9

Capture, Customer Insight and Information Boundaries

CASE FILE

Bramley Networks had a detailed capture plan for a local-government connectivity framework.

It contained names, job titles, public comments, inferred preferences, screenshots from social media and a note saying one evaluator was 'anti-incumbent'. The source was an account manager who had heard it from somebody at an event.

The plan was commercially energetic.

It was also an information-governance problem and a weak strategy.

Capture is lawful understanding, not private access

Capture improves the organisation's position before and during a competition through customer understanding, market research, competitive analysis, solution shaping, partner decisions, evidence and strategy.

Information security adds boundaries.

Use public sources, authorised customer engagement, existing delivery knowledge, properly governed account records, market data, published plans and permissioned partner information. Respect procurement fairness, confidentiality, privacy, contractual restrictions and the organisation's own policies.

The objective is relevant understanding.

It is not collection for its own sake.

Build a source and handling hierarchy

Classify material insight by reliability and handling.

Authoritative: formal customer document, clarification, published policy, contract, official plan or direct recorded response through a permitted route.

Strong: approved engagement record, verified performance report, committee paper, annual report, public award information or current operational evidence.

Indicative: professional opinion, partner experience, historic pattern or public commentary that may support a hypothesis.

Speculative: rumour, assumed budget, unsupported incumbent story, private preference or memory without source.

Then add handling:

- public;
- internal;
- customer-confidential;

- partner-restricted;
- personal data;
- security-sensitive;
- another organisation-specific category.

Reliability and sensitivity are different. A public rumour can be unreliable. A verified customer conversation can be confidential.

Bramley removed several personal notes, retained job-relevant public information and marked unsupported opinions as hypotheses. The plan became shorter and safer.

It also became more honest.

Data minimisation belongs in capture

Collect and retain what is necessary for a defined purpose.

A stakeholder map may need role, responsibility, relevant outcome, public source, engagement status and internal owner. It rarely needs birthdays, family information, personal interests or unrelated social-media detail.

The fact that a sales platform can collect something does not make the collection useful or lawful.

For personal data, consider purpose, legal basis, transparency, accuracy, access, retention and rights. Involve competent privacy advisers where required.

A capture record should be capable of being shown to a reasonable person without the team wishing the screen would go dark.

Customer requirements, underlying need and security hypothesis

Separate:

- formal requirement;
- underlying operational or public need;
- evidence the buyer can evaluate;
- supplier security hypothesis.

A buyer may formally require encryption at rest and in transit. The underlying need may include protection of vulnerable-user information and contractual assurance. The evaluation may ask for key management, access, testing and incident evidence. The supplier hypothesis may be a managed service with customer-controlled keys and tested recovery.

The hypothesis remains a hypothesis until architecture, price and evidence support it.

Do not use capture insight to rewrite the question.

Threat intelligence can inform capture

Information about current and emerging threats may affect opportunity risk and solution design. Use reputable, relevant and current sources. Consider sector alerts, customer environment, supplier advisories, vulnerability information and internal incidents.

Do not turn generic threat reports into theatre.

A public-sector buyer procuring remote-access services may care about credential theft, supply-chain compromise and administrative access. The capture team can prepare evidence and controls accordingly. It should not claim knowledge of a secret attack unless that information was lawfully obtained and permitted for use.

Threat intelligence is useful when it changes design, risk, evidence or prioritisation.

'Cybercrime is rising' does not differentiate a bid.

Stakeholder mapping with restraint

Map professional roles involved in need, procurement, information ownership, technical assurance, privacy, legal, finance, use and delivery.

For each role, ask:

- what outcome or risk they are responsible for;
- which published requirement connects to that responsibility;
- what evidence would reduce reasonable doubt;
- how engagement is permitted;
- what information must not be assumed;
- what handling restrictions apply to the record.

Do not claim that every mapped person will evaluate. The map helps design an offer that can survive the responsibilities represented in the procurement.

Bramley mapped procurement, network operations, cyber security, data protection, service desk, finance, accessibility and business continuity. It stopped trying to predict which individual would like which slide.

The strategy improved.

Competitive intelligence and security

Use lawful sources such as published contracts, certificates, case studies, recruitment, service locations, technology partnerships, public incidents, customer feedback and your own direct experience.

Security-related competitive analysis might consider:

- certification scope and public assurance;
- service architecture and hosting model;
- known supplier ecosystem;
- public security incidents and response;
- regulatory position;
- customer integration and transition burden;
- likely strengths and constraints;
- what the competitor may say about your security position.

Avoid attacking a competitor through unverified breach rumours. Do not retain personal data about their staff without purpose.

A black-hat review should create a credible rival strategy, not a list of insults.

Bramley's review concluded that the incumbent would sell continuity, existing network knowledge and lower transition risk. Bramley had planned to lead with new technology. The strategy changed. It had to prove secure transition before innovation mattered.

Win themes must survive assurance

A security win theme is an important, distinctive, defensible and deliverable reason the buyer can prefer the offer.

Test:

Importance: Does it address a material requirement, risk or outcome?
Difference: Is it meaningfully different from credible competitors?
Proof: Is evidence current, relevant, permissioned and within scope?

Delivery: Are people, technology, suppliers and cost available?
Traceability: Where will the evaluator see and score it?

'Bank-grade security' fails.

'Named UK-based incident leads, customer-tested escalation, immutable audit evidence and a rehearsed recovery path achieving the stated four-hour restoration target across three comparable services' is closer. It still needs exact proof and careful wording.

Avoid too many themes. Three strong arguments can shape the pursuit. Twelve security slogans create fog.

Capture information needs owners and expiry

Insight changes. People move. contracts end. Threats evolve. Public plans are revised.

For material information, record:

- source and date;
- owner;
- confidence;
- handling classification;
- intended use;
- review or expiry;
- affected decision;
- contradiction or superseded status.

A customer architecture diagram obtained during an earlier contract may remain confidential and no longer reflect the environment. It should not become a permanent capture asset because the folder is convenient.

Secure engagement before and during procurement

Before a live procurement, published market engagement and legitimate account activity can help the organisation understand needs and feasibility. Keep records, provide accurate information and respect confidentiality.

During a live procurement, use the formal channel unless documents permit another route. Do not ask an employee of the customer to privately explain a security schedule. Do not send a draft architecture to obtain unofficial approval.

If a customer provides information outside the expected route, record it and obtain guidance where necessary. Fairness and information security may both be involved.

A relationship is not authority to bypass process.

Capture actions need control

Useful actions may include:

- confirm a hosting or data-location condition through published engagement;
- obtain permission for a security case study;
- test a secure integration concept;
- reserve a cleared specialist;
- conduct supplier due diligence;
- close a certification-scope gap;
- develop missing incident metrics;
- model transition and data migration;

- validate a threat assumption;
- brief leadership before tender release.

Record owner, due date, expected output, information handling and gate effect.

'Improve cyber relationship' cannot be completed.

'Attend the published technical briefing on 12 September and confirm whether privileged support must be performed solely by customer-cleared UK personnel' can.

Concept, baseline and approved offer

Capture teams develop solution ideas before formal requirements are complete. Mark maturity.

Concept: possible approach requiring validation.

Baseline: agreed basis for response planning, with assumptions and open issues.

Approved offer: designed, costed, assessed, evidenced and authorised.

The label protects integrity.

Bramley had a February slide showing customer-managed encryption keys. The design was a concept. By June, the commercial model and provider contract did not support it. Without status, the diagram would have returned in the final answer as an approved commitment.

It remained in the capture archive, clearly superseded.

Capture review points

Run reviews for decisions.

Early position review: Is the customer need and security environment understood enough to justify continued investment?

Security strategy review: Are the risk position, control themes, suppliers, evidence and differentiators credible?

Pre-solicitation readiness: Are resources, approved tools, information boundaries, assurance evidence and first-forty-eight-hour actions ready?

Post-solicitation reset: What changed when formal requirements arrived?

The last review matters. Teams fall in love with capture assumptions and force the tender to fit them.

Bramley expected a heavy weighting on technical security. The actual tender placed more marks on mobilisation and customer support. The secure-transition theme became central. A planned zero-trust architecture appendix became supporting evidence rather than the story.

The capture plan bent when the buyer spoke formally.

Capture audit

Select one material insight and trace it.

Where did it come from? Is it fact, inference or unknown? What is its handling classification? Why is it retained? Which decision changed? Where is it reflected in qualification, risk, design, price or evidence? Has later information contradicted it? Who can access it? When will it be reviewed or removed?

If the chain breaks, fix the information before polishing the strategy.

Bramley's original plan said the buyer had lost confidence in the incumbent after a security incident. The incident was public. The claimed loss of confidence was not. The team removed the statement.

What remained was enough: the buyer required secure transition, stronger event visibility and demonstrable supplier control.

A serious bid did not need the rumour.

CHAPTER 10

Tender Intake, Classification and the Secure Bid Room

CASE FILE

At 08:52, Greyfell Engineering downloaded the tender pack.

There were thirty-six files. The business-development manager saved twenty to his desktop, forwarded six to the bid team, uploaded eight to a shared drive and left two inside the portal because he did not recognise the format.

At 09:31 the information-security lead asked where the authoritative customer documents were.

Four people sent links.

The bid had been open for thirty-nine minutes. Integrity had already become a group opinion.

Receipt is a controlled event

Treat a solicitation as an important information input. Preserve the native files, portal messages, dates, customer route and original metadata before people create working copies.

The intake record should identify:

- opportunity and lot;
- customer and portal;
- authorised accounts;
- issue, clarification and submission dates;
- document list and version;
- amendments and notices;
- source storage and working storage;
- owner;
- initial classification and restrictions;
- personal, confidential or security-sensitive information;
- access population;
- integrity checks where proportionate;
- first security and qualification actions.

Do not convert everything immediately. Spreadsheets, signatures, hidden instructions, macros and metadata may matter. Preserve the originals in read-only form.

Greyfell created 00_Source with restricted write access. Working copies lived in controlled workstreams. When the buyer replaced a security schedule, the old file remained available as superseded evidence. Nobody had to remember which attachment came from which email.

Establish the authoritative baseline

A baseline is the defined set of customer documents and instructions against which the team is working at a stated point.

It may include the notice, invitation, evaluation method, specifications, security schedules, contract, data-processing terms, pricing files, appendices, policies, clarification responses and portal guidance.

Name the baseline. Date it. Record changes.

The baseline does not freeze the buyer's process. It gives change somewhere to start.

For higher-risk bids, consider checksums or another integrity method for native source files and released outputs. The purpose is not technical decoration. It is confidence that the file reviewed is the file used.

Classify before sharing

Information classification helps people understand value, sensitivity, handling and access.

Use the organisation's approved scheme. Avoid inventing a new set of colours for each bid.

A simple internal model may distinguish:

- public;
- internal;
- confidential;
- highly restricted.

Customer markings may use different terms. Map rather than overwrite them. Contractual handling rules outrank internal convenience.

Classification should consider:

- customer designation;
- personal data;
- commercial sensitivity;
- security architecture or vulnerability detail;
- legal privilege;
- intellectual property;
- impact of disclosure, alteration or loss;
- retention and transfer requirements.

Do not mark everything at the highest level. Overclassification makes the system unusable and encourages bypass. Underclassification exposes information.

Build the secure bid room around roles

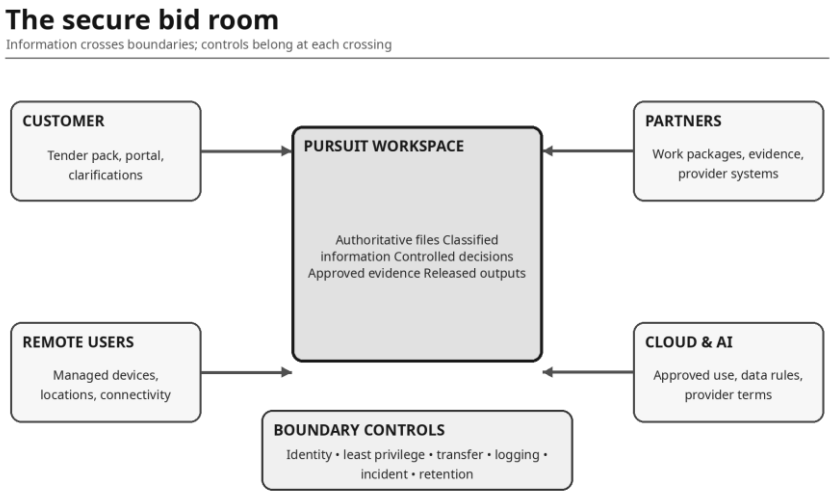

Figure 4 - A five-zone secure bid workspace, separating source, working, restricted, external and released information.

The working environment should support the pursuit while limiting access to business need.

Design groups or roles such as:

- core bid team;
- solution and technical;
- commercial and finance;
- legal and privacy;
- external reviewers;
- partner-specific workspaces;
- production and release;
- read-only leadership;
- audit or assurance access.

Do not grant access one person at a time without a model when the platform supports roles. Define who approves membership, who administers it, default expiry and review triggers.

External participants should receive only the information required for their work. A writer working on mobilisation does not automatically need competitor analysis, full pricing and employee vetting records.

Need-to-know is not mistrust. It is controlled design.

Segregate customer and opportunity information

Prevent accidental cross-client access and reuse.

Use separate workspaces or clearly controlled boundaries. Avoid shared folders where one search can reveal another customer's tender pack. Configure AI retrieval and knowledge systems so content does not cross matters without authorisation.

Greyfell's proposal platform used one global evidence library and separate opportunity spaces. Customer source files remained within each opportunity. Approved reusable evidence was linked from the library. Customer-specific content could not be promoted without owner review and permission.

The library became useful without becoming a mixing bowl.

Identity and authentication in the bid room

Use named accounts. Avoid shared credentials. Apply authentication proportionate to risk, including multi-factor authentication where required by policy and platform capability.

Verify external identities through a trusted route. A message appearing to come from a partner is not enough when the invitation grants access to sensitive information.

Control privileged roles. Workspace owners can often invite users, alter retention, export content and delete evidence. Grant those rights deliberately and review them.

A bid manager may administer ordinary membership while the system owner controls platform administration. The distinction protects both the system and the bid manager.

Access lifecycle

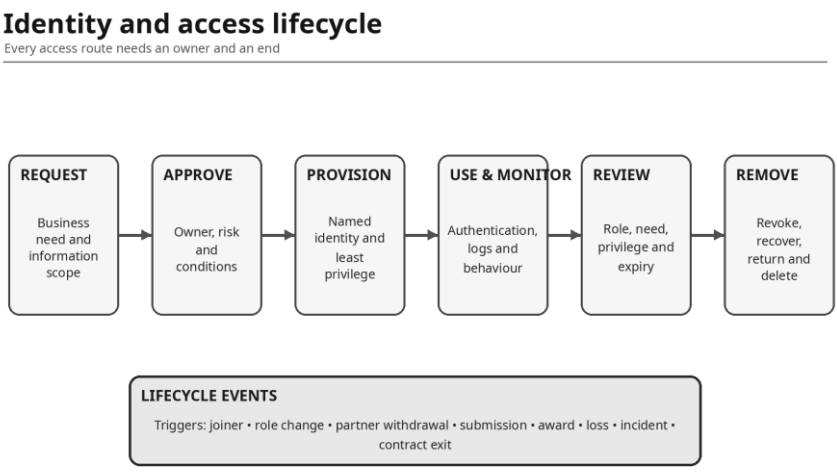

Figure 5 - The joiner, mover, reviewer and leaver lifecycle for pursuit access.

Request: identify person, role, information, duration, device or location conditions and sponsor.
Approve: authorised owner confirms business need and handling conditions.
Provision: administrator grants the minimum role and records it.
Use: activity is monitored where appropriate; people report anomalies.
Review: at planned intervals and events such as role change, submission, delay, result or inactivity.
Remove: revoke promptly, recover assets, confirm local copy treatment and retain necessary evidence.

Guest access without an owner or expiry is delayed disclosure.

Personal data in bids

CVs, contact details, employment history, qualifications, vetting status, signatures and diversity information may be personal data. Collect only what the tender and lawful purpose require. Use redaction or tailored profiles where possible.

Do not place full identity documents or unnecessary home details into general bid folders. Restrict access and retention. Confirm customer instructions and transparency to staff.

A buyer asking for named personnel does not automatically require every field in the HR system.

Greyfell replaced full CVs with controlled bid profiles containing relevant experience, qualifications and role. HR retained the authoritative record. The bid team no longer copied passport scans into the proposal workspace because one security schedule mentioned identity verification.

Local copies, printing and offline work

People download files to work quickly. The ISMS should define when local storage is permitted, which devices are approved, encryption, backup, synchronisation, secure deletion and travel rules.

Printing may be necessary for review or site work. Control printers, collection, storage, clear desks, transport and disposal. Record particularly sensitive copies where risk justifies it.

'No local copies' may be appropriate for some information and impractical for other work. Design a route people can follow.

When a reviewer needed to work on a train, Greyfell provided an encrypted managed device with offline synchronisation and automatic return to the controlled workspace. Emailing the pack to personal storage was no longer the easiest route.

Approved transfer routes

Define methods for internal, customer and supplier transfer. Consider encryption, recipient verification, link expiry, download restrictions, authentication, logging and file size.

Email may be suitable for some information. It may be prohibited or weak for sensitive content. A secure portal may be appropriate but unavailable to one partner. The solution is not to improvise silently.

Use an exception route with compensating controls.

Before sending, verify recipient, address, attachment, classification and authority. Autocomplete has no knowledge of confidentiality.

A two-person check may be proportionate for highly sensitive customer data or final commercial submissions.

Supplier and tool onboarding

Before a new external service processes bid information, assess:

- business purpose and data types;
- provider identity and ownership;
- security assurance and certifications;
- access and authentication;
- data location and subprocessors;
- retention, deletion and training use;

- encryption and key management;
- logging, monitoring and incident notification;
- backup, continuity and exit;
- contract, confidentiality and data protection;
- customer restrictions;
- integration and configuration;
- human review and accountability.

Do not wait until after upload because the tool is only being tested.

The bid-room operating rules

For each pursuit, make essential rules visible:

- authoritative source and baseline;
- classification and handling;
- approved systems;
- access owner and expiry;
- customer communication route;
- supplier and AI restrictions;
- file naming and status;
- change and approval;
- incident reporting;
- release, archive and disposal.

Keep the list short. Link to fuller policy.

The rules should be read at kick-off and updated when the information changes.

Availability and recovery

A secure bid room must be available when the process needs it.

Plan for:

- platform outage;
- internet failure;
- identity-service failure;
- unavailable administrator;
- corrupt file;
- accidental deletion;
- ransomware or malware;
- customer portal failure;
- office or climate disruption;
- supplier outage.

Define backups, recovery, alternative communication, authorised deputies and tested procedures. Be careful that the fallback does not remove security entirely.

A personal email account is not a business-continuity plan.

Greyfell exported an encrypted controlled contingency pack at defined milestones for Strategic bids. Access was restricted and the pack was verified. When the collaboration platform failed for two hours, work continued on approved priority files and reconciled back after recovery.

The fallback had been designed before the outage.

Malware, macros and unusual files

Tender packs and partner inputs can contain macros, compressed archives, executable content or unfamiliar formats. Use approved scanning and safe handling. Do not disable security controls because the pricing workbook requires macros without competent assessment.

Preserve the native file, scan it, open through the approved environment and confirm integrity. Escalate suspicious content.

The customer may legitimately provide a complex workbook. The control should enable use without exposing the wider environment unnecessarily.

The first forty-eight hours

Hour 0-2: preserve the pack, establish baseline, confirm portal, dates, completeness, classification and initial access.

Hour 2-6: conduct triage, identify fatal security conditions, personal data, unusual files, supplier restrictions and immediate clarification needs.

Hour 6-12: update qualification, begin requirements and contract review, establish the secure workspace and grant role-based access.

Day 2 morning: hold kick-off covering customer outcomes, security requirements, handling, roles, systems, risks, incident route and schedule.

Day 2 afternoon: baseline the compliance matrix, security workstreams, risk actions, supplier reviews, evidence requests, assurance points and release route.

Do not spend day one designing a security-themed cover page.

Audit the bid room

Select one external user and one sensitive file.

For the user: who requested access, who approved, which role was granted, when was it reviewed and when will it end?

For the file: where did it come from, which classification applies, who can alter it, what is authoritative, where has it been transferred, how is integrity checked and how long will it remain?

Greyfell's audit found that the secure workspace was configured well. The partner had downloaded a copy to an unmanaged laptop before the new rules were briefed.

The response was not another access restriction. The team improved onboarding, required managed access for that data class and confirmed deletion of the copy.

The bid room became secure when the process reached beyond the folder permissions.

CHAPTER 11

Information Security Risk Assessment, Treatment and the Statement of Applicability

CASE FILE

At 15:06, the security lead opened the risk register for the pursuit.

There were thirty-eight risks. Every one was amber.

The first said Data breach. The treatment said Follow company policy. The owner was Bid team. The review date was the submission deadline.

Nobody could explain whether the risk concerned the authority's tender pack, staff CVs, the pricing model, the proposed cloud service or the personal mobile phone being used by the consortium lead.

The register contained security language. It did not yet contain a security decision.

Clause 6.1.2 is a method requirement

ISO/IEC 27001 requires the organisation to define and apply an information security risk-assessment process. The process must establish and maintain risk criteria, produce consistent and comparable results, identify risks associated with loss of confidentiality, integrity and availability, identify risk owners, analyse consequences and likelihood, determine levels of risk and evaluate them against the criteria.

That does not prescribe one scoring formula.

A small consultancy may use a five-by-five matrix with clear definitions. A larger supplier may use several methods for enterprise, project, privacy, technical and supplier risk, provided they connect coherently and produce results the organisation can understand and repeat.

The important point is that the method exists before the meeting becomes anxious.

Set the criteria before rating the opportunity

Risk criteria should define at least:

- impact dimensions;
- likelihood or frequency scale;
- method for combining them;
- thresholds for acceptance and escalation;
- who may own and accept risk;
- when reassessment is required;
- how uncertainty is handled;
- how legal, contractual and customer requirements affect tolerance.

Impact in bid work is not only financial. Consider:

- unauthorised disclosure of customer information;
- corruption of price, solution or submitted files;
- inability to meet a deadline or continue a critical pursuit;
- loss of personal data;
- breach of procurement confidentiality;
- misrepresentation in a tender response;
- regulatory or contractual consequences;
- harm to customer trust;
- compromise of the proposed solution;
- wider organisational or national-security consequence.

A £20,000 quotation may involve sensitive employee data. A £20 million framework application may contain little more than public corporate evidence. Headline value does not determine information risk by itself.

Start with assets and activities, not threat vocabulary

The risk workshop should know what is being protected and what the pursuit is doing.

Select an information asset, supporting asset, process or activity. Examples include:

- tender documents;
- customer data room;
- personal data in CVs and references;
- solution architecture;
- commercial model;
- credentials and authentication information;
- bid workspace;
- partner exchanges;
- AI-assisted drafting;
- final submission pack;
- portal account;
- post-award promise register.

Then ask what unwanted event could occur, why it might occur, which vulnerability or condition makes it possible, and what the consequence would be.

A usable risk statement might be:

> **WORKING WORDS**
>
> Customer-confidential network diagrams may be disclosed to unauthorised external contributors because the collaboration workspace uses broad inherited access and guest reviews are not time-limited, leading to breach of tender conditions, loss of customer confidence and possible legal or contractual action.

The statement has edges. It can be challenged. It points towards control.

Data breach - follow policy cannot do any of those things.

Threat, vulnerability and consequence

Teams often mix the terms and then argue about the score.

A threat is a possible cause of an unwanted incident: malicious outsider, careless insider, supplier compromise, malware, fire, flood, equipment failure or deliberate fraud.

A vulnerability is a weakness or condition that can be exploited or allow the event: excessive access, unsupported software, poor authentication, unmanaged device, unclear instruction, missing backup, untrained user or an unreviewed transfer route.

A consequence is what happens to the organisation, customer or other party: disclosure, corruption, delay, financial loss, service interruption, regulatory exposure or loss of trust.

Not every organisation needs separate database fields for all three. The assessment must still make the causal logic clear enough to choose treatment.

Existing controls must be real

Assess risk with the current controls in view. Do not credit a control because a policy mentions it.

If the workspace is described as role-based, inspect the role groups. If backups reduce availability risk, identify the backup, frequency, restoration test and recovery time. If supplier confidentiality terms are relied upon, obtain the signed agreement and confirm scope.

A control can exist and be ineffective.

At Langmere Systems, the risk assessment credited multi-factor authentication. External guest accounts used a separate route on which MFA was optional. The control description was true for employees and false for the people who presented the immediate risk.

The rating changed when the team looked at the actual boundary.

Risk ownership is not administration

The risk owner should have authority to understand the consequence, decide treatment and accept residual exposure within defined limits. The person maintaining the register is not automatically the owner.

A bid manager may own the risk of late submission. The commercial director may own exposure from sensitive pricing access. The data-protection officer may advise on privacy risk without owning the commercial decision. The solution director may own risk created by a proposed cloud architecture. Top management may need to accept risk beyond normal tolerance.

Bid team is not a person and rarely has authority.

Assign one accountable owner. Record advisers and treatment owners separately where useful.

Clause 6.1.3 turns analysis into treatment

After evaluating risk, the organisation selects appropriate treatment options, determines controls needed to implement those options, compares necessary controls with Annex A to check that none have been omitted, produces a Statement of Applicability, creates a treatment plan and obtains risk-owner approval of both the plan and accepted residual risk.

Typical treatment options include:

- avoid the activity or opportunity;
- reduce likelihood or consequence through controls;
- share or transfer part of the exposure through contract or insurance;
- retain the risk by informed acceptance.

Security language sometimes treats avoidance as weakness. In bidding, it may be the most professional decision. Do not enter a data room your organisation cannot protect. Do not promise a service requiring security clearance you cannot obtain. Do not provide restricted material to a partner whose control environment has not been assessed.

Choose controls from the risk, then compare with Annex A

The sequence matters.

First determine what controls are necessary to treat the identified risks and meet relevant requirements. Then compare the proposed set with Annex A to ensure no necessary control has been missed. The organisation may select controls from Annex A, design additional controls or use controls from other sources.

Annex A is not a compulsory shopping list. It is also not a list to ignore because the team has invented its own terminology.

A risk involving a freelance writer and confidential customer data may need controls for supplier relationships, confidentiality, access, secure transfer, endpoint protection, awareness, event reporting and return or deletion of information. The precise set comes from the exposure and requirements.

The comparison against Annex A is a completeness test.

The Statement of Applicability

Figure 6 - From risk criteria and treatment decisions to the Statement of Applicability and operating evidence.

The Statement of Applicability, commonly called the SoA, is one of the central records of an ISMS. It should show the necessary controls, why they are included, whether they have been implemented, and why any Annex A control is excluded as unnecessary.

A practical SoA may contain:

- control reference;

- control description in organisational language;
- inclusion status;
- justification for inclusion or exclusion;
- risk, legal, contractual or business source;
- implementation status;
- control owner;
- evidence location;
- linked policy or process;
- planned action or review date.

The SoA should be understandable to people outside the security function. It is not a spreadsheet whose purpose is to satisfy one auditor for two days.

Exclusion needs reasoning

An Annex A control may be unnecessary within the defined scope. The justification should relate to risk and context.

Not applicable because we do not think it applies is circular.

A.7.12 cabling security is excluded from the bid-services ISMS because the organisation operates entirely from serviced offices and approved cloud services; it owns no communications cabling within scope. Physical and supplier risks associated with the serviced-office network are addressed through provider due diligence, network controls and contractual requirements is a reasoned position.

The conclusion might still be challenged. At least it can be evaluated.

Be careful with outsourced services. Outsourcing an activity does not automatically remove the related risk or control need. It often changes the control from direct operation to supplier selection, agreement, monitoring and assurance.

Included does not mean fully implemented

The SoA can show that a control is necessary but not yet completely implemented. Hiding the gap weakens the system.

Use status such as:

- implemented and evidenced;
- partly implemented;
- planned;
- not implemented;
- not applicable with justification.

Link incomplete controls to the treatment plan, owner, target date and risk decision.

During certification preparation, teams sometimes mark every control implemented because an auditor is approaching. That creates a second problem: the SoA no longer describes the ISMS.

The risk-treatment plan

For each required action, record:

- risk and control affected;
- intended change;
- owner;

- resources;
- target date;
- dependencies;
- acceptance criteria;
- verification method;
- residual-risk review;
- status.

A treatment plan should be integrated with business work. If the action is to restrict external access, the workspace owner and supplier onboarding process need to change. If the action is to strengthen evidence of secure software development, the solution and engineering teams need time to produce it. If the action is to introduce an approved AI environment, technology, legal, privacy, procurement and bid operations may all be involved.

A security project list without authority and resource is an inventory of good intentions.

Operational risk assessment under clause 8.2

The organisation must perform information security risk assessments at planned intervals and when significant changes are proposed or occur. Clause 8.2 is where the defined method meets live operation.

Bid-related triggers can include:

- receipt of unusually sensitive information;
- a new customer sector or jurisdiction;
- change in the proposed technical solution;
- use of a new cloud or AI service;
- addition or replacement of a partner;
- remote work from another country;
- personal data at greater scale;
- new security schedule or contract obligation;
- material incident or near miss;
- change in workspace, identity provider or submission route;
- climate-related disruption affecting availability.

Do not assess the entire enterprise again because one file changed. Assess the relevant risk and its interactions.

Operational treatment under clause 8.3

Clause 8.3 requires implementation of the risk-treatment plan and retention of results. The control must leave evidence that it operated.

For a live Strategic pursuit, treatment evidence might include:

- approved workspace and access review;
- signed supplier security schedule;
- encrypted transfer record;
- device-compliance report;
- completed secure-working briefing;
- risk acceptance;
- technical security review;
- tested backup and recovery;
- incident exercise;

• deletion or access-removal confirmation.

The risk register is not evidence that the control happened.

The treatment workshop

Run the workshop after assets, requirements and initial risks are understood, but before architecture, suppliers and working practices become difficult to change.

For each material risk:

1. confirm the information and business process involved;
2. test the risk statement and current controls;
3. agree consequence, likelihood and uncertainty;
4. compare with acceptance criteria;
5. select treatment option;
6. identify necessary controls;
7. compare against Annex A;
8. assign owner, resource and date;
9. define evidence and residual-risk approval;
10. set reassessment triggers.

Keep one difficult risk on screen until the whole route is complete. Ten superficially reviewed risks are less useful than one treatment the organisation can actually implement.

A bid-risk example

Vantage Health Analytics received pseudonymised patient data for a tender demonstration. The team initially rated disclosure risk low because direct identifiers had been removed.

The privacy lead challenged the assumption. The dataset included rare conditions, location, age and treatment dates. Re-identification remained possible. Two external developers needed access, the demonstration environment used a public cloud tenant and the tender required deletion within ten working days of the result.

Treatment changed:

• the dataset was classified at the required level;
• access was limited to named users;
• external developers used managed accounts and devices;
• the cloud tenant was reviewed and logged;
• downloads were blocked where practicable;
• test outputs were checked for disclosure;
• a deletion task and evidence requirement were added;
• the residual risk was accepted by the accountable owner.

No new firewall was purchased.

The assessment had found the controls the work required.

Quality test - can the risk decision survive daylight?

Choose one high risk and ask:

• Which information is at risk?
• Which security property could be harmed?
• What event and condition create the exposure?
• What is the consequence and to whom?

- Which current control has been verified?
- What criterion makes the risk acceptable or unacceptable?
- Who owns it?
- Which treatment option was selected?
- Which control will change the exposure?
- Where is the control represented in the SoA?
- What evidence will show implementation?
- Who accepts the residual risk?
- What event requires reassessment?

If the answers cannot be found without the security manager translating the register, improve the record.

At 17:18, the team returned to the thirty-eight amber risks.

Nine became low after current controls were verified. Seven became high. Four were combined because they described the same exposure. Six were removed because they were generic threats without a connection to the scope. Three created treatment actions. One caused the organisation to decline the proposed demonstration method.

The register became shorter.

The decisions became visible.

CHAPTER 12

Secure Solution Design, Pricing and Evidence

CASE FILE

The proposed service looked secure on the architecture diagram.

There were shields around the cloud, locks beside the databases and a dark blue line labelled **encrypted transfer**. At the solution review, the customer-security lead asked who would create the first administrator account.

The room looked at the diagram.

The diagram looked back.

Nobody had designed the first administrator account.

Security is a property of the offer

A bid does not merely describe an existing information security management system. It often designs a customer-specific service, operating model, transition or technology arrangement. Security therefore belongs inside solution design, not in a separate answer added after the service has been decided.

The design must address applicable customer, legal, regulatory, contractual and organisational requirements. It also needs to reflect the risk assessment and selected treatments.

For a service proposal, security design may include:

- information flows and trust boundaries;
- identity and access model;
- responsibilities between customer, supplier and partners;
- data locations, transfers, retention and disposal;
- technical architecture and configuration;
- logging, monitoring and incident response;
- business continuity and recovery;
- secure development and change;
- physical and remote-working conditions;
- supplier and cloud controls;
- personnel screening, competence and confidentiality;
- assurance, reporting and evidence;
- mobilisation and exit.

The security response should explain this design. It should not manufacture it.

Begin with security requirements

Collect design inputs from controlled sources:

- tender questions and specifications;

- security schedules and contracts;
- data-protection requirements;
- customer policies and technical standards;
- legal and regulatory obligations;
- classification and handling instructions;
- risk assessment and treatment decisions;
- customer architecture and service constraints;
- user and operational needs;
- threat intelligence where relevant;
- internal security policies and approved patterns;
- provider capabilities and shared-responsibility models;
- previous incidents, audits and lessons.

Reconcile contradictions early.

A customer may require UK data residency in one schedule and permit broader processing in another. A proposed SaaS provider may describe backups in marketing material while the contract excludes restoration commitments. A security questionnaire may ask for twenty-four-hour monitoring when the price model assumes business-hours support.

These are not writing issues.

Build a security requirements trace

For each material requirement, record:

- exact source;
- interpretation;
- design response;
- owner;
- control or treatment;
- evidence;
- customer dependency;
- price or resource effect;
- verification or validation method;
- final response location;
- handover obligation.

This is not necessarily a separate spreadsheet. It may be a security view of the wider compliance matrix or solution design record.

The purpose is to stop security commitments from becoming detached from the service that must deliver them.

Architecture begins with information movement

Before drawing products and logos, map information.

What enters the service? Where does it come from? Which party owns or controls it? Where is it processed, stored, copied, backed up, logged and deleted? Which people, systems and providers can reach it? What leaves the service, in what form and through which route?

Mark trust boundaries. A boundary may exist between:

- customer and supplier;
- employee and privileged administrator;

- corporate network and cloud service;
- prime and subcontractor;
- production and development;
- approved device and personal device;
- public information and customer-confidential information;
- human reviewer and AI service.

Controls belong where trust changes.

At Moreton Digital, the original diagram showed one secure platform. The information-flow map revealed five exports: monthly reports, support logs, analytics files, developer troubleshooting bundles and invoice evidence. Two travelled by email. The proposed security position was only as strong as the least-controlled export.

Shared responsibility must be written down

Cloud and managed services divide responsibility. The provider may secure physical infrastructure and underlying platform components while the customer or supplier remains responsible for identities, configuration, data, logging, retention and user behaviour.

Do not use hosted in an accredited cloud as a complete control explanation.

For each boundary, state:

- who configures;
- who monitors;
- who approves access;
- who patches;
- who responds to incidents;
- who preserves evidence;
- who communicates with the customer;
- who backs up and restores;
- who deletes data;
- who proves performance.

Where responsibility is shared, name the interface and escalation.

A blank between two responsible parties is not shared responsibility. It is an unowned control.

Design the privileged path

Ordinary user access receives attention because many people use it. Privileged access can change the system, read broader information, disable controls or erase evidence.

Design:

- how privileged identities are created;
- approval and segregation;
- authentication;
- least privilege;
- time limitation or just-in-time access where appropriate;
- logging and review;
- emergency access;
- supplier administrator access;
- removal after change or termination;

• monitoring of high-risk activity.

Return to the first administrator account.

At Axon Borough Services, the proposed mobilisation process required the implementation partner to create the tenant and then hand it over. The partner's administrator would remain as a recovery account. Nobody had approved that arrangement. The design changed to customer-authorised named accounts, controlled handover, removal of bootstrap access and verified recovery credentials.

One line in the mobilisation plan became four controlled actions.

Secure development where the bid includes change

If the offer includes software development, configuration, integration, automation or substantial technical change, define the secure development lifecycle.

Consider:

- security requirements;
- architecture and threat modelling;
- coding standards;
- source-code access;
- secrets management;
- dependency and vulnerability management;
- code review;
- security testing;
- separation of development, test and production;
- test-data control;
- release and change approval;
- outsourced development;
- defect and incident handling.

Do not claim a secure development lifecycle because the engineering team uses a ticketing system.

Ask for objective evidence: process, roles, sample records, scan results, code-review practice, release controls, penetration-test governance and corrective actions.

The tender response should be accurate about scope. A company may have mature secure development for its core platform and weaker control for low-code automations built by business teams. If the proposed service relies on both, the difference matters.

Verification and validation

Verification asks whether design outputs meet the identified inputs. Validation asks whether the resulting solution can achieve the intended secure operation in realistic conditions.

Verification may include:

- requirements trace;
- architecture review;
- configuration comparison;
- contract and provider review;
- access-model check;
- privacy or security assessment;
- calculation and capacity check;

- evidence review.

Validation may include:

- tabletop incident exercise;
- recovery test;
- user-access walkthrough;
- penetration or vulnerability testing;
- phishing or social-engineering exercise where justified;
- supplier scenario;
- failover test;
- secure mobilisation rehearsal;
- demonstration with representative data;
- exit and deletion exercise.

A document can verify that a recovery time has been written. Only a suitable test can show whether recovery is credible.

Design the difficult security day

Run scenarios before the answer becomes final.

- A privileged account is compromised during mobilisation.
- A subcontractor reports ransomware.
- The customer sends information at a higher classification than expected.
- Logging fails during a suspected incident.
- An employee leaves with access still active.
- The cloud region becomes unavailable.
- A vulnerability is disclosed in a critical component.
- The customer asks for an urgent data export.
- The AI service retains content contrary to the assumed arrangement.
- A physical office becomes inaccessible during final submission.

For each scenario ask:

1. How is the event detected?
2. Who decides severity?
3. What is contained first?
4. Which service and information remain available?
5. Who informs the customer and when?
6. What evidence is preserved?
7. How does recovery work?
8. Which contractual clock applies?
9. What changes after the event?

The answer should not depend on the person who wrote the tender being awake.

Price the control environment

Security controls consume resource. Price them.

Costs may include:

- licences and security tooling;
- identity, logging and monitoring;
- specialist personnel;

- screening and training;
- assurance and testing;
- penetration tests;
- certification and independent review;
- secure devices and connectivity;
- provider charges;
- backup, storage and retention;
- incident response cover;
- travel or secure facilities;
- legal and privacy advice;
- transition and exit;
- contingency and remediation.

A security answer that promises continuous monitoring, annual penetration testing, twenty-four-hour incident response and dedicated customer reporting while the price contains none of them is not persuasive value. It is an unfunded operating model.

Use a security cost ledger

For each material security commitment, record:

- requirement or risk;
- proposed control;
- owner;
- one-off cost;
- recurring cost;
- volume or usage assumption;
- provider price;
- customer dependency;
- contract treatment;
- evidence and measure;
- decision to retain, redesign or remove.

The ledger allows the team to respond intelligently when price pressure arrives.

Cutting a duplicate dashboard may be sensible. Removing monitoring needed to detect a contracted incident is a different decision.

At Moreton Digital, a director proposed removing the managed security service to reduce price. The ledger showed that the service supported the promised monitoring window, incident response and monthly assurance. The team instead reduced bespoke report design and retained the control.

The cheaper offer still described the same security model.

Avoid security theatre in value claims

Buyers do not award points merely because a bidder lists more tools. Explain the customer consequence.

Weak:

> **WORKING WORDS**
>
> We use leading security technologies, industry best practice and military-grade encryption.

Stronger:

> **WORKING WORDS**
>
> Named customer administrators approve access through the service portal. Privileged access is time-limited, protected by multi-factor authentication and logged. The security team reviews privileged events each working day and escalates defined anomalies under the incident process. The customer receives a monthly access and exception report.

The second statement can be tested, priced and handed over.

Be cautious with military-grade, unhackable, zero trust and fully compliant. These phrases often create more questions than confidence.

Evidence must match the claim

Security evidence may include:

- ISO/IEC 27001 certificate and exact scope;
- Statement of Applicability extract where appropriate and permitted;
- independent audit or assurance report;
- penetration-test governance and remediation summary;
- vulnerability and patch metrics;
- incident and recovery records;
- access-review evidence;
- secure-development records;
- supplier evaluations;
- training and competence evidence;
- customer references;
- system architecture and configuration evidence;
- business-continuity tests;
- privacy and security assessments.

A certificate is useful evidence of a management system within a defined scope. It is not proof that the proposed customer solution has been securely designed.

Check entity, site, service, edition, expiry, certification body and accreditation. Do not upload a certificate belonging to a parent company and describe it as the bidder's without explaining the relationship and scope.

Security evidence cards

For reusable evidence, record:

- claim supported;
- source and owner;
- scope and boundary;
- date and period;
- method and sample;

- result;
- independent assurance;
- confidentiality and permission;
- limitations;
- review date;
- approved use.

A penetration-test statement should identify what was tested and when, without exposing sensitive details. A training percentage should state the population and period. An incident statistic should define what counted as an incident.

No breaches in ten years may mean excellent control, incomplete detection, narrow definition or marketing enthusiasm. Give the number bones.

Customer security questionnaires

Security questionnaires can contain hundreds of questions. Do not answer from memory or copy a previous submission without checking the proposed service.

Classify responses:

- corporate ISMS control;
- service-specific control;
- planned treatment;
- customer responsibility;
- provider responsibility;
- not applicable with reason;
- clarification required.

Link answers to evidence and owners. Reconcile them with the contract, solution and price.

If one answer says logs are retained for twelve months and another says ninety days, the buyer sees more than an editorial inconsistency. It sees a service whose control environment is unknown.

Security schedules become delivery obligations

Extract every material answer and schedule response into the promise register.

Include:

- control or service commitment;
- responsible owner;
- customer dependency;
- evidence and reporting;
- timing;
- resource and cost;
- provider involvement;
- incident or exception route;
- contract location;
- mobilisation action.

A security schedule may be incorporated into the contract. Treat it as design output, not a questionnaire completed by whichever person had time.

Design change under pressure

Security design changes when the customer clarifies, the solution evolves, the price moves or a provider changes. Assess impact across:

- requirements;
- risks and SoA;
- architecture;
- data and privacy;
- access;
- suppliers;
- continuity;
- incident response;
- price;
- evidence;
- narrative;
- mobilisation and contract.

At 19:42, two days before release, Axon's cloud provider confirmed that one logging feature required a higher service tier. The feature supported a contractual monitoring commitment.

The team had three choices: buy the tier, redesign the control or qualify the commitment through the permitted route. It chose the higher tier and updated price, architecture, supplier record and evidence.

It did not leave the paragraph unchanged and hope the licence became generous after award.

Security solution review

A useful review asks:

1. Which information and systems are in scope?
2. Which customer and legal security requirements apply?
3. What risks have been assessed and treated?
4. Which controls are necessary and where are they implemented?
5. How are responsibilities divided between parties?
6. Are identities, privileged access and lifecycle controlled?
7. How are data transfer, retention and deletion managed?
8. Does the design work during incident and disruption?
9. Are suppliers and cloud services controlled?
10. Are security commitments resourced and priced?
11. What evidence supports the claims?
12. What remains assumed?
13. What must be verified or validated before release?
14. Who approves the baseline and residual risk?

Record decisions. Do not produce a transcript of everyone saying security is important.

Quality test - trace one security promise

Choose the most important security promise in the bid and trace it through:

- customer requirement;
- information asset and risk;

- treatment decision;
- Annex A or other control;
- SoA;
- solution design;
- provider responsibility;
- resource and price;
- evidence;
- response wording;
- verification or validation;
- approval;
- promise register;
- delivery measure.

If the links describe different realities, the promise is not ready.

The first administrator account at Axon eventually appeared in the mobilisation plan. A named role requested it. A separate authority approved it. The identity was protected, logged, time-bound and removed after handover. Recovery access followed another controlled route.

The architecture diagram changed by one small box.

The operating model changed considerably more.

CHAPTER 13

Writing as Controlled Information Processing

CASE FILE

At 10:38, a writer pasted three pages of customer material into a generative-AI tool.

The material was not highly classified. It did contain the authority's network weaknesses, named administrators and a timetable for replacing an unsupported system.

The writer had been told not to upload confidential information. She did not think of the passage as an upload. She thought she was asking for help with structure.

The security policy had used the word processing.

The writer had used the word writing.

The information did not care which word they preferred.

A bid answer is an information product

Writing receives requirements, solution decisions, evidence, personal data, commercial assumptions and customer information. It transforms those inputs into an output that may be disclosed to evaluators, incorporated into a contract and retained for years.

That makes writing part of the ISMS.

Control should cover:

- authorised inputs;
- classification and handling;
- access and roles;
- approved tools;
- source provenance;
- personal and customer data;
- version and change;
- factual and security claims;
- external contributors;
- review and approval;
- final preservation, transfer and retention.

The purpose is not to make writers fearful. It is to make the safe route ordinary enough that urgency does not replace it.

Plan the answer before distributing information

An answer plan reduces both quality and security risk. It identifies what information is actually needed before the team sends broad folders to every contributor.

Record:

- question and response objective;
- required components;
- customer and security requirements;
- approved solution position;
- evidence required;
- contributors and access need;
- information classification;
- permitted tools and transfer routes;
- facts or claims requiring specialist approval;
- word or page constraint;
- review and release route.

A freelance writer asked to draft a 1,000-word security answer does not necessarily need the complete customer data room, full risk register and unredacted employee records. Give the minimum controlled inputs needed for the assigned task.

Source discipline

Every material claim should be traceable to an approved source or clearly identified as a proposed commitment requiring approval.

Useful sources include:

- customer documents;
- approved corporate policies;
- current technical standards;
- controlled solution baselines;
- provider agreements;
- verified performance records;
- approved evidence cards;
- named subject-matter decisions;
- risk and treatment records;
- current certificates and assurance reports.

We said it last time is not a source class.

A previous tender can help identify material. It may contain outdated systems, old scope, another customer's requirements or an overstatement that happened not to be challenged.

Preserve provenance when text moves. A paragraph copied without its source and limitations becomes easier to misuse each time.

Classification follows the content

Writers often work in fragments: one paragraph, one screenshot, one table. The classification still follows the information.

A redacted case study may be suitable for a broader writing team while the underlying customer report remains restricted. A public certificate may be stored beside a confidential SoA extract. A CV may become less sensitive after personal contact details are removed, but it remains personal information.

Mark content or containers in a way users can understand. Avoid classification labels so complicated that people guess.

The writing brief should state the handling rule:

WORKING WORDS

Customer Confidential. Use only in the approved pursuit workspace. Do not download to unmanaged devices, forward outside the named team or submit to external AI services. Retain until the controlled campaign archive is created, then follow the project disposal instruction.

That tells a person what to do.

Access at question level where necessary

Not every contributor needs every answer.

Highly sensitive pursuits may separate:

- commercial pricing;
- security architecture;
- employee information;
- legal advice;
- customer data;
- partner-confidential material;
- executive risk acceptance.

Use role-based workspaces, restricted sections or controlled exchanges. Keep the bid manager able to integrate the campaign without granting broad access by convenience.

Segregation must not destroy coherence. The commercial lead may not see detailed security vulnerabilities, but must understand the resources and costs created by treatment. The writer may not see a full penetration-test report, but needs an approved assurance statement and limitations.

Design information interfaces, not isolated rooms.

Personal data in bid content

Bids commonly include CVs, biographies, contact details, qualifications, employment history, references, equality information, security-clearance status and photographs.

Determine:

- lawful and fair use;
- minimum information required;
- notices or consent where applicable;
- customer instruction;
- access and transfer;
- retention;
- accuracy;
- security;
- reuse in future bids;
- rights and internal responsibilities.

Do not keep a permanent library of unredacted CVs because future tenders may ask for them. Maintain controlled profile information, review it with the individual and generate opportunity-specific content with minimum necessary detail.

At Rowan Infrastructure, a writer reused a CV containing a former home address and old mobile number. Neither was requested. The error did not improve the answer. It only widened exposure.

The profile template changed after that afternoon.

Customer and third-party property

Tender documents, data, systems access, sample materials, intellectual property and confidential provider information may be customer or third-party property. Identify it and protect it.

If property is lost, damaged, corrupted or used improperly, follow the required incident and customer-communication route. Do not quietly replace a missing file from somebody's email and assume the issue ended.

Writers should know that permission to read a document does not imply permission to reproduce it in a different answer, place it in a public portfolio or send it to another client.

AI-assisted writing begins with an approved use case

Do not begin governance at the prompt. Begin with the purpose.

Possible approved uses may include:

- structuring an answer from non-sensitive approved inputs;
- comparing controlled documents;
- identifying inconsistent terminology;
- summarising approved evidence;
- suggesting alternative wording;
- testing readability;
- generating reviewer questions;
- extracting candidate commitments.

Higher-risk or prohibited uses may include:

- uploading customer-confidential documents to an unapproved public service;
- generating security claims without controlled sources;
- making legal or compliance decisions;
- processing sensitive personal data without an assessed route;
- creating fictitious evidence;
- allowing automated submission without human release;
- using customer information to train an uncontrolled model.

The boundary depends on provider terms, configuration, data class, jurisdiction, contract and organisational risk.

Retrieval does not remove responsibility

A retrieval-augmented system can ground drafting in approved sources. It can also retrieve the wrong source accurately.

Control:

- source ownership;
- access inheritance;
- currency;
- metadata;
- document chunking;

- citation or source link;
- restricted content;
- model and provider route;
- output review;
- refusal where evidence is absent.

Require the writer to inspect the supporting passage. A generated sentence should not become true because a source number appears beside it.

At Fieldstone Security, the assistant cited a current policy but interpreted an aspirational target as achieved performance. The citation was real. The claim was not.

Human review corrected the meaning.

Prompts can contain sensitive information

A prompt may reveal more than an uploaded file. It can include customer names, weaknesses, assumptions, prices, staff information and strategy.

Minimise. Replace unnecessary identifiers. Use approved accounts and retention settings. Do not place secrets into reusable prompt libraries.

Where prompt logs are retained for assurance, protect them as information assets. Where they are not retained, decide how sufficient provenance and accountability will still be shown.

We delete all prompts and we log every prompt forever can both be poor controls when applied without context.

Human accountability needs a name

Every AI-assisted answer requires a content owner who can explain:

- what the question required;
- which sources were used;
- what the model contributed;
- which claims and commitments appear;
- how confidentiality was protected;
- what was rejected;
- who approved the final text.

The owner does not need to preserve every keystroke. They need enough evidence to show controlled production and release.

A model cannot be the approver, reviewer or risk owner.

Natural prose and security truth

Security writing becomes unconvincing when every paragraph follows the same polished pattern. Real operations contain boundaries, exceptions and awkward dependencies.

Use varied paragraph length. State a decision briefly when brevity helps. Explain complexity when it genuinely exists. Include roles, systems, timings, triggers and evidence. Use a short scenario where it reveals behaviour under pressure.

Do not introduce deliberate errors to appear human.

The aim is writing that reflects considered work rather than automated confidence.

Weak:

WORKING WORDS

We take information security extremely seriously and employ robust, industry-leading measures to ensure complete protection of all data at all times.

Operational:

WORKING WORDS

The bid manager grants workspace access against the approved team list. Guest access expires after fourteen days unless the information owner renews it. The platform records access and file activity. At campaign close, the manager removes external users, transfers the released record to the controlled archive and obtains deletion confirmation for locally held partner copies where required.

The second answer is less dramatic and more secure.

Write boundaries as well as controls

A trustworthy answer states where the control applies and what depends on another party.

Examples:

- monitoring covers the managed platform, not customer endpoints outside the service boundary;
- the supplier deletes working copies after acceptance, while statutory records are retained separately;
- customer approval is required before named administrators receive access;
- recovery time assumes connectivity and customer dependencies stated in the plan;
- background screening follows the legal and role requirements applicable in the relevant jurisdiction.

Boundaries prevent later conflict and help an evaluator understand the offer.

Do not hide material limitations. Resolve them through design, clarification or a controlled assumption.

Security terminology needs control

Create a terminology and entity dictionary for:

- customer and bidder legal names;
- systems and environments;
- data classifications;
- security roles;
- incident levels;
- service periods;
- providers;
- locations;
- controls and policies;
- regulatory terms.

One answer may refer to Security Operations Centre, another to SOC, and a third to Cyber Monitoring Team. They may be the same service or three different things. The evaluator should not have to decide.

Be careful with acronyms. Define them once. Use customer terminology where accurate. Do not borrow a customer's internal role name if your service assigns different authority.

Security claims need evidence and scope

Extract material claims during drafting:

- certified to ISO/IEC 27001;
- all data encrypted;
- 24/7 monitoring;
- zero security incidents;
- UK-based support;
- annual penetration testing;
- all staff screened;
- data deleted within thirty days;
- 99.99 per cent availability.

For each, ask:

- Which entity, service, information or population does this cover?
- What period applies?
- What exceptions exist?
- Which evidence supports it?
- Who approves it?
- Is it priced and deliverable?
- Does another document say something different?

Absolute claims deserve particular suspicion.

All data is encrypted may fail for logs, backups, email, temporary files, keys or a customer-selected integration. State the actual control.

Review generated and human text by the same standard

Do not create a lower assurance route for generated text or assume human text is safer.

Review both for:

- coverage of requirements;
- factual accuracy;
- source provenance;
- confidentiality;
- consistency;
- security design and risk;
- commitments;
- legal and contractual meaning;
- customer language;
- evidence;
- readability.

AI may invent. People may exaggerate, copy stale content or misunderstand. The release criterion concerns the output, not the ego of the author.

Working versions and change

Define one authoritative working version. Use statuses such as Draft, Technical Review, Independent Review, Approved Content, Released and Submitted.

Control material changes affecting:

- security claims;
- scope;
- architecture;
- risk;
- provider responsibility;
- incident timing;
- retention;
- certification;
- price;
- customer dependency.

A late edit from may notify to will notify within one hour is not grammar. It is an incident-response commitment.

Return it to the relevant owner and approval route.

Comments can contain sensitive material

Review comments and tracked changes may reveal vulnerabilities, legal advice, pricing, personal information or internal disagreement. They are part of the information set.

Protect the review environment. Remove comments and tracked changes from released files. Verify that hidden content, document properties, embedded objects and previous versions are not unintentionally disclosed.

Do not rely on visual appearance alone. Inspect the final file and its metadata using appropriate tools.

External writers and editors

Before access:

- approve the provider;
- define scope and deliverables;
- agree confidentiality, data protection and intellectual property;
- assess system and device requirements;
- grant minimum access;
- brief classification and incident reporting;
- define acceptance and review.

During work, review early output. After work, remove access, confirm return or deletion and evaluate performance.

The supplier remains responsible for the submitted answer.

A fast writer working outside the control environment can create more risk in two days than a slow internal process creates in a month.

Secure content-production cadence

For a complex security response due Friday:

Monday morning: confirm requirements, classification, answer plan, solution baseline, evidence and permitted tools.
Monday afternoon: interview accountable specialists; record decisions, sources and gaps.
Tuesday: develop complete content; update claims, evidence and promise registers.
Wednesday morning: technical, privacy, commercial and provider approval where relevant.
Wednesday afternoon: independent review against requirement, risk and evaluator confidence.
Thursday morning: controlled correction, source verification and cross-document consistency.
Thursday afternoon: content approval, secure production and metadata checks.
Friday: contingency, release and submission. Not planned invention of the security model.

Shorter bids compress the sequence. They should not remove source control and accountable release.

Quality test - follow a paragraph

Choose one paragraph containing a material security claim.

- Who requested it?
- Which requirement does it answer?
- Which information classification applies to its inputs?
- Who had access?
- Which source supports each material fact?
- Did AI or an external provider contribute?
- Which solution and risk decision does it describe?
- Who approved technical truth?
- Which commitment does it create?
- Where is that commitment priced and handed over?
- Does the released file contain the approved text and no hidden review material?

At 16:20, the writer who had used the AI service helped reconstruct the event. The organisation did not treat her as the security problem. The approved-use guidance had described files but not prompts, the tool was accessible through a personal account and no safe alternative had been made easy.

The immediate content was removed and the customer impact assessed. The use rules changed. The approved system was configured. Training used the actual scenario.

The next writer still asked for help with structure.

This time the information stayed inside the route designed for it.

CHAPTER 14

People, Suppliers, Cloud, AI and Remote Work

CASE FILE

The consortium partner joined the bid room on Wednesday.

By Thursday afternoon, its solution architect could see pricing, employee profiles, the customer's security schedule and a draft legal-departures table. He needed the architecture folder and two questions.

The access request had said Full access - urgent.

At 17:11 on Friday, the partner withdrew from the pursuit.

His account remained active until the following month because the person who approved access assumed IT would know.

IT did not know the partner had withdrawn.

The access system had worked exactly as instructed.

Security follows the working relationship

Bid operations rely on employees, contractors, advisers, partners, subcontractors, cloud services, software providers and customer platforms. Each relationship changes information risk.

The ISMS should control the lifecycle:

- selection and screening;
- terms and responsibilities;
- access and equipment;
- awareness and competence;
- supervision and monitoring;
- change of role or scope;
- incident reporting;
- termination, return and deletion;
- performance and re-evaluation.

Do not treat onboarding as an administrative start and offboarding as an HR finish. Access, knowledge, devices and obligations move throughout the relationship.

Screening follows role and law

Screening should be proportionate to role, information, customer requirements, legal conditions and risk. It may include identity, employment history, qualifications, references, right to work, criminal-record checks, financial or security vetting where lawful and relevant.

Do not promise universal screening without understanding jurisdictions, workforce types and provider arrangements.

A tender may require baseline personnel security standards for everyone with access to certain information. The bid team needs to know whether named personnel already meet the condition, how new people will be screened, how evidence is protected and what happens if clearance is delayed.

At Marshwell Consulting, a proposal said all personnel were screened before access. Two freelance designers were onboarded through a purchase order and had never entered the HR process. The claim was narrowed and the provider route corrected.

The sentence had found an organisational boundary.

Terms must carry security responsibilities

Employment, contractor and supplier terms should communicate relevant responsibilities:

- confidentiality;
- acceptable use;
- customer and company information;
- intellectual property;
- remote working;
- incident and event reporting;
- monitoring where lawful;
- return and deletion;
- obligations continuing after the relationship;
- disciplinary or contractual consequence;
- compliance with customer-specific rules.

A non-disclosure agreement is not the whole security relationship. It may prohibit disclosure while saying nothing about device security, subcontracting, cloud tools, deletion or incident timing.

Use contracts and working instructions together.

Awareness must reach the actual risk

Annual information-security training creates a baseline. Live pursuits need local awareness.

At kick-off, brief:

- customer handling rules;
- classifications;
- approved workspace and transfer routes;
- personal-data use;
- supplier and AI boundaries;
- phishing and impersonation risk;
- unusual file handling;
- incident reporting;
- release and disposal;
- any customer-specific obligation.

Keep it short enough that people listen. Use examples from the work.

Do not use personal email is clear. So is The customer's pricing workbook may be shared only through the restricted commercial folder; do not attach it to meeting invitations.

Awareness is shown when a person recognises the situation and acts correctly, not when a learning platform records completion.

Competence for security decisions

Different roles need different competence.

A bid manager should understand classification, access, supplier onboarding, incident escalation and the security effect of changes.

A security architect should understand the proposed technical service, customer requirements, risk method, provider responsibilities and evidence.

A writer should recognise sensitive inputs, unsupported claims and prohibited tools.

A reviewer should test whether the answer describes a credible control environment rather than rewarding vocabulary.

An uploader should know account, device, file-integrity and receipt controls.

A senior approver should understand what residual risk is being accepted.

Training may support competence. Practical exercise, supervised work, professional qualification, observed performance and incident learning may provide stronger evidence.

Disciplinary process and fair consequence

Deliberate or repeated violation may require disciplinary or contractual action. The process should be understood, lawful and consistent.

Do not use discipline to avoid examining control design.

If a person repeatedly transfers customer information through an unapproved service after clear instruction and available safe alternatives, individual accountability matters. If half the team uses the service because the approved route cannot accept large files, the system is speaking as well.

Both may need action.

A mature investigation separates intent, competence, workload, incentives, tool design and control failure.

Role change and termination

Access should change when responsibility changes, not only when employment ends.

Trigger review when:

- a person joins or leaves a pursuit;
- a partner's work package changes;
- an employee changes role;
- a contractor's assignment ends;
- a supplier is replaced;
- a customer stage closes;
- a bid moves into mobilisation;
- an incident affects trust;
- privileged work is complete.

Remove or adjust access promptly. Recover assets. Transfer records and knowledge. Confirm continuing confidentiality and deletion duties.

The withdrawal at the start of this chapter should have created an access-removal event. It did not because partner status and identity management lived in separate processes.

The corrective action joined them.

Remote working is an operating model

Bid teams work from homes, trains, hotels, customer offices, shared workspaces and other countries. Remote work changes physical, technical and human controls.

Consider:

- authorised location and jurisdiction;
- privacy from household or public observation;
- secure device and patching;
- network and VPN;
- storage and printing;
- clear screen and conversation;
- theft and loss;
- backup and availability;
- technical support;
- working hours and fatigue;
- disposal;
- emergency access;
- customer restrictions.

Do not write a policy that assumes every home has a private office. Define minimum conditions and alternatives.

A reviewer on a train may read a low-sensitivity draft with an approved privacy screen. They may not review a restricted security architecture while another passenger can photograph it. Proportionality still has boundaries.

Supplier risk begins before procurement

An external provider may contribute to the bid process or the offered service. Both matter.

Assess:

- criticality and information access;
- competence and capacity;
- security posture and relevant certification;
- legal entity and location;
- use of subcontractors;
- cloud and data arrangements;
- incident history where appropriate;
- continuity and exit;
- contractual terms;
- customer requirements;
- assurance and monitoring.

Selection should not rely on a questionnaire alone. Use evidence proportionate to risk: certificate scope, independent reports, technical information, demonstrations, references, contract review, audit rights or other assurance.

The cheapest freelance design service may be appropriate for a public brochure. It may be entirely unsuitable for a restricted defence submission.

Security in supplier agreements

Agreements should address relevant controls and responsibilities. Depending on the service, include:

- information classification and permitted use;
- access and identities;
- devices, networks and locations;
- confidentiality and privacy;
- subcontracting;
- cloud services;
- security incidents and notification;
- vulnerability and change;
- continuity and recovery;
- evidence and audit;
- return, deletion and exit;
- intellectual property;
- customer flow-down requirements;
- consequence of breach.

Make the clauses workable. A requirement to notify within fifteen minutes may be impressive until the supplier has no twenty-four-hour route and the prime has not funded one.

Security terms should match the operating relationship.

ICT supply-chain risk

Technology products and services contain their own suppliers, components, updates, dependencies and support chains. A proposed solution may depend on libraries, managed services, hardware, telecommunications and specialist subcontractors the prime does not directly operate.

Ask:

- Which components are critical?
- Who supplies and maintains them?
- How are vulnerabilities and updates handled?
- What provenance and assurance exist?
- What happens if support ends?
- Which geopolitical, concentration or availability risks matter?
- How does the customer learn of material change?

Do not promise complete supply-chain visibility where the market cannot provide it. State the due-diligence and monitoring approach, limits and escalation.

Monitor supplier services after signature

Supplier approval is not permanent.

Monitor:

- service and security performance;
- incidents;
- access;
- assurance evidence;
- certification changes;

- subcontractors;
- vulnerabilities;
- material service change;
- capacity and continuity;
- contract compliance;
- customer feedback.

Set review frequency according to risk. Trigger immediate review after material incident, ownership change, service relocation, control failure or proposed change.

For live bids, check that a provider's current position still supports the claims being made. Last year's certificate and this year's architecture may not belong to the same service.

Cloud services need lifecycle control

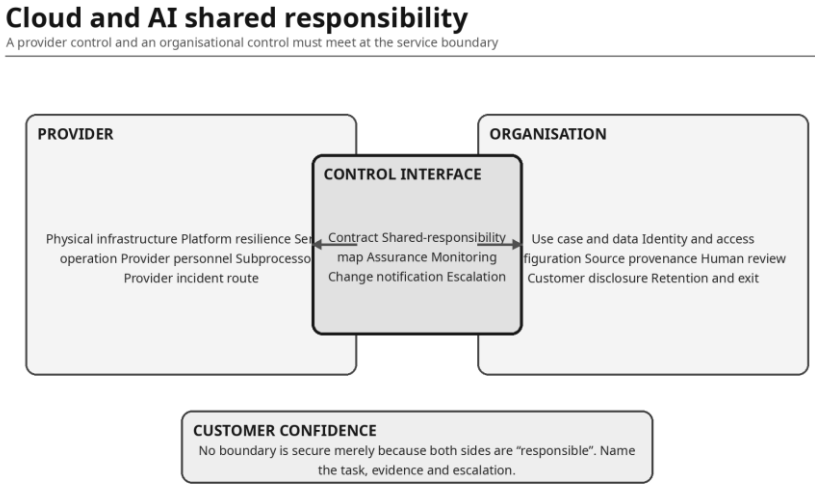

Figure 7 - Cloud and AI responsibility must be allocated across provider, shared and organisational control.

Cloud adoption creates decisions at acquisition, use, management and exit.

Establish:

- service owner;
- business and security requirements;
- data classes permitted;
- regions and transfers;
- identity integration;
- configuration baseline;
- logging and monitoring;
- backup and recovery;
- encryption and key responsibility;
- provider access;
- incident route;

- resilience and concentration;
- contractual assurance;
- change notification;
- deletion and exit.

A cloud service can be certified to ISO/IEC 27001 and still be configured unsafely by the customer. Certification belongs to a scope and management system. Configuration belongs to the actual use.

SaaS in the bid room

Proposal platforms, transcription tools, design systems, virtual data rooms, e-signature services and AI assistants are cloud services.

Before use, ask:

- What information enters?
- Does the provider train models or analyse content?
- Where is information stored?
- Which people and subprocessors can reach it?
- How is access managed?
- What retention and deletion apply?
- Can the organisation export records?
- What evidence is available?
- What happens at contract end?
- Does the customer's tender permit the use?

Enterprise is a commercial plan, not a risk-treatment decision.

AI providers and model risk

AI introduces provider, data, output and operational risks. Consider:

- confidential input;
- personal data;
- model training and retention;
- output fabrication;
- bias or inappropriate content;
- prompt injection and malicious documents;
- source provenance;
- dependency and availability;
- model or feature change;
- intellectual property;
- regulatory and customer disclosure;
- human over-reliance.

Control the service and the use case.

A low-risk grammar suggestion on public text differs from generating a security architecture from customer-confidential documents. The same product may sit in both scenarios. Risk depends on configuration and use.

Approved tool register

For each material tool, record:

- owner;
- purpose and approved use;
- prohibited use;
- provider and service tier;
- data classes;
- regions and subprocessors where relevant;
- access and authentication;
- retention and deletion;
- security evidence;
- integration and configuration;
- incident route;
- review date;
- exit plan.

Do not build a register nobody consults. Integrate approval into procurement, onboarding and workspace design.

When a user tries to add an unapproved tool to a pursuit, provide an assessment route and safe interim alternative. A prohibition without a workable route will be tested by the deadline.

External provider onboarding for a live bid

Before access:

1. confirm business need and scope;
2. classify information;
3. assess provider and contractual controls;
4. approve tool, device and location;
5. sign relevant terms;
6. create named identity and least-privilege access;
7. brief handling, incident and customer rules;
8. test access and working route;
9. record expiry and owner.

During work:

- monitor output and behaviour;
- review access after change;
- control transfers;
- preserve decisions;
- respond to incidents.

At end:

- remove access;
- recover assets;
- obtain return or deletion evidence where required;
- transfer records;
- evaluate performance;
- retain only authorised information.

Supplier truth in the tender

The prime's answer and the supplier's actual position must agree.

Ask each critical provider to review:

- service description;
- security responsibilities;
- locations;
- certifications;
- incident timing;
- continuity;
- personnel requirements;
- data handling;
- performance measures;
- mobilisation;
- price and assumptions.

A partner signature on a generic letter does not approve detailed commitments.

At Marshwell, the cloud partner approved the architecture but not the one-hour incident-notification commitment. Its standard agreement allowed notification without a fixed time. The prime either needed a negotiated term, another control or different wording.

It chose a managed monitoring service with a prime-owned initial notification route. The provider commitment remained accurate.

Quality test - remove one person and one supplier

Choose the person with the most privileged knowledge and the supplier with the most critical dependency.

For the person:

- What access do they hold?
- Which competence and screening apply?
- Who can act in their absence?
- How does role change remove access?
- Which knowledge must transfer?

For the supplier:

- What information and service do they control?
- Which requirements and risks apply?
- What agreement and evidence exist?
- How is performance monitored?
- What happens after incident, material change or exit?
- Can the offer still be delivered if they fail?

The consortium partner's account was eventually removed. The more important change came earlier. Partner withdrawal became a trigger in the pursuit process. The partner manager updated status, the identity owner removed access, the solution lead assessed impact and the bid manager controlled information return.

Nobody had to assume IT would know.

The system told it.

CHAPTER 15

Assurance, Review, Release and Secure Submission

CASE FILE

The security response had been reviewed by six people.

One corrected the spelling of authorisation. One changed the font in the architecture table. Two added references to their departments. The chief technology officer replaced reduces risk with eliminates risk because he thought the earlier wording sounded uncertain.

Nobody checked whether the certificate attached to the response covered the service being offered.

It did not.

The review had generated activity. Assurance had not occurred.

Define what the review is meant to establish

A security review may have several jobs:

- confirm customer and contractual requirements;
- assess risk and treatment;
- challenge architecture and service design;
- verify factual claims and evidence;
- validate operation under realistic scenarios;
- assess provider and cloud responsibilities;
- check privacy, legal or regulatory position;
- reconcile security commitments with price;
- evaluate the answer as an evaluator;
- confirm release and submission readiness.

Do not call all of these security review and invite everyone to one meeting.

Set purpose, scope, maturity, criteria, reviewers, inputs, outputs, finding method, closure and decision authority.

Security assurance is evidence-based confidence

Assurance is not absolute proof that no incident can occur. It is a reasoned level of confidence that requirements and controls are understood, designed, implemented or planned appropriately, and supported by evidence.

Evidence may come from:

- management-system certification;
- independent audits;
- technical testing;

- control operation records;
- architecture and design review;
- supplier assurance;
- risk assessment and SoA;
- incident and recovery exercises;
- competence evidence;
- customer references;
- internal verification;
- management decisions.

Match evidence to the claim.

An ISO/IEC 27001 certificate can support confidence in the management system within scope. It does not replace a technical assessment of a new customer integration. A penetration test can support confidence in the tested system at a point in time. It does not prove every operational control in the service.

Certificate verification

Before using a certificate, confirm:

- legal entity;
- certificate number;
- standard and edition;
- scope wording;
- sites or boundaries;
- issue, expiry and status;
- certification body;
- accreditation where claimed;
- relevance to the offered service;
- any transition or suspension issue.

Use authoritative verification routes where available. Do not trust a cropped logo or marketing statement.

A certificate may be valid and irrelevant. A parent company may be certified while the bidder operates outside scope. A cloud provider may be certified for infrastructure services while the proposed application falls under the customer's configuration responsibility.

Write the relationship accurately.

Statement of Applicability and sensitive evidence

Customers sometimes request the SoA or detailed control evidence. Decide what can be shared, at what level and under which protections.

A full SoA may reveal control gaps, architecture, providers or internal references. A proportionate response may provide a controlled extract, summary, relevant control mapping or access under confidentiality.

Do not refuse automatically and do not disclose automatically.

Assess customer requirement, procurement fairness, confidentiality, security and commercial impact. Record approval. Redact carefully without changing meaning.

Review entry criteria

Before a security review begins, confirm that the work is mature enough for the question.

For a solution-security review, entry criteria may include:

- current customer security requirements;
- risk assessment and treatment position;
- proposed architecture and information flows;
- provider responsibilities;
- data and privacy assessment;
- identity and access model;
- incident, continuity and recovery approach;
- commercial assumptions;
- known gaps and decisions.

For a near-final response review, add:

- complete draft;
- current evidence;
- verified certificates and claims;
- reconciled price;
- approved residual risk;
- word and format compliance;
- material provider commitments;
- review brief and scoring criteria.

If inputs are missing, change the review purpose or delay it. Pretending the draft is ready wastes reviewer attention and creates false closure.

Reviewer competence and independence

Choose reviewers for the risk and question.

Possible competence includes:

- ISMS and ISO/IEC 27001;
- cyber and technical architecture;
- privacy and data protection;
- procurement and tender evaluation;
- legal and contract;
- cloud and supplier risk;
- secure development;
- business continuity;
- operational delivery;
- accessibility and production.

One person will rarely cover everything.

Independence is proportional. The solution architect may verify technical accuracy but should not be the only person challenging their own design. A small business may use cross-review or competent external support.

A senior title is not an assurance method.

Brief the reviewer

Provide:

- review purpose;
- customer context and criteria;
- information classification;
- scope and exclusions;
- maturity expected;
- known risks and assumptions;
- evidence available;
- finding severity;
- time and access;
- secure handling;
- closure and escalation route.

Tell reviewers whether they may download, print or use external tools. Review itself can create information risk.

A reviewer who copies restricted material into a personal annotation service has weakened the control while trying to assess it.

Score confidence before editing

Ask evaluator-style reviewers to record what the text allows them to conclude before proposing wording.

For each material section:

- likely score or confidence;
- direct evidence in the response;
- unresolved doubt;
- security or delivery consequence;
- severity;
- most valuable correction.

This separates an assurance gap from stylistic preference.

Weak comment:

> **WORKING WORDS**
>
> Add more detail on access control.

Useful finding:

> **WORKING WORDS**
>
> The answer states that access is role-based but does not define who approves roles, when guest access expires or how privileged activity is reviewed. The evaluator cannot determine whether access remains controlled through mobilisation and supplier change. Major finding against security criterion 2.3.

The second finding can be owned and verified.

Finding severity

Use a simple, understood scale.

Critical: likely non-compliance, false or materially misleading statement, unacceptable exposure, inability to meet a security requirement, or release of information through an unsafe route.
Major: substantial loss of score or confidence, unsupported key control, important design or supplier weakness, unresolved high risk, or inconsistency affecting delivery.
Minor: local clarity, evidence, traceability or presentation weakness with limited consequence.
Observation: improvement opportunity or preference not required for release.

Define which findings block progression. A critical open finding should not become minor because the deadline is close.

Risk acceptance must have authority and evidence.

Verification of the response

Verification checks whether the output meets its inputs and defined criteria.

Check:

- all security requirements addressed;
- clause, schedule and contract positions consistent;
- risk treatments represented accurately;
- SoA claims correct;
- certificate scope and status verified;
- control descriptions match actual service;
- provider responsibilities confirmed;
- figures, periods and populations defined;
- architecture, narrative and price aligned;
- incident and continuity timing consistent;
- personal data minimised;
- classifications and handling followed;
- AI and external-provider use controlled;
- commitments approved;
- required evidence included;
- final files match approved content.

Automation can help compare names, dates, retention periods, service levels, provider names and claims. It does not decide whether the security model is sufficient.

Validation of the secure offer

Where proportionate, test whether the proposed service can achieve intended secure use.

Methods may include:

- architecture threat review;
- tabletop incident exercise;
- access-provisioning walkthrough;
- recovery or failover test;
- technical demonstration;
- penetration or configuration testing;
- secure development evidence review;
- supplier scenario;
- mobilisation rehearsal;
- data-deletion test;

• user and administrator test.

The result may cause redesign.

At Kestrel Public Services, the incident exercise showed that the proposed customer notification depended on a security manager who was not on call. The bid promised one-hour initial notification at all times. The team funded an on-call duty route, updated the incident matrix and tested it again.

The promise became operational before it became contractual.

Closure requires evidence

For each critical or major finding, record:

- finding and source;
- requirement or risk;
- severity;
- owner;
- action;
- affected outputs;
- due date;
- verifier;
- closure evidence;
- residual risk and acceptance.

Resolved in meeting is rarely enough.

If the finding concerns certificate scope, closure may be the verified certificate and corrected wording. If it concerns access design, closure may be an approved model and provider confirmation. If it concerns price, closure requires a revised commercial baseline and approval.

The person correcting the issue should not always verify closure.

Gold review is not a licence to improvise

An executive or final review should confirm strategy, material commitments, residual risk, commercial position and readiness. It should not introduce unreviewed security promises because the existing language feels modest.

Set change control after content freeze. Any material change affecting security scope, timing, architecture, risk, supplier, price or customer dependency must return to appropriate owners.

The chief technology officer's change from reduces to eliminates at the start of this chapter would have required evidence that the risk could be removed entirely. None existed.

The wording returned to reduces, with the actual control and residual risk explained.

Production can damage security and meaning

Final production may expose or alter information through:

- hidden comments and tracked changes;
- document properties;
- embedded files;
- broken redaction;
- inaccessible or unreadable diagrams;
- missing pages;

- converted symbols;
- altered links;
- unprotected working copies;
- incorrect file names;
- temporary cloud converters;
- unapproved compression tools.

Use approved production systems. Inspect the rendered output. Compare with approved source. Remove hidden content. Check metadata and attachments. Protect temporary files and dispose of them under the retention rule.

A black rectangle over text is not necessarily redaction. Ensure the underlying content is removed where true redaction is needed.

Release criteria

Release is the authorised decision that the exact output is suitable for submission.

Criteria may include:

- current document baseline used;
- mandatory security schedules complete;
- requirements independently verified;
- risk assessment and treatment current;
- residual risk approved;
- claims and certificates verified;
- provider commitments confirmed;
- price and security model reconciled;
- critical and major findings closed or accepted by authority;
- personal and customer data handled correctly;
- final files inspected and secure;
- portal route rehearsed;
- submission manifest complete;
- authorised uploader and deputy available;
- incident and contingency routes active.

The release record should identify the exact files and versions.

Do not sign a generic checklist on Thursday and create different files on Friday.

Submission identity and device

Use named authorised accounts, approved devices and supported browsers. Confirm multi-factor authentication, permissions and access before the final day.

Avoid shared credentials. They weaken accountability and may breach portal terms. Maintain a deputy with their own authorised access.

Where submission information is particularly sensitive, check device compliance, network route, physical environment and screen privacy. Do not submit a restricted pack over hotel Wi-Fi because the office connection failed and nobody designed a fallback.

The submission manifest

List:

- lot or response area;

- exact filename;
- format and size;
- classification;
- approved source and version;
- checksum where proportionate;
- required portal field;
- upload status;
- uploader;
- independent verifier.

The manifest connects release to the portal.

It also supports incident reconstruction. If the customer later asks what was submitted, the organisation should not rebuild the answer from browser history.

File integrity and checksums

For higher-risk submissions, use hashes or other integrity checks to confirm that the uploaded file matches the released baseline. A checksum does not prove the content is correct. It proves the file is unchanged relative to the calculated version.

Record the algorithm and value, and protect the manifest.

For lower-risk bids, controlled naming, read-only storage and independent visual verification may be sufficient. Risk chooses depth.

Submit with protected contingency

Upload before the external deadline and preserve time for:

- file rejection;
- portal delay;
- account lockout;
- conversion issue;
- missing field;
- support contact;
- controlled correction.

Do not consume contingency through planned drafting.

During upload, restrict changes. One person uploads. Another verifies against manifest. A decision authority remains available. Other team members do not create alternative final packs unless instructed through control.

Secure receipt and archive

After submission:

- confirm portal status;
- obtain receipt or reference;
- compare portal contents with manifest;
- retain exact submitted files;
- preserve approval and risk records;
- restrict archive access;
- maintain availability for clarification;
- remove unnecessary live access;

• apply retention and disposal.

A submitted bid may need to remain available for challenge, audit, contract and learning. It also contains information that should not stay in every participant's downloads folder.

Close the live workspace deliberately.

What if the portal fails?

Follow the customer's published route. Preserve timestamps, screenshots, error messages and support communications. Do not invent email submission unless authorised.

Use rehearsed contingency files and connections. If a file must be changed, control the source, impact, approval, reproduction and reverification.

Do not lower resolution until an architecture diagram becomes unreadable. Do not remove an attachment because it is large. Escalate while options remain.

Security incident during submission

An incident may occur at the same time as the deadline: phishing message, compromised account, lost device, malicious file or accidental disclosure.

Security consequence can outrank submission urgency.

Activate the incident process. Contain exposure. Protect evidence. Decide whether credentials or files remain trustworthy. Notify the customer where required. Use alternative authorised routes only if safe and permitted.

The decision should be made by defined authority, not by the person nearest the keyboard.

Assurance performance

Measure whether reviews and release controls work:

- reviews held at defined maturity;
- security findings by severity and source;
- repeated findings;
- closure time;
- claims corrected after review;
- provider discrepancies;
- post-freeze security changes;
- release exceptions;
- submission incidents;
- internal confidence versus evaluator feedback;
- mobilisation issues linked to missed findings.

A falling number of findings may indicate improvement or weak challenge. Compare with later results.

Quality test - could the assurance decision be defended?

Choose one released security response.

- Which requirements and criteria governed review?
- Who reviewed, and why were they competent?
- What evidence supported the main claims?
- Which risks remained?
- How were providers and price reconciled?

- Which critical or major findings were raised?
- What proved closure?
- Who accepted residual risk?
- Which exact files were released?
- Did the portal receive those files?
- What receipt and integrity evidence remains?

The certificate at the start of this chapter was removed. The bidder obtained the correct certificate for a different group entity and explained that the proposed service would operate within that certified scope only after a planned organisational change. That was not sufficient for the current tender.

The team therefore described its existing control environment honestly, provided other relevant assurance and marked the certification commitment as future treatment rather than present fact.

The answer lost one convenient sentence.

It gained a position the organisation could defend.

CHAPTER 16

Clarification, Negotiation, Incident and Handover

CASE FILE

The authority's clarification contained one sentence.

The account director replied from his phone.

The incident plan used a four-hour initial assessment window. The subcontractor contract used twenty-four hours. The price included business-hours cover.

The reply was still sitting in Drafts when the bid manager saw it.

Thirty minutes had almost become a contractual service without risk, design, supplier or commercial review.

Post-submission communication remains controlled work

Submission does not end the ISMS boundary around the pursuit. Clarifications, presentations, demonstrations, negotiation, best-and-final offers, award notices and contract finalisation can change information, risk and commitment.

Control each customer request against the submitted baseline.

Record:

- source and authority;
- deadline and communication route;
- information classification;
- affected requirement and answer;
- effect on security design, risk, price, provider and contract;
- owner and contributors;
- approval and release;
- new or changed commitment;
- receipt and retained record.

A two-line email may create more security exposure than a forty-page method statement.

Clarify without redesigning in secret

A clarification response should explain the submitted position or provide permitted information. If the customer allows change, control it openly.

Before answering, ask:

- What exactly is being requested?
- Does the submitted answer already contain the position?
- Is the question exposing ambiguity, inconsistency or nonconformity?
- Would the response change scope, timing, architecture, risk or price?

- Does a supplier or customer dependency change?
- Is new approval required?
- Will the response become contractual?

The incident-notification question at the start of this chapter required an integrated decision. The team could not confirm thirty minutes honestly. It proposed a thirty-minute acknowledgement and a risk-based initial assessment within the existing controlled window, subject to the customer's acceptance and the final contract.

The answer was longer than Confirmed and considerably cheaper than discovering the difference during an incident.

Presentations expose the operating model

A presentation or demonstration is not a relaxed version of the written bid. Evaluators may test security understanding, people, systems and response under pressure.

Plan:

- permitted attendees;
- access to customer information;
- approved slides and demonstrations;
- environment and data;
- questions and decision authority;
- live commitments;
- screen sharing and recording;
- physical and remote security;
- contingency;
- follow-up and retained evidence.

Use representative or synthetic data unless real customer information is necessary and approved. Clean demonstration environments. Disable unrelated notifications. Check that browser bookmarks, recent files and chat messages will not appear during screen sharing.

The most advanced encryption claim can be undermined by a presenter's desktop revealing another customer's folder.

Rehearse ordinary security questions

Prepare for questions such as:

- Who approves administrator access?
- What happens if the named security lead is unavailable?
- How quickly will you tell us about a suspected incident?
- Where are backups stored and when were they restored?
- Which subcontractors can access our data?
- What happens when the cloud provider changes a service?
- How do you remove a departing user?
- Which part of the solution is outside your certificate scope?
- How will you prove deletion at exit?

Train participants to say I do not know; I will confirm through the formal route where that is the truthful position.

An invented answer delivered confidently in a presentation remains invented.

Negotiation changes risk

Negotiation may alter:

- liability and indemnity;
- incident notification;
- audit and assurance;
- data location;
- retention and deletion;
- security testing;
- service levels;
- supplier rights;
- customer responsibilities;
- intellectual property;
- price and resource;
- mobilisation and exit.

Prepare authority before the meeting.

Define:

- objectives;
- red lines;
- positions that may be exchanged;
- approval levels;
- cost and risk impact;
- note-taking;
- change control;
- confirmation route.

Do not reduce price while keeping every security control and service level unchanged unless a real efficiency supports the reduction. Do not accept an audit right the supplier chain cannot honour. Do not promise data deletion on a timescale that conflicts with legal retention.

Best-and-final offer

A revised offer should be treated as a new controlled baseline where material changes occur.

Reconcile:

- customer request;
- risk assessment;
- SoA and treatment;
- architecture;
- providers;
- price;
- contract;
- security answers;
- evidence;
- release;
- handover.

A final discount entered directly into the pricing workbook can change staffing and monitoring capability even when no security paragraph changes. Assess the service effect.

Incident during the pursuit

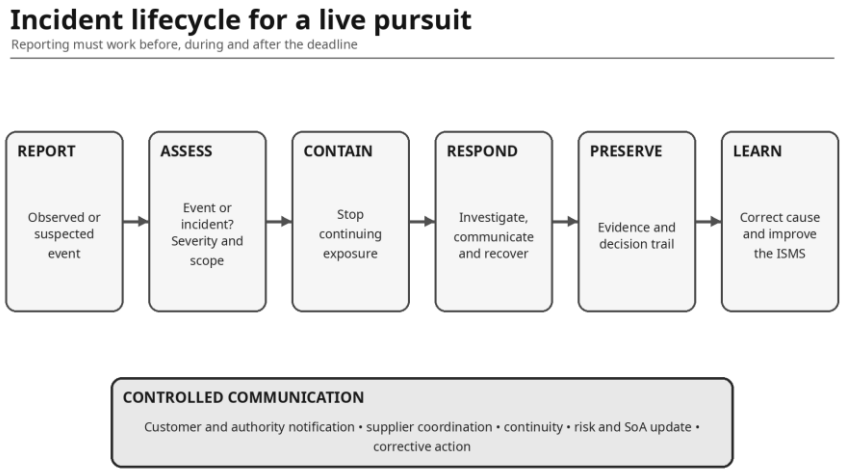

Figure 8 - The incident route from event detection through decision, response, recovery and learning.

Bid-related incidents may include:

- misdirected email;
- compromised account;
- lost device;
- malware in a tender file;
- unauthorised workspace access;
- personal data exposed;
- confidential material used in an AI service;
- supplier breach;
- corrupted pricing or response file;
- deliberate leakage;
- portal impersonation or phishing;
- loss of availability near deadline.

People need a reporting route that works during pressure.

The first response is not to protect the bid's appearance. It is to protect information, customer and evidence.

Event or incident?

Not every event is an incident. The organisation should define criteria for assessment and decision.

Consider:

- information and scope;
- actual or possible effect on confidentiality, integrity or availability;
- customer and legal requirements;

- scale and duration;
- threat and continuing exposure;
- affected people and services;
- evidence available;
- need for escalation or notification.

A suspicious login may be contained without confirmed compromise. A misdirected email may be recalled but still constitute unauthorised disclosure. A corrupted draft may be a local error or evidence of malicious activity.

Use competent assessment. Record the decision.

Incident response needs authority

Define who can:

- contain access;
- isolate devices or systems;
- stop work or submission;
- contact the customer;
- notify regulators or authorities;
- engage specialists;
- preserve evidence;
- approve recovery;
- accept temporary risk.

The bid manager may coordinate the pursuit. The security incident lead should direct technical containment. Legal and privacy advisers may determine notification obligations. Top management may need to decide commercial and customer action.

Roles should meet before the event, not in the forwarding chain afterwards.

Preserve evidence

Incident handling may require logs, emails, device data, file versions, access records, screenshots, witness accounts and timelines.

Preserve integrity and chain of custody proportionately. Avoid altering evidence through casual investigation. Restrict access. Record who collected what, when, where and how.

Serious events may require specialist forensic or legal support.

A bid team should not attempt amateur forensic work on a customer-sensitive incident merely because one person understands spreadsheets.

Customer and regulatory communication

Notify through applicable legal, regulatory, contractual and customer routes. Timing may begin from awareness, detection, confirmation or another defined event. Understand the actual wording.

Prepare factual communication:

- what is known;
- what remains unknown;
- information and services affected;
- immediate containment;
- current risk;

- actions and next update;
- contact and authority.

Do not speculate. Do not delay solely to produce a perfect explanation.

The tender may itself require notification of bid-stage incidents. Check the documents.

Learn without exposing more information

After containment and recovery, examine cause and control performance. Share learning at the level needed for improvement without distributing sensitive incident details unnecessarily.

Update:

- risk assessment;
- SoA and controls;
- supplier requirements;
- awareness;
- tooling;
- access;
- incident playbooks;
- bid procedures;
- evidence and customer communication;
- management review.

An incident lesson stored only in the security team's restricted archive cannot improve the bid process unless a controlled action reaches it.

Award activates a security transition

On award, transfer the complete security position into mobilisation.

Include:

- final submitted security responses;
- clarifications and negotiation;
- contract and security schedules;
- information classification and customer rules;
- risk assessment and treatment;
- relevant SoA position;
- architecture and information flows;
- identity and access model;
- provider commitments;
- security promises and measures;
- incident, continuity and recovery;
- testing and assurance;
- personal-data responsibilities;
- open assumptions and decisions;
- evidence and reporting;
- retention and exit.

Delivery should accept the handover. A meeting invitation is not acceptance.

The security promise register

Extract material commitments with:

- exact wording and source;
- requirement;
- control and risk;
- owner;
- implementation date;
- measure and evidence;
- resource and price;
- provider dependency;
- customer dependency;
- reporting;
- incident or exception route;
- contract location;
- status.

Security questionnaires often contain commitments that do not appear in the main contract schedule. The promise register exposes them.

At Waverley Managed Services, the register contained 164 security commitments. Thirty-seven required action before contract start. Twelve depended on the customer. Seven referred to a supplier agreement still under negotiation.

The mobilisation plan had previously shown one line: `Complete security onboarding.`

That line was retired.

Access transition

Mobilisation creates new identities and access. Control:

- role and need;
- customer approval;
- screening or clearance;
- authentication;
- privileged access;
- devices and locations;
- supplier identities;
- start and expiry;
- review;
- emergency access;
- removal after change.

Do not clone the bid workspace into delivery and keep everyone. Bid participants may have had access for response development that is unnecessary after award.

Close pursuit access while opening service access through the correct route.

Information transfer and archive

Move only necessary records into delivery systems. Preserve the submitted baseline and audit trail in the controlled archive. Avoid transferring every draft and comment into operational spaces.

Classify and retain:

- contractual records;
- evidence of commitments;

- risk and design decisions;
- customer information;
- personal data;
- provider evidence;
- incidents;
- bid learning.

Dispose of working copies according to policy and customer requirements. Confirm partner deletion where required.

The handover should not create another uncontrolled copy universe.

Unsuccessful result

A loss, cancellation or delay still requires security closure.

- preserve the formal result;
- decide whether legal or procurement review is required;
- retain the submitted baseline;
- remove unnecessary access;
- return or delete customer information;
- close supplier access and obligations;
- retain permitted evidence and learning;
- review incidents or near misses;
- update risks and controls;
- maintain appropriate customer confidentiality.

Do not keep the complete data room because the opportunity may return in three years. Retention needs a lawful and business basis.

Post-award assurance

Within the first thirty, sixty and ninety days, compare the tender security position with reality.

Ask:

- Were access and screening completed as promised?
- Did providers deliver required controls?
- Are logs, backups and monitoring operating?
- Have incidents or exceptions occurred?
- Are customer dependencies being met?
- Are security measures and reports available?
- Which tender assumptions were wrong?
- Which controls are difficult or underfunded?
- Which evidence can support future bids?

Correct discrepancies before they become contract failure.

The clarification audit

Select one post-submission question and trace:

- customer request;
- submitted baseline;
- impact assessment;
- security, supplier and commercial input;

- approval;
- final response;
- changed commitment;
- receipt;
- handover.

Then select one award commitment and ask delivery to explain it without help from the bid team.

If the delivery owner first sees the wording during the audit, the handover was ceremonial.

Quality test - what changed after submission?

For one completed pursuit, list every change after initial submission:

- clarification;
- presentation answer;
- demonstration result;
- negotiated term;
- best-and-final price;
- provider change;
- incident;
- contract clarification;
- mobilisation decision.

For each, identify who approved the security and commercial effect and where delivery received it.

The thirty-minute notification at the start of this chapter never left the phone. The team answered through the formal route, revised its incident design and negotiated supplier support. The final contract required prompt acknowledgement and defined staged notification based on severity and available facts.

The account director still attended the presentation.

He no longer had authority to answer security commitments from memory.

CHAPTER 17

The Organisational Control Arsenal - Annex A.5

CASE FILE

At 09:24, the bid team opened Annex A and began assigning controls to departments. Access went to IT. Supplier security went to Procurement. Privacy went to Legal. Physical security went to Facilities. The bid manager was relieved because every control now belonged somewhere else.

At 10:06, somebody asked who controlled the confidential tender pack already sitting in the pursuit workspace.

The room became less departmental.

The thirty-seven organisational controls in Annex A provide a reference set for governance, information, suppliers, incidents, continuity, compliance and operating practice. They do not replace risk assessment and they are not all automatically necessary. When selected, however, they should live through the processes that actually handle information. The following sections paraphrase each control and place it inside bid and proposal work.

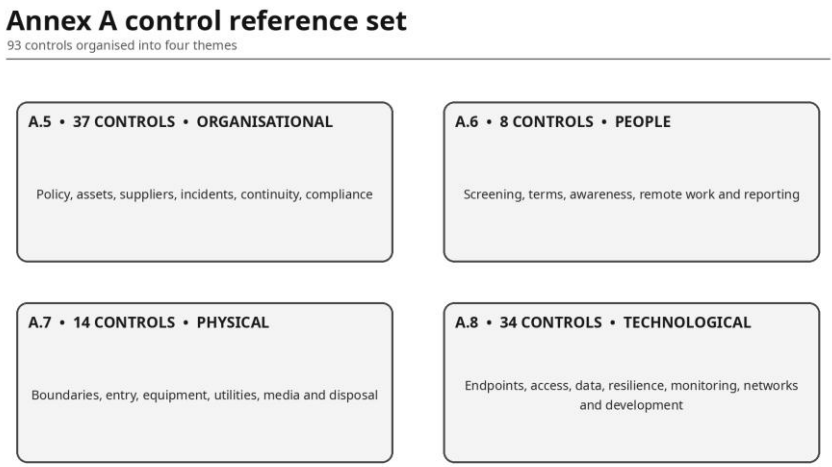

Figure 9 - Annex A contains 93 controls grouped into organisational, people, physical and technological themes.

A.5.1 - Govern the information-security policy framework

Set approved direction for information security and the supporting topic-specific rules. In bid work, policy should reach classification, access, remote working, supplier use, AI, incident reporting, retention and secure submission. It should be reviewed when the organisation, threat environment, customer requirements or standards change.

A practical pursuit pack links the relevant policy rules at kick-off rather than attaching a forty-page policy nobody opens. Evidence may include approval, review history, staff awareness and decisions that follow the policy.

Failure appears when the tender claims strong governance while the live bid uses personal storage, broad access and unapproved tools. The policy exists, but the operating route teaches something else.

A.5.2 - Assign security roles and accountabilities

Define who owns information, risk, access, incident response, supplier assurance, technical design, privacy, release and handover. Responsibility should include authority. A bid manager can coordinate the campaign without becoming the owner of every security decision.

Use a role and authority matrix showing deputies and escalation. Retain risk ownership, access approval, security review and release decisions.

The common failure is a RACI crowded with contributors and empty of decision rights. When the security lead is absent, nobody knows who may accept residual risk or stop submission.

A.5.3 - Separate incompatible duties

Reduce the chance that one person can create, approve and release a material security position without challenge. Proportionality matters: a small firm may use cross-review or external assurance rather than a large segregation model.

Separate author from independent reviewer where possible; separate commercial model ownership from final approval; require a second person to verify portal contents; prevent workspace administrators from approving their own privileged access.

Failure occurs when the same person grants access, uploads the file and confirms that the upload was correct. The process may be fast. It cannot independently detect its own mistake.

A.5.4 - Make managers responsible for secure behaviour

Managers should ensure people follow information-security requirements relevant to their work. That includes resourcing, local briefing, access discipline, safe challenge and response when controls are bypassed.

Evidence is visible in workload decisions, corrected unsafe practice, role briefings, removal of unapproved tools and action after near misses.

A manager who signs the policy and then asks a writer to use a personal account because the approved platform is slow has issued the real instruction.

A.5.5 - Maintain contact with competent authorities

Identify which authorities may need to be contacted for incidents, legal obligations, cyber threats or sector requirements. The exact route depends on jurisdiction, industry and event.

A bid-stage incident plan should state who decides whether to contact law enforcement, regulators, the NCSC, a contracting authority or another competent body, and how evidence is preserved.

Do not search for the correct authority during the first hour of a serious incident. Equally, do not notify externally without defined authority and competent legal or regulatory assessment.

A.5.6 - Use relevant security communities and specialist groups

Maintain contact with professional groups, sector forums, trusted communities and specialist advisers that improve awareness of threats, practice and obligations.

For pursuit teams this may support current knowledge on public-sector security expectations, cloud risk, vulnerability disclosure, supplier assurance or secure development. Record how information is assessed before it changes the ISMS.

Membership logos are not threat intelligence. The control works when useful external knowledge changes a risk, design, training or response.

A.5.7 - Operate a threat-intelligence process

Collect and analyse information about relevant threats so that it becomes actionable. Intelligence should be timely, contextual and connected to assets and decisions.

A high-risk technology bid may need current knowledge about sector attacks, exploited vulnerabilities, supplier compromise, phishing campaigns or threats to the proposed platform. The output may change treatment, architecture, monitoring or bid/no-bid.

Copying a weekly threat bulletin into a folder is collection, not intelligence. Ask what changed because the organisation learned it.

A.5.8 - Build security into project and pursuit management

Information security should be integrated into projects, programmes and pursuits from initiation through closure. Security requirements, risks, responsibilities and assurance should appear in the plan rather than arrive at final review.

Use security gates, risk actions, secure workspaces, design reviews, supplier checks, incident routes, release criteria and handover. Scale depth to the opportunity.

The failure pattern is familiar: the security questionnaire lands with IT three days before submission, after solution and price have already been fixed.

A.5.9 - Maintain an inventory of information and supporting assets

Know which information and associated assets exist within scope, who owns them and where they are located. The inventory may be federated rather than one giant spreadsheet.

For a pursuit, inventory source documents, workspaces, datasets, pricing models, credentials, devices, providers, AI tools, final files and archives. Link classification, owner, retention and access.

A file cannot be protected or deleted reliably when the organisation does not know that a partner downloaded it or that a local copy exists.

A.5.10 - Define acceptable use

State how information and associated assets may and may not be used. Rules should cover devices, email, storage, printing, collaboration, personal accounts, AI, customer systems and removable media as relevant.

Make bid-specific restrictions visible at kick-off and in provider briefs. Provide a workable authorised route.

A prohibition that requires three days to obtain secure file transfer will be tested by a deadline in three hours. Acceptable use must be supported by usable systems.

A.5.11 - Recover or account for assets at the end of access

Ensure information, devices, credentials and other assets are returned or otherwise accounted for when employment, assignment, supplier work or pursuit participation ends.

Remove guest access, recover loan devices and tokens, transfer records, confirm deletion of controlled copies and preserve continuing obligations.

The control fails when a consultant leaves the project but retains downloaded tender material because offboarding only disabled the corporate account.

A.5.12 - Classify information by consequence and requirement

Classify information according to confidentiality, integrity, availability, legal, contractual and business needs. The scheme should guide treatment rather than decorate documents.

Bid classifications may distinguish public notices, internal strategy, customer-confidential material, personal data, privileged legal advice and restricted technical information. Map customer labels to internal handling.

Everything marked Confidential creates noise. Nothing marked Confidential creates exposure. The label should change access, transfer, storage, retention or review.

A.5.13 - Label information so people can handle it correctly

Apply labelling appropriate to the classification and medium. Labels may appear in document headers, metadata, workspace status, email subject conventions or system tags.

Provide clear instructions for inherited customer labels and for files that cannot carry visible markings, such as pricing workbooks or portal fields.

A label is ineffective when external contributors do not understand it or when it remains after a document has been properly sanitised for public use.

A.5.14 - Control information transfer

Protect information transferred internally and externally, including email, collaboration links, APIs, physical media, messaging and verbal exchange.

Define approved routes, recipient checks, encryption where needed, access expiry, transfer records, supplier rules and incident response. Verify unusual destinations and high-risk attachments.

The ordinary failure is the correct file sent securely to the wrong Martin. Technology helps; recipient and purpose checks still matter.

A.5.15 - Establish access-control principles

Set rules for physical and logical access based on business need, least privilege, segregation, classification and risk. The policy should cover normal, privileged, temporary and emergency access.

In the bid room, access should follow role, question, information class and campaign stage. Customer or legal restrictions may require tighter boundaries.

Broad access granted because the deadline is near becomes the permanent position unless expiry and review are designed.

A.5.16 - Manage identities through their lifecycle

Create, change, review and remove identities in a controlled way. Identities should be unique where accountability matters, including external users and service accounts.

Link onboarding and offboarding to the pursuit roster, partner status and role changes. Control shared and non-human identities separately.

A dormant guest account is not harmless because the partner has stopped attending meetings. The identity remains a route until the system closes it.

A.5.17 - Protect authentication information

Manage passwords, tokens, keys, recovery codes and other authentication information securely through issue, use, storage, reset and disposal.

Avoid credentials in bid documents, chat or shared spreadsheets. Use approved password or secrets management and separate emergency recovery.

The portal password taped into the upload checklist may solve availability for one afternoon and create an accountability problem for months.

A.5.18 - Provision, review and remove access rights

Authorise access rights, review them at suitable intervals and after change, and remove them promptly when no longer needed.

For live pursuits, review guest and privileged access at gates, after supplier change, at submission and at closure. Retain approval and review evidence.

The access list should show why a person still needs the information, not merely that the platform allows them to see it.

A.5.19 - Manage security risk in supplier relationships

Identify and address information-security risks arising from suppliers and other external parties. Risk depth should follow access, criticality, service and customer requirement.

Bid-related suppliers include freelance writers, designers, hosting providers, proposal platforms, data-room services, AI tools and delivery partners.

The failure is approving a supplier because another department already uses it, without examining the different information and purpose in the pursuit.

A.5.20 - Put security requirements into supplier agreements

Agreements should contain relevant information-security requirements, responsibilities and assurance. Cover access, confidentiality, incidents, subcontracting, locations, continuity, return, deletion and customer flow-down as needed.

Requirements must be understood by both parties and reconciled with the prime bid. Retain signed terms and approved exceptions.

A one-hour customer notification cannot be supported by a supplier contract allowing notice within twenty-four hours unless another control closes the gap.

A.5.21 - Address security across the ICT supply chain

Manage risks from technology components, service dependencies, development chains, updates and concentration. Understand critical suppliers and relevant downstream dependencies.

In a bid, ask how proposed platforms, libraries, hardware, telecommunications and managed services are sourced, supported, changed and monitored.

A supplier certificate gives assurance within scope; it does not reveal every component dependency or guarantee future availability.

A.5.22 - Monitor supplier performance, assurance and change

Review supplier services and security performance, and control material change. Use incidents, reports, certifications, vulnerabilities, service reviews and contract evidence.

Reassess when ownership, location, subprocessors, architecture, control scope or customer requirements change. Update bid claims accordingly.

The provider approved last year may no longer deliver the same service. Current tender evidence needs a current provider position.

A.5.23 - Govern acquisition, use and exit from cloud services

Manage cloud services through the full lifecycle. Define service ownership, shared responsibilities, data classes, regions, identities, configuration, logging, incident, continuity, change and exit.

This applies to the offered solution and to cloud tools used to produce the bid. The same SaaS platform may have different risks under different use cases.

Cloud certification does not configure the tenant. A secure provider can host an insecurely managed customer environment.

A.5.24 - Prepare for information-security incidents

Establish incident roles, plans, priorities, communications, resources, evidence routes and exercises before an event. Coordinate technical, legal, privacy, customer and business decisions.

The pursuit incident plan should include misdirected files, compromised accounts, malicious tender content, supplier incidents and portal disruption.

A phone tree last checked three years ago is not preparation. Test a realistic bid-stage scenario and record what failed.

A.5.25 - Assess events and decide whether they are incidents

Define how reported or detected events are assessed, classified and escalated. Use impact, information, scope, threat, customer obligation and continuing exposure.

Record the decision and authority. Not every suspicious event is a confirmed incident, but uncertainty may still require containment.

The control fails when every event is ignored until harm is proven, or when every anomaly triggers the same crisis response.

A.5.26 - Respond to incidents under controlled authority

Contain, investigate, communicate, recover and record incidents using planned procedures. Protect customer interests and business continuity.

Bid operations should know who may stop submission, revoke access, contact the customer and approve recovery. Supplier routes must align.

Urgency is not permission for five people to investigate the same account and destroy the evidence trail.

A.5.27 - Learn from incidents

Use incident causes, response performance and consequences to improve controls, risk assessment, awareness and design.

Feed learning into qualification, supplier onboarding, workspace rules, AI use, review and handover. Share only the detail needed for action.

A lessons report stored in a restricted incident folder does not improve bidding unless controlled changes reach the people and process.

A.5.28 - Collect and preserve evidence

Define methods for identifying, collecting, acquiring and preserving evidence in a manner suitable to the potential legal, disciplinary, contractual or technical use.

Relevant evidence may include logs, emails, file versions, access records, devices, screenshots and timelines. Use competent support for serious cases.

Casual copying, editing or opening of evidence may change metadata or integrity. The first person curious about the incident should not become the forensic method.

A.5.29 - Maintain security during disruption

Plan how essential security controls continue during disruption. Decide minimum controls, temporary arrangements, authority and return to normal.

A bid team working through platform outage still needs controlled files, identities, communications and release. The fallback should not be personal email and unmanaged storage.

Continuity that preserves productivity but abandons confidentiality or integrity has solved only one part of the problem.

A.5.30 - Ensure ICT can support continuity requirements

Plan, implement, maintain and test ICT readiness based on business continuity needs. Align recovery capability with required times and dependencies.

For critical pursuits and services, identify collaboration, identity, communication, backup, portal and provider dependencies. Test restoration and alternate routes.

A backup that has never been restored is a hope stored on another system.

A.5.31 - Identify and comply with legal, regulatory and contractual duties

Maintain a process for identifying, accessing and meeting applicable security obligations. Requirements vary by jurisdiction, sector, customer and information.

The register should connect obligations to controls, owners, evidence and change monitoring. Tender and contract requirements belong in the same operational route.

Copying a generic list of laws into the ISMS is not compliance. Show which duty changed a process, retention rule, notification route or design.

A.5.32 - Protect intellectual-property rights

Respect ownership, licences, copyright, trade secrets and contractual rights in software, documents, data, methods and third-party material.

Bid teams should control reuse of customer content, competitor material, licensed standards, images, source code and partner evidence. Define rights in external contributor agreements.

A previous customer's diagram remains protected even after the company name is removed.

A.5.33 - Protect records

Protect records from loss, destruction, falsification, unauthorised access and premature disposal. Retention should reflect legal, contractual, business and evidential needs.

Bid records include released submissions, approvals, risk decisions, receipts, clarifications, incidents, contracts and audit trails. Ensure readability and retrieval over the period.

Keeping every draft forever is not records protection. It can conceal the authoritative record and extend unnecessary exposure.

A.5.34 - Protect privacy and personal information

Identify and meet privacy and personal-data requirements through governance, design, access, minimisation, accuracy, retention, transfer and rights handling.

Bids involve CVs, references, user data, demonstrations and customer datasets. Align privacy roles with security controls and customer commitments.

A security answer can be technically strong and still fail because personal data was collected or reused without a valid and transparent basis.

A.5.35 - Obtain independent review of information security

Review the organisation's security approach independently at planned intervals and after significant change where appropriate. Independence should match scope and risk.

Use internal audit, external specialists, certification audits, technical assurance or peer review. Findings should reach management and corrective action.

The architect explaining that their own design is secure is useful input. It is not independent assurance.

A.5.36 - Check compliance with security policies and standards

Managers and control owners should review whether relevant policies, rules and standards are followed, and correct deviations.

Sample live pursuits: access, classification, AI use, supplier onboarding, retention and release. Distinguish approved exception from silent bypass.

The audit should not begin and end with whether a policy was signed. Follow the information through the actual work.

A.5.37 - Maintain clear operating procedures where needed

Document procedures for activities whose consistent and secure performance depends on clear instruction. Detail should reflect competence, complexity, risk and change.

Bid procedures may cover secure intake, guest access, incident reporting, portal submission, evidence sanitisation, archive and disposal. Keep them accessible at the point of work.

A procedure written for an auditor and unavailable during the deadline is not an operating procedure. Equally, do not write thirty pages where a controlled checklist will do.

Control-room review

Take one Strategic pursuit and mark which A.5 controls are necessary because of its risks, customer requirements or operating model. Then ask where each control is implemented, who owns it and what evidence exists. Do not assign controls to departments merely to make the table complete. Follow the information.

By the end of the workshop, the tender pack belonged to an information owner, access had a lifecycle, the partner route had an agreement and the incident plan had a customer contact. The departments still mattered. The interfaces mattered more.

CHAPTER 18

People Controls - Annex A.6

CASE FILE

The proposal director described the security problem as human error.

A new starter had forwarded a restricted schedule to a personal address so she could work from home. Her corporate laptop had not arrived. The deadline had not moved. Her manager had told her to find a way.

The person made the transfer. The organisation built the conditions.

The eight people controls in Annex A look at the relationship before, during and after work. They cover screening, terms, learning, discipline, continuing responsibilities, confidentiality, remote work and reporting. In bid operations, these controls need to function for employees and for the temporary workforce that appears around a major pursuit.

A.6.1 - Screen people proportionately

Determine screening appropriate to the role, information, legal environment and customer requirement. Verify identity, experience, qualifications or security clearance where relevant and lawful.

Bid application: confirm named personnel and external contributors meet tender conditions before relying on them. Protect screening evidence and track expiry or role change.

Failure: the response says everyone is screened while freelance or acquired personnel sit outside the process.

A.6.2 - Put security duties into employment and engagement terms

Terms should state information-security responsibilities for employees and relevant external workers, including confidentiality, acceptable use, incident reporting and return of assets.

Bid application: ensure temporary bid roles and seconded staff receive obligations that fit the information they handle.

Failure: a contractor signs an NDA but has no duty to use approved devices, report incidents or delete working copies.

A.6.3 - Build awareness, education and training around real work

People need appropriate security awareness and role-based learning, refreshed as risks and responsibilities change.

Bid application: brief customer handling, phishing, AI, classification, remote work, supplier exchange and submission incidents at kick-off. Test understanding with practical scenarios.

Failure: annual training is complete, but nobody recognises that a prompt can disclose customer-confidential information.

A.6.4 - Use a fair disciplinary process

Establish a communicated process for breaches of information-security rules, consistent with law, contracts and organisational policy.

Bid application: distinguish deliberate misuse, repeated disregard, competence gap and system design failure. Apply consequence without using one individual to hide systemic causes.

Failure: every event produces generic retraining, or the first person to report a near miss is punished and reporting stops.

A.6.5 - Control duties after role change or departure

Identify security responsibilities that continue after termination or change, and communicate them. Adjust access, recover assets and transfer knowledge.

Bid application: when a person leaves the pursuit, remove access, preserve records, confirm confidentiality and redirect customer communications.

Failure: employment access ends, but guest accounts, local downloads and customer portal invitations remain.

A.6.6 - Use confidentiality agreements where appropriate

Determine, document and review confidentiality or non-disclosure requirements with employees and external parties.

Bid application: agreements should cover customer information, partner material, pricing, intellectual property, duration, permitted disclosure and return or deletion.

Failure: the NDA names the wrong entity, excludes subcontractors or conflicts with the customer's tender conditions.

A.6.7 - Secure remote working

Protect information accessed, processed or stored away from organisational premises according to risk and role.

Bid application: define device, network, screen privacy, printing, travel, location, support, storage and disposal rules. Consider cross-border work and customer restrictions.

Failure: the policy assumes a private home office while staff routinely work in trains, hotels and shared spaces.

A.6.8 - Make event reporting easy and immediate

People should report observed or suspected information-security events through accessible channels without delay.

Bid application: include misdirected messages, suspicious portal emails, lost devices, malware, unapproved AI use and supplier concerns. Provide a route outside the affected system.

Failure: staff delay because they cannot decide whether the event is serious enough. Assessment belongs to the incident process, not the frightened individual.

People-control drill

Select one employee, one contractor and one delivery partner with access to a live bid. For each, trace screening, terms, competence, awareness, remote-working conditions, event reporting, current access and the end-of-assignment route. The three paths may differ. The security outcome should not depend on whether HR happens to own the relationship.

The new starter received her managed laptop the next day. More importantly, the onboarding gate was changed so that people could not be assigned sensitive work before the secure route existed. The incident did not become a story about one careless person.

CHAPTER 19

Physical Controls - Annex A.7

CASE FILE

At 18:35, the cleaner folded the bid-room flipchart so that it would fit into the recycling trolley.

The chart showed the customer's incumbent weaknesses, target price, named evaluators and three unresolved security risks. The room had a keypad. The flipchart did not.

Physical security in bidding is easy to underestimate because most information is digital. People still read screens, print documents, use devices, discuss strategy, enter buildings and throw things away. The fourteen physical controls in Annex A address those ordinary routes.

A.7.1 - Establish physical security boundaries

Define physical perimeters appropriate to the information and facilities protected. Boundaries may include offices, secure rooms, data centres, archives and temporary bid rooms.

Bid application: identify where sensitive documents, devices and discussions are permitted. A serviced office boundary may rely partly on provider controls.

Failure: the restricted bid room has a locked door while printed drafts sit in the open shared printer area.

A.7.2 - Control physical entry

Authorise and monitor entry to secure areas. Use badges, reception, visitor records, escorts or other controls proportionate to risk.

Bid application: manage visitors, external reviewers, cleaners and delivery partners around bid information. Remove temporary access after the session.

Failure: a meeting-room booking grants building access long after the confidential review ended.

A.7.3 - Secure offices, rooms and facilities

Design and use offices, rooms and facilities to protect information and equipment. Consider doors, windows, layout, storage and visibility.

Bid application: choose rooms suitable for sensitive reviews and calls. Do not place war-room boards where public visitors can see them.

Failure: the secure video call is held beside a glass wall displaying the customer name, price and win strategy.

A.7.4 - Monitor physical areas where justified

Use suitable monitoring to detect unauthorised physical access, respecting legal and privacy requirements.

Bid application: monitoring may protect secure offices, archives, device stores or data-centre facilities supporting the proposed service.

Failure: cameras exist, but footage is unavailable, clocks are wrong or nobody reviews alerts after an access event.

A.7.5 - Protect against physical and environmental threats

Assess fire, flood, heat, power, civil disruption and other environmental threats. The 2024 climate amendment can make these issues more explicit in context.

Bid application: consider home offices, serviced premises, print rooms, data centres and the availability of the bid process during severe weather.

Failure: continuity assumes access to an office that sits inside the same flood zone as the primary equipment.

A.7.6 - Control work in secure areas

Apply procedures and supervision for work performed in secure areas, including restrictions on devices, photography, visitors and unattended material.

Bid application: brief participants before restricted reviews or customer data-room work. Remove materials afterwards.

Failure: the room is secure, but a participant photographs the whiteboard to work from home.

A.7.7 - Keep desks and screens clear when needed

Reduce exposure from unattended papers, removable media and displayed information. Apply clear-desk and clear-screen rules according to risk.

Bid application: lock screens, clear meeting rooms, collect printouts and avoid sensitive wall displays between sessions.

Failure: the final PDF is protected while reviewer notes and CV printouts remain beside the office kitchen.

A.7.8 - Site and protect equipment

Place equipment to reduce unauthorised access, damage, interference and environmental exposure.

Bid application: position screens away from public view, secure network equipment and protect devices used for restricted work.

Failure: a laptop used for pricing is left beside an unlocked street-level window during an overnight render.

A.7.9 - Protect assets used away from premises

Apply security to devices, media and information off-site. Consider transport, storage, supervision, theft and local conditions.

Bid application: laptops, phones, printouts and encrypted media used by remote or travelling bid teams need defined handling and incident response.

Failure: the device is encrypted, but the notebook beside it contains portal credentials and customer names.

A.7.10 - Control storage media

Manage removable and other storage media through acquisition, use, transport, protection, reuse and disposal.

Bid application: prohibit or control USB use for customer packs, offline contingencies and print production. Encrypt and inventory where necessary.

Failure: an encrypted drive is secure in transit but nobody can identify which version of the bid it contains.

A.7.11 - Protect supporting utilities

Protect facilities and information-processing equipment from utility failure, including power, cooling, telecommunications and other dependencies.

Bid application: consider office power, home connectivity, data-centre utilities and submission-day alternatives.

Failure: the backup internet router exists in a cupboard with an expired SIM and no charged battery.

A.7.12 - Secure power and communications cabling

Protect cabling carrying power or data from interception, interference and damage according to risk.

Bid application: usually relevant to controlled facilities, data centres, print rooms or service environments rather than every home office. Supplier assurance may carry much of the control.

Failure: the control is marked not applicable solely because cabling is outsourced, without assessing provider and physical dependency.

A.7.13 - Maintain equipment securely

Maintain equipment to preserve availability, integrity and security. Use authorised personnel, records and protection during repair.

Bid application: ensure critical laptops, scanners, secure printers, network and service equipment are maintained and that repair does not expose customer data.

Failure: a faulty laptop containing tender material is sent to an unapproved repair shop without controlled deletion or custody.

A.7.14 - Dispose of or reuse equipment safely

Verify that information and licensed software are removed or protected before equipment is disposed of or reused.

Bid application: wipe devices used by temporary teams, return leased equipment and control printer or storage components that retain data.

Failure: an old multifunction printer leaves the office with scanned security schedules still on its internal storage.

Physical walk-through

Walk from the street to the most sensitive information used by the bid. Include reception, meeting rooms, printers, storage, screens, devices, utilities, waste and remote work. Repeat the route after normal office hours. Controls that exist only while a manager is watching are weak controls.

The flipchart incident changed the room-close checklist. The final person photographed nothing, removed papers, wiped boards, checked waste and locked the room. The cleaner was not made responsible for understanding the win strategy.

CHAPTER 20

Technological Controls - Annex A.8

CASE FILE

The bid team had bought more security products than it could explain.

Endpoint protection, data-loss prevention, a cloud access broker, vulnerability scanning, log analytics and a password manager all appeared in the tender response. During review, the evaluator-style reviewer asked which alert would detect a partner downloading the complete data room at 02:00.

Three tools could record part of the event. None had an owner or threshold that turned it into action.

The thirty-four technological controls in Annex A cover endpoints, identities, data, resilience, monitoring, networks and secure development. Technology matters. It becomes a control only when configured, operated, monitored and connected to risk and responsibility.

A.8.1 - Secure user endpoint devices

Manage laptops, phones, tablets and other endpoints through configuration, patching, protection, encryption, access and monitoring.

Bid use: require managed devices for sensitive work, control local storage and provide a lost-device route.

Failure: a secure cloud workspace is accessed from an unsupported personal laptop that keeps local copies.

A.8.2 - Control privileged access

Restrict and govern powerful access rights through approval, least privilege, time limitation, monitoring and review.

Bid use: control workspace administrators, cloud engineers, portal managers and emergency accounts.

Failure: the person administering the bid room can read all pricing and approve their own access indefinitely.

A.8.3 - Restrict information access

Enforce access restrictions according to policy, classification and business need across applications, databases, files and interfaces.

Bid use: separate pricing, legal, personal and restricted technical material while preserving necessary integration.

Failure: a link setting of anyone in the organisation quietly overrides the role design.

A.8.4 - Protect source code

Control access to source code, development tools and related libraries to prevent unauthorised change or disclosure.

Bid use: relevant where the solution includes software demonstrations, code samples or development. Share extracts only through approved routes.

Failure: a developer uploads proprietary code to a public repository to help the proposal team review it.

A.8.5 - Use secure authentication

Implement authentication methods suitable to risk, including multi-factor authentication and secure session handling where appropriate.

Bid use: protect collaboration, portals, cloud services and privileged functions. Test external-user routes as well as employee access.

Failure: MFA protects employees but not guest accounts, which hold the customer data.

A.8.6 - Manage capacity

Monitor and plan capacity to meet current and expected demand.

Bid use: test collaboration, logging, storage, support, network and proposed service capacity, including peak review and submission periods.

Failure: the security monitoring promise works at normal volume but drops logs during the customer's peak scenario.

A.8.7 - Protect against malware

Use prevention, detection, recovery and awareness controls appropriate to malicious software risk.

Bid use: scan tender packs, macros, archives, partner files and production assets; maintain endpoint and email protection.

Failure: staff disable macro security globally because one customer pricing workbook needs signed macros.

A.8.8 - Manage technical vulnerabilities

Obtain information about vulnerabilities, assess exposure and take timely action based on risk.

Bid use: confirm vulnerabilities and patch position for the proposed service and the tools handling customer information.

Failure: the tender promises thirty-day remediation while a critical unsupported component has no supplier patch route.

A.8.9 - Control configuration

Define, implement, monitor and review secure configurations for hardware, software, networks and services.

Bid use: preserve approved baselines for cloud tenants, bid workspaces, endpoints and demonstrations.

Failure: a platform is secure by policy but a new workspace inherits public sharing from a marketing template.

A.8.10 - Delete information securely

Delete information from systems, devices and media when no longer required, subject to retention obligations.

Bid use: close campaign workspaces, remove partner copies, delete demonstration data and retain only authorised records.

Failure: the team removes the folder link but provider backups and downloaded copies remain outside the deletion plan.

A.8.11 - Mask sensitive data where useful

Use masking, pseudonymisation or similar techniques to reduce exposure while preserving legitimate use.

Bid use: create demonstrations with masked or synthetic customer data and redact CVs or case evidence.

Failure: names are removed while rare attributes still make individuals identifiable.

A.8.12 - Prevent inappropriate data leakage

Apply controls to detect or prevent unauthorised disclosure through email, endpoints, cloud, web and other routes.

Bid use: protect customer data, pricing, architecture and personal information; tune controls so urgent legitimate transfers have a secure route.

Failure: DLP blocks the final approved upload and the team bypasses it through personal email because no exception route exists.

A.8.13 - Back up information

Maintain backups according to business and security needs and test restoration.

Bid use: protect source packs, working baselines, pricing, final files and critical service data. Keep backup access and retention controlled.

Failure: automatic sync copies corruption everywhere and is mistaken for a recoverable backup.

A.8.14 - Provide processing redundancy where required

Use redundant facilities or components to meet availability needs.

Bid use: consider identity, collaboration, connectivity, monitoring and proposed customer service. Redundancy depth follows consequence.

Failure: the design claims high availability while both primary and backup depend on the same region or identity service.

A.8.15 - Create and protect logs

Record relevant activities, exceptions, faults and security events; protect and retain logs according to need.

Bid use: workspace access, privileged actions, file events, portal activity and service security logs may support assurance and incident response.

Failure: logs exist but are overwritten before the contract notification period or cannot be linked to unique users.

A.8.16 - Monitor systems and activity

Observe networks, systems and applications for anomalous behaviour and potential incidents, with defined response.

Bid use: explain coverage, hours, thresholds, responsibilities and customer reporting. Price the service.

Failure: the tender says continuous monitoring while alerts are reviewed next working day.

A.8.17 - Synchronise clocks

Use agreed time sources so logs and records can be correlated accurately.

Bid use: critical for incident timelines, access records, submissions, evidence and distributed services.

Failure: three systems record the same event in different time zones and the team cannot establish whether notification was on time.

A.8.18 - Restrict powerful utility programs

Control tools capable of bypassing system and application controls.

Bid use: limit administrative, diagnostic or extraction utilities used in demonstrations and support.

Failure: a convenient export utility allows a contractor to download the complete customer dataset outside normal access restrictions.

A.8.19 - Control software installation

Manage installation of software on operational systems and endpoints.

Bid use: prevent unapproved converters, browser extensions, plugins and AI tools from entering the pursuit environment.

Failure: a designer installs a free PDF tool that uploads documents for processing.

A.8.20 - Secure networks

Protect networks and network devices through design, configuration, management and monitoring.

Bid use: address office, remote, cloud and customer connectivity; identify who owns each segment.

Failure: the proposal describes encrypted application traffic but ignores an unmanaged wireless network used by the delivery team.

A.8.21 - Define security for network services

Establish security mechanisms, service levels and management requirements for network services, whether internal or outsourced.

Bid use: include VPN, connectivity, DNS, firewall, managed network and customer links in supplier and service design.

Failure: availability and incident obligations in the bid exceed the telecommunications provider agreement.

A.8.22 - Segregate networks where risk requires

Separate groups of services, users and systems to reduce exposure and limit movement.

Bid use: distinguish development, production, customer, administrative and guest environments.

Failure: a demonstration environment shares credentials and connectivity with production because separation was considered too expensive.

A.8.23 - Filter access to harmful web content

Use web access controls to reduce exposure to malicious or inappropriate sites in line with risk and policy.

Bid use: protect endpoints used for tender research and file acquisition while maintaining a controlled exception route.

Failure: filtering is absent on contractor devices or so restrictive that users switch to personal equipment.

A.8.24 - Use cryptography under controlled policy

Define and manage cryptographic use, algorithms, keys, certificates and responsibilities according to information and legal requirements.

Bid use: support data in transit and at rest, secure transfer, backups and customer solutions. State boundaries and key ownership.

Failure: the answer says AES-256 without explaining where encryption applies or who controls the keys.

A.8.25 - Operate a secure development lifecycle

Integrate security requirements and activities throughout system or software development.

Bid use: show governance from requirements and threat modelling through coding, testing, release, vulnerability and maintenance.

Failure: the company has a secure development policy for its product but the bid relies on unmanaged scripts outside that lifecycle.

A.8.26 - Define application security requirements

Identify, approve and manage security requirements when developing or acquiring applications.

Bid use: derive requirements from customer, risk, privacy, architecture, authentication, logging, resilience and provider obligations.

Failure: security requirements are added after the application design and treated as optional hardening.

A.8.27 - Use secure architecture and engineering principles

Establish and apply principles for designing secure systems and services.

Bid use: document trust boundaries, defence in depth, least privilege, secure defaults, resilience and shared responsibility.

Failure: the architecture diagram uses security icons but has no design principles or threat assumptions.

A.8.28 - Apply secure coding practices

Use coding standards and controls that reduce vulnerabilities, including review, secrets handling and dependency management.

Bid use: verify that proposed development teams and subcontractors follow controlled practices.

Failure: the tender quotes secure coding guidance while code review is optional and secrets appear in repositories.

A.8.29 - Test security during development and acceptance

Plan and perform security testing appropriate to risk before release or acceptance.

Bid use: specify static and dynamic testing, vulnerability assessment, penetration testing, remediation and acceptance criteria.

Failure: a penetration test is promised annually, but no test occurs before go-live and critical findings have no release threshold.

A.8.30 - Control outsourced development

Govern externally developed systems and components through requirements, agreements, oversight, testing and acceptance.

Bid use: align subcontractor methods, code access, vulnerability, IP, evidence and customer flow-down.

Failure: the prime promises a secure lifecycle that does not apply to the offshore component team.

A.8.31 - Separate development, test and production

Maintain appropriate separation to reduce unauthorised change, disclosure and operational impact.

Bid use: control environments, identities, data and deployment paths; use representative but protected test data.

Failure: live customer data is copied into development because the demonstration needed realistic examples.

A.8.32 - Control system and service changes

Assess, approve, test, implement and review changes affecting information security.

Bid use: connect customer clarification, architecture change, provider update and price movement to risk, design, evidence and approval.

Failure: a late feature is added to strengthen the bid but bypasses security testing and supplier review.

A.8.33 - Protect test information

Select, protect, manage and delete test data appropriately.

Bid use: prefer synthetic or masked data; control access, copies and retention for demonstrations and validation.

Failure: a sample customer dataset becomes permanent development content after the tender ends.

A.8.34 - Protect operational systems during audit or testing

Plan and agree audit tests so they do not harm live systems, data or availability.

Bid use: coordinate penetration tests, demonstrations, evidence collection and customer assurance with owners, windows, scope and recovery.

Failure: an assurance test is run against production during a critical submission or service period without approved safeguards.

Technology assurance drill

Choose one customer information flow and one material service promise. Follow them across endpoint, identity, application, network, cloud, logging, backup, supplier and change. Ask which control prevents, detects, contains or recovers from failure, and who watches the evidence.

After the 02: 00 question, the team set a monitored bulk-download threshold, restricted partner export, defined an incident route and tested it. The products had not changed. The control environment had.

CHAPTER 21

Monitoring, Internal Audit and Management Review

CASE FILE

The board dashboard showed information-security performance at 98 per cent.

The green number came from completion of mandatory training, antivirus deployment and closure of audit actions. It did not include supplier incidents, stale guest accounts, untested recovery, customer complaints or the security commitments delivery had rejected after award.

The number was mathematically correct.

It was answering a question nobody had asked.

Clause 9.1 begins with information needs

ISO/IEC 27001 requires the organisation to determine what needs to be monitored and measured, the methods, timing, responsibilities and when results will be analysed and evaluated. Evidence of results must be retained.

The requirement is not to build the largest dashboard.

Start with decisions:

- Is the ISMS achieving its intended outcomes?
- Are material information-security risks changing?
- Are controls operating and effective?
- Are customer and contractual security requirements being met?
- Are incidents, weaknesses and near misses increasing?
- Are suppliers and cloud services performing?
- Is the secure pursuit process becoming more reliable?
- Which resource or improvement decision is required?

Select measures that help answer those questions.

Measure outcomes, control operation and process health

A balanced security scoreboard may include several layers.

Risk and outcome: high residual risks, risk-treatment progress, significant incidents, customer impact, regulatory or contractual events and loss of availability.

Control operation: access reviews, vulnerability remediation, backup restoration, monitoring coverage, supplier assurance, training effectiveness, deletion, incident exercises and secure configuration.

Bid-process security: sensitive pursuits classified on time, access granted and removed, security requirements identified, provider checks completed, unsupported claims found, security findings closed before release, submission incidents and handover acceptance.

Capability and improvement: competence gaps, audit findings, corrective-action effectiveness, evidence renewal and repeated failure.

Avoid treating every operational count as a KPI. The number of logs generated does not show monitoring effectiveness. The number of security policies does not show secure behaviour.

Define every measure

For each measure, record:

- purpose;
- definition;
- numerator and denominator where relevant;
- data source;
- owner;
- frequency;
- target, threshold or expected range;
- segmentation;
- known limitation;
- data-quality check;
- action trigger;
- reporting route.

Access reviews complete - 100 per cent is incomplete without scope and timing.

Does it include guest access, privileged identities, service accounts and customer portals? Were reviews performed before or after the relevant people left? Did reviewers confirm business need or click Approve All?

A measure needs a definition strong enough to survive curiosity.

Leading and lagging signals

Incidents and customer complaints are lagging. They matter, but they arrive after exposure.

Leading indicators may include:

- high-risk pursuits with security assessment before solution freeze;
- critical providers approved before their capability is promised;
- guest access with expiry;
- high-impact evidence verified before Red review;
- critical security findings closed before release;
- recovery exercises completed;
- material security promises accepted by delivery before submission;
- changes reassessed after clarification or negotiation.

A leading measure can be gamed. Pair it with outcomes and sample quality.

The team may complete every risk assessment on time by copying last month's risks. Audit the content and later incidents.

Control effectiveness is more than completion

A control can be implemented, operated and ineffective.

A phishing exercise may show a low click rate while event reporting remains poor. Backups may complete successfully while restoration exceeds business need. Supplier questionnaires

may be current while critical evidence is unverified. MFA may be deployed while legacy access bypasses it.

Evaluate the intended effect.

For each material control, ask:

- Which risk or requirement does it address?
- What should change when it works?
- Which evidence shows operation?
- Which outcome or indicator shows effectiveness?
- What limitation or residual risk remains?

This connects monitoring to the SoA and risk treatment.

Customer perception and security trust

Monitor customer perception using more than security incidents.

Sources may include:

- tender evaluator feedback;
- security-questionnaire responses;
- clarification patterns;
- assurance requests;
- contract reviews;
- complaints;
- audit findings;
- incident communications;
- reference willingness;
- repeat awards;
- service performance;
- mobilisation feedback.

Silence is not proof of confidence.

A customer may accept the service while repeatedly requesting access evidence because reporting is unclear. That is a perception signal before it becomes a complaint.

Analyse relationships, not isolated arrows

Look for patterns:

- security findings rise when capture is short;
- supplier discrepancies cluster in consortium bids;
- access removal is late after unsuccessful pursuits;
- unsupported security claims originate in one content library;
- incidents increase during remote international work;
- mobilisation problems follow late security design;
- vulnerability commitments miss target when providers own patching;
- review quality falls under concurrent-bid pressure.

Use trend charts, Pareto analysis, control charts, heat maps or simple tables as appropriate. Statistics should reveal a decision, not produce distance from the work.

At Armitage Technology, 68 per cent of material security findings came from three causes: provider evidence obtained late, certificate scope misunderstood and incident commitments

not priced. The company stopped adding generic awareness slides and changed the provider and commercial gates.

Data integrity applies to the dashboard

Secure and govern monitoring data. Define source, access, calculation, change and retention. Protect sensitive incident and vulnerability information.

Check missing data. A low incident rate after a reporting-system outage is not improvement. A supplier-performance score excluding the provider that left the contract is not a complete population.

Where manual fields are used, define entry and quality checks. If teams interpret security review completed differently, the metric will be consistent only in colour.

Clause 9.2.1 - internal audit as an evidence trail

Internal audit determines whether the ISMS conforms to the organisation's requirements and ISO/IEC 27001, and whether it is effectively implemented and maintained.

The audit should follow processes, risks, controls and results.

Do not audit only the presence of policies and the SoA. Select a live or completed pursuit and follow information from opportunity to closure.

An audit might trace:

- customer document into classification and workspace;
- guest access from request to removal;
- security risk into treatment and SoA;
- provider evidence into the tender claim;
- security commitment into price and delivery;
- incident into correction and learning;
- KPI into management decision.

The trail either holds or it breaks.

Clause 9.2.2 - build an audit programme

Plan an audit programme considering process importance, change, risk and previous audit results. Define objectives, criteria, scope, frequency, methods, responsibilities, planning and reporting.

A bid-security audit programme may include:

- annual end-to-end ISMS audit;
- more frequent access and workspace audits;
- supplier and cloud assurance;
- secure development or technical control review;
- high-risk pursuit sampling;
- post-incident targeted audit;
- certification preparation;
- follow-up on corrective action.

Avoid auditing every control with the same frequency. A stable low-risk physical control and a rapidly changing AI service may deserve different attention.

Sample the untidy routes

Include:

- one win;
- one loss;
- one no-bid;
- one live pursuit;
- one supplier-dependent bid;
- one event or near miss where available.

Do not select only the campaign prepared for audit.

A no-bid can reveal whether security risk influences qualification. A loss reveals closure and deletion. A win reveals promise transfer. Live work reveals behaviour before records are tidied.

Competence and independence of auditors

Auditors need competence in audit method and enough subject understanding for the scope. Technical audits may require specialist support. Bid-process audits need someone who can follow requirements, submissions and commercial interfaces.

Independence should prevent auditors judging their own work without challenge. In a small organisation, use cross-audit, an external professional or carefully bounded roles.

The auditor can ask questions and identify evidence. They should not design the complete corrective action during the audit and then later declare it effective.

Audit criteria

Criteria may include:

- ISO/IEC 27001 requirements;
- the organisation's policies and processes;
- SoA controls;
- legal and contractual requirements;
- customer security schedules;
- risk-treatment plans;
- applicable technical standards;
- defined objectives and acceptance criteria.

State the criteria before the finding.

Security could be stronger is not an auditable conclusion.

Findings need requirement and evidence

A clear nonconformity identifies:

- requirement not fulfilled;
- objective evidence;
- scope and sample;
- consequence or significance where relevant.

Weak:

WORKING WORDS

Guest access management needs improvement.

Stronger:

WORKING WORDS

For three of five sampled pursuits, external guest accounts remained active between 21 and 74 days after the recorded supplier or campaign end. This does not conform to the Bid Workspace Procedure section 6.3 requiring access removal within two working days and does not demonstrate effective operation of the selected access-rights control.

The second finding can be corrected, investigated and followed up.

Distinguish nonconformity from observation and improvement opportunity. Do not inflate every preference into a failure. Do not soften a repeated material breach into advice.

Audit control design and operation

For selected controls, ask:

- Why is the control necessary?
- Where is it described in the SoA?
- Who owns it?
- How is it implemented?
- What evidence shows operation?
- How is effectiveness evaluated?
- Which exceptions occurred?
- How are changes controlled?
- What happens when the control fails?

The SoA entry should lead to actual evidence. A control marked implemented because a policy exists may fail when sampled.

Audit Annex A through risk

Do not turn the audit into ninety-three isolated tick boxes.

Select material risks and follow the set of controls acting together. A risk of unauthorised partner disclosure may involve organisational, people, physical and technological controls. Test the chain: agreement, identity, access, device, transfer, awareness, monitoring and removal.

Then sample specific controls where needed for coverage and assurance.

The audit should confirm that Annex A comparison and SoA decisions are reasoned, not that every control has been made green.

Correct and follow up promptly

Audit results should reach relevant management. Correction and corrective action should occur without undue delay according to consequence. Follow-up should verify implementation and effectiveness.

Do not wait for the next annual audit to discover that a critical action was never funded.

Use action ownership, due date, evidence and escalation. Retain audit programme and results.

Clause 9.3.1 - management review

Top management must review the ISMS at planned intervals to ensure continuing suitability, adequacy and effectiveness.

Management review is not an annual presentation delivered by the security manager while everyone else checks email. It is a leadership decision forum.

A high-volume bid operation may use monthly operational security reviews and a formal quarterly or six-monthly management review. A small consultancy may combine them. The interval should reflect change, risk and organisational need.

Clause 9.3.2 - required inputs in working language

Management review should consider, as applicable:

- status of previous actions;
- changes in external and internal issues;
- changes in interested-party needs and expectations;
- feedback on information-security performance;
- nonconformities and corrective actions;
- monitoring and measurement results;
- audit results;
- achievement of information-security objectives;
- feedback from interested parties;
- risk-assessment results and treatment-plan status;
- improvement opportunities.

Translate them into business decisions.

For bid management, include:

- customer and evaluator confidence;
- material pursuit risks;
- incidents and near misses;
- supplier and cloud changes;
- security claims and evidence gaps;
- resource and competence;
- access and information lifecycle;
- standards and regulatory change;
- delivery failures originating in tender commitments.

Clause 9.3.3 - outputs must record decisions

Retain evidence of management-review results, including decisions on improvement and changes to the ISMS.

A useful output records:

- decision;
- rationale;
- owner;
- resource;

- due date;
- affected risk, objective or process;
- follow-up route.

Continue to monitor may be valid where evidence supports it. It should not be the automatic conclusion to repeated failure.

Management review agenda for secure pursuits

1. Changes in strategy, markets, customers, technology, threat and law.
2. Interested-party and climate-related requirements.
3. Security objectives and trends.
4. Risk assessment, treatment and SoA change.
5. Incidents, near misses and customer impact.
6. Bid-process security and release performance.
7. Supplier, cloud and AI assurance.
8. Audit and corrective action.
9. Competence, capacity and working environment.
10. Improvement, certification and resource decisions.

Keep supporting analysis available. Put the decision on the page leadership sees.

The dangerous comfort of green

Dashboards tend to reward green status. Security systems need honest amber and red.

Use thresholds as signals. Avoid punishing owners for surfacing risk. Review whether measures create concealment or superficial completion.

If every control remains green through a supplier incident, platform migration and major scope change, the dashboard may be measuring administrative stability rather than security.

Quality test - what decision did the evidence cause?

Choose one metric, one audit finding and one management-review action.

For the metric: what is defined, what trend appears and what decision followed?

For the finding: which requirement and evidence support it, what cause was addressed and how was effectiveness checked?

For the management action: who owns it, what resource was approved and how will completion be known?

The 98 per cent dashboard at the start of this chapter was replaced with a one-page view. It showed high risks, treatment progress, incidents, supplier assurance, access lifecycle, recovery testing, bid-security findings and handover exceptions. Several indicators were red.

The board funded an identity workflow, moved supplier review earlier and required delivery acceptance before security promises were released.

The overall percentage disappeared.

Nobody missed it after the second meeting.

CHAPTER 22

Improvement, Certification and the Ninety-Day Build

CASE FILE

At 08:30 on Monday, the managing director announced that the company would achieve ISO/IEC 27001 certification in twelve weeks.

A tender required certification in thirteen.

By Wednesday, a consultant had sent fifty-four templates. By Friday, department heads had assigned them to the information-security manager. The sales director asked whether the certificate could be dated before the audit because the system would be substantially complete.

The ISMS project had started with a deadline and no scope.

That is a quick way to produce documents and a slow way to produce security.

Clause 10.1 - continual improvement

ISO/IEC 27001 requires continual improvement of the suitability, adequacy and effectiveness of the ISMS.

Improvement is not constant expansion.

A mature system may improve by:

- removing duplicate access processes;
- simplifying classification;
- replacing broad shared drives with controlled workspaces;
- moving supplier review earlier;
- improving risk criteria;
- reducing unverified claims;
- automating account expiry;
- testing recovery;
- strengthening evidence;
- changing objectives;
- stopping a control that creates work without changing risk.

Use monitoring, audit, incidents, customer feedback, technology change, threat intelligence, staff experience and management review to select priorities.

The ISMS should become easier to operate as it learns, not heavier because every lesson becomes a new form.

Clause 10.2 - nonconformity and corrective action

When nonconformity occurs, the organisation must react, control and correct it where applicable, deal with consequences, evaluate the need to remove causes, implement action, review

effectiveness and make necessary changes to the ISMS. Evidence of the nature, actions and results must be retained.

The requirement is not write a root cause for every typo.

Scale response to consequence and recurrence.

What is nonconformity in a secure bid process?

Examples include:

- customer handling requirement not followed;
- unauthorised access;
- required risk assessment not performed;
- SoA status inaccurate;
- unsupported certificate or security claim submitted;
- supplier security term absent despite defined process;
- security incident not reported through required route;
- final file differs from released baseline;
- customer data retained beyond agreed period;
- internal audit not completed as planned;
- corrective action closed without effectiveness evidence;
- security promise not transferred into delivery.

Not every lost bid is a nonconformity. The evaluator may prefer a stronger offer. Be precise about the requirement that was not fulfilled.

Contain before investigating

For a live event:

1. stop or limit continuing exposure;
2. protect customer and affected information;
3. correct what can be corrected;
4. manage notification and contractual consequences;
5. preserve evidence;
6. then investigate causes proportionately.

Do not hold a two-hour root-cause workshop while an external guest still has access to the data room.

Containment is immediate control. Corrective action comes later.

Cause is usually a system of conditions

Use five whys, event timeline, barrier analysis, fishbone, fault tree or structured interviews as suitable. Do not force one method on every issue.

A misdirected security schedule may involve:

- similar recipient names;
- autocomplete;
- no recipient confirmation for high-risk attachments;
- pressure and fatigue;
- email used instead of a controlled link;
- unclear classification;
- no delay or recall protection;

- weak manager behaviour;
- absence of a practical secure route.

User error describes the final action. It does not explain why the error reached the customer information.

Corrective action should change the cause

Possible actions include:

- redesigning access workflow;
- changing role authority;
- adding an independent check;
- improving supplier agreements;
- replacing an unsuitable tool;
- revising risk criteria;
- strengthening awareness with practical assessment;
- moving a gate earlier;
- introducing automated expiry;
- changing workload or contingency;
- updating the SoA and treatment plan.

Generic retraining is appropriate only when competence or awareness is genuinely causal and the action can be evaluated.

Define effectiveness before closure

Set the test and period:

- sample the next five pursuits;
- confirm guest accounts close within two working days;
- run a restoration test;
- review supplier notifications over three months;
- repeat a practical AI-use exercise;
- check that all critical security promises have delivery owners;
- monitor recurrence of the same finding;
- interview users about bypass and friction.

A document update proves that a document changed. It does not prove the control works.

If the action creates new unsafe behaviour, adjust it.

At Fenwick Systems, data-loss prevention blocked legitimate tender uploads. Staff began using personal email. The corrective action was not stricter blocking. It was a controlled exception route with approval, logging and suitable transfer.

Near misses are useful evidence

Record material near misses: unapproved AI use caught before disclosure, wrong certificate found before release, guest access removed before misuse, corrupted file restored before upload.

Do not punish reporting. Review patterns.

Zero near misses may mean extraordinary control. More often it means the threshold or culture prevents people from reporting them.

A short monthly review of one serious near miss can improve the system without waiting for customer harm.

Certification is an assessment, not an implementation method

ISO/IEC 27001 certification provides independent assessment of an ISMS within a defined scope. Certification bodies audit conformity and implementation. Accredited certification can provide additional confidence in the certification body's competence.

The organisation still has to design and operate the system.

Choose certification for a business reason:

- customer or tender access;
- assurance;
- governance;
- risk management;
- growth;
- supplier confidence;
- integration after acquisition;
- internal discipline.

Competitors have it may be commercially relevant. It does not define scope, controls or intended outcomes.

Obtain authorised standards

Use authorised copies of ISO/IEC 27001:2022 and Amendment 1:2024. Obtain supporting standards and guidance appropriate to the implementation, such as current ISO/IEC 27000 vocabulary, ISO/IEC 27002 control guidance, ISO/IEC 27005 risk guidance and ISO/IEC 27007 audit guidance.

Do not implement from a free checklist whose source, edition and interpretation are unknown.

The standard is concise. The organisational decisions are not.

Scope before templates

Define:

- legal and organisational boundaries;
- sites and remote operations;
- products and services;
- information and technology;
- bid and proposal activities;
- interfaces and outsourced processes;
- interested parties and requirements;
- justified boundaries;
- certification scope wording.

A bid consultancy might use:

WORKING WORDS

Provision of capture, bid management, proposal writing, tender review and related commercial advisory services, including the information systems, remote workforce and approved external providers supporting those services.

A wider supplier may include the bid process within a scope covering the services delivered to customers.

Do not design the scope only to obtain a tender checkbox. It should describe a coherent ISMS the organisation can manage.

Gap assessment against reality

Assess clauses 4 to 10 and the organisation's risk-treatment and Annex A comparison.

For each requirement, record:

- current process;
- evidence;
- conformity status;
- risk and consequence;
- action;
- owner;
- priority;
- target date.

Use statuses such as Conforming, Partly Conforming, Not Conforming and Not Applicable only where applicability is genuinely relevant.

A missing policy may be a manageable documentation gap if the control operates effectively. A polished policy may conceal a major implementation gap.

Interview people. Follow live information. Test the system.

Build the management system before the certificate pack

Minimum viable secure-pursuit ISMS:

- context, interested parties and scope;
- process map and information flows;
- leadership, policy, roles and objectives;
- risk assessment, treatment and SoA;
- asset, classification, access and transfer controls;
- supplier, cloud, AI and remote-work controls;
- secure solution, writing, review and release;
- incident and continuity;
- documented information and records;
- competence and awareness;
- monitoring and measurement;
- internal audit;
- management review;
- nonconformity and corrective action.

Use live pursuits to build evidence. Do not wait until every document is visually complete.

Certification-body selection

For UK-accredited certification, identify a certification body with appropriate UKAS accreditation for ISO/IEC 27001 and relevant capability. Verify status through authoritative UKAS routes. Compare:

- accreditation and scope;
- sector and technical competence;
- audit approach;
- locations and remote operations;
- availability;
- cost;
- transition and surveillance arrangements;
- impartiality;
- customer references where useful.

Do not choose solely on the promise of the fastest certificate.

A certification body should not act as the consultant designing the ISMS it later audits.

Stage 1 and Stage 2

Certification commonly includes a Stage 1 audit and Stage 2 audit, with exact arrangements set by the certification body and applicable accreditation requirements.

Stage 1 usually examines scope, context, documented system, risk method, SoA, internal audit, management review, readiness and planning for Stage 2.

Stage 2 assesses implementation and effectiveness across the scope. Auditors sample people, processes, locations, risks, controls and records. They may identify nonconformities requiring correction and corrective action.

Prepare people to explain work honestly. Do not give them scripts containing clause numbers they do not understand.

Evidence before the audit

Useful evidence includes:

- context and scope decisions;
- risk assessments and treatment;
- SoA and control evidence;
- security objectives and monitoring;
- opportunity and supplier risk decisions;
- access, classification and transfer records;
- incident and recovery exercises;
- secure solution and release records;
- bid submissions and archives;
- competence and awareness;
- provider monitoring;
- internal audits;
- corrective actions with effectiveness checks;
- management-review decisions;
- continual-improvement results.

One perfect demonstration pursuit is not an ISMS.

The ninety-day build

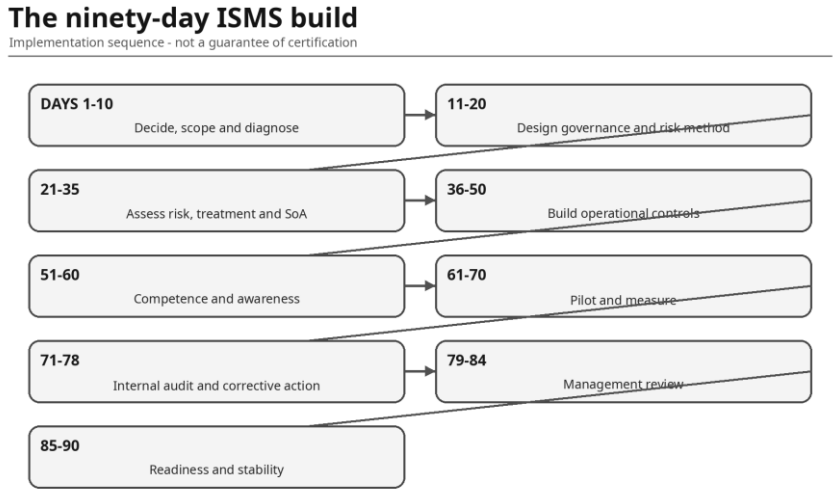

Figure 10 - A ninety-day sequence for establishing and testing a practical secure-pursuit ISMS.

Ninety days can establish a credible working system in a focused organisation with leadership support and existing maturity. It cannot guarantee certification readiness, audit availability or a certificate. Use the sequence to build implementation evidence quickly and honestly.

Days 1-10 - decide and diagnose

Confirm the business case, sponsor, implementation lead, resources, intended scope and certification intention. Obtain the standards. Review context, interested parties and climate relevance. Map current bid and information processes. Identify critical customer, legal and contractual requirements.

Conduct a factual gap assessment. Select one routine and one higher-risk live pursuit as proving grounds where possible.

Outputs: charter, draft scope, current-state map, context register, interested-party register, initial gap and risk priorities.

Days 11-20 - design the ISMS

Agree process architecture, policy, objectives, roles, authority, risk method, acceptance criteria, asset and classification approach, documented-information structure and measures.

Define how the bid process sits inside the ISMS. Decide which existing tools and controls remain. Remove duplicate forms before creating new ones.

Outputs: approved scope, policy, objectives, role matrix, process map, risk method and information architecture.

Days 21-35 - assess risk and build the SoA

Inventory material information and supporting assets. Identify risks to confidentiality, integrity and availability. Evaluate them against approved criteria. Select treatment options and controls. Compare with Annex A. Build the SoA and treatment plan. Obtain risk-owner approval.

Do not mark every control implemented. Make gaps visible.

Outputs: risk register, treatment plan, SoA, residual-risk decisions and priority control actions.

Days 36-50 - establish operational controls

Implement or revise secure opportunity intake, workspace, classification, access, transfer, supplier, cloud, AI, remote work, incident, continuity, design, writing, review, release, submission, archive and disposal.

Configure systems. Create minimum working records. Establish security requirements in bid plans and provider briefs.

Outputs: process cards, configured workflows, access model, supplier controls, incident route, release and archive controls.

Days 51-60 - competence and awareness

Assess role competence. Train and evaluate by role. Brief top management, bid teams, reviewers, IT, providers and delivery. Test reporting, access and secure-working scenarios.

Use real examples. Correct working conditions that force bypass.

Outputs: competence matrix, learning records, practical assessments, awareness evidence and resource actions.

Days 61-70 - pilot and measure

Use the system on live pursuits. Record friction, bypass, errors and missing interfaces. Operate risk assessment, access review, supplier checks, security review, release and closure. Gather initial measures and customer or internal feedback.

Adjust controls through planned change.

Outputs: live evidence, pilot review, corrected controls, initial KPI data and near-miss records.

Days 71-78 - internal audit and corrective action

Conduct risk-based internal audits with competent, sufficiently independent auditors. Sample a live pursuit, completed bid, supplier route and control chain. Raise precise findings. Contain and correct material issues. Begin cause-based corrective action.

Outputs: audit programme, plans, reports, findings, corrective actions and follow-up dates.

Days 79-84 - management review

Present context, interested parties, objectives, performance, incidents, audit, suppliers, resources, risks, treatment, SoA, improvement and certification readiness to top management.

Record decisions, resources, owners and dates.

Outputs: management-review record, approved changes, resource decisions and revised priorities.

Days 85-90 - readiness and stability

Reassess clauses 4 to 10, risk treatment and selected controls. Confirm scope, records, open actions, competence, audit logistics and certification-body arrangements. Close material gaps or control them visibly.

Avoid unnecessary system change immediately before Stage 1. Brief people on their work, not on scripted answers.

Outputs: readiness report, evidence index, open-action plan, certification plan and controlled improvement backlog.

Small organisation version

A five-person consultancy can implement proportionately.

The managing director may be sponsor, risk owner and management-review chair. A bid lead may own the pursuit process and documented information. An external competent professional may support internal audit or technical review. Systems may be simple: controlled cloud workspace, password manager, managed devices, access register, risk and SoA record, incident route, release checklist and archive.

Do not imitate a multinational.

Maintain enough segregation and challenge to prevent one person's memory becoming the ISMS.

High-volume version

A national supplier needs portfolio governance, federated risk ownership, automated identity lifecycle, provider tiers, security review pools, technical assurance, integrated data and segmented measures.

Central definitions should coexist with service- or sector-specific controls. Local teams may adapt implementation where risk and customer requirements differ, but core authority, evidence and incident routes should remain coherent.

Scale must not make ownership anonymous.

Audit-day behaviour

Provide requested evidence promptly and securely. Let people answer in their own words. If a record is missing, say so. Do not create it during lunch and pretend it existed.

Challenge an auditor respectfully where interpretation appears unsupported. Listen first. Certification audit is not an argument to win.

A nonconformity is not humiliation. Use the same corrective-action process the ISMS requires.

After certification

Maintain the system through surveillance and recertification, but do not let audit dates become the only cadence.

Continue:

- risk assessment and treatment;
- SoA review;
- objectives and monitoring;

- access and supplier lifecycle;
- incident and continuity exercises;
- internal audit;
- management review;
- corrective action;
- standards and regulatory monitoring;
- scope and organisational change;
- secure pursuit and delivery learning.

The certificate may help win work. The operating system must still protect it.

Final readiness questions

Can top management explain why the ISMS exists and what it is achieving?

Can a bid manager follow customer information from receipt to secure closure?

Can the organisation show how risks produced controls and how the SoA reflects them?

Can a supplier commitment be traced into agreement, monitoring and exit?

Can a security claim be traced to current evidence and scope?

Can people report an event without guessing whom to tell?

Can delivery find and own every material security promise after award?

Can the system operate when its strongest security person is absent?

Can an internal auditor follow one live risk through evidence and improvement?

Can leadership show what changed because the ISMS produced uncomfortable information?

The company at the start of this chapter postponed its certification audit. It reduced the templates, defined scope, completed risk treatment, corrected supplier access and ran one real internal audit. The tender deadline passed without the certificate.

The sales director was not pleased.

Six months later, the ISMS could show live controls, incidents, audits, management decisions and secure pursuit records. Certification followed after the organisation was ready to be assessed.

The next security questionnaire took less time.

The answers also meant something.

ISO/IEC 27001 Clause-to-Bid Crosswalk

TOOLKIT PURPOSE

This crosswalk is an implementation aid. It paraphrases the current requirements and cannot replace an authorised copy of ISO/IEC 27001:2022 with Amendment 1:2024. All requirements in clauses 4 to 10 apply to an organisation claiming conformity. The design and evidence depend on scope, context and risk.

Clause 1 - Scope of the standard

Working meaning: ISO/IEC 27001 specifies requirements for establishing, implementing, maintaining and continually improving an ISMS. It also requires risk assessment and treatment tailored to the organisation.
Bid application: decide whether the pursuit process sits inside the ISMS and whether the services promised by the bid sit inside the intended certification scope.
Minimum evidence: approved ISMS scope, products and services, organisational boundaries, process map and applicable certificate scope where certified.

> **Failure pattern:** the certificate is presented as universal proof although the bidder, location, bid service or proposed customer solution sits outside its scope.

Clause 2 - Normative references

Working meaning: the standard relies on the terms and definitions in the referenced ISO/IEC 27000 vocabulary.
Bid application: use controlled terminology for risk, control, incident, confidentiality, integrity, availability and ISMS. Resolve customer-specific definitions where they differ.
Minimum evidence: terminology or glossary where needed, authorised supporting standards and consistent use in process and tender responses.

> **Failure pattern:** incident, event, breach and nonconformity are used as interchangeable words, creating different notification and response decisions.

Clause 3 - Terms and definitions

Working meaning: the vocabulary governs interpretation of the requirements.
Bid application: ensure risk owners, auditors, writers, engineers and delivery teams share the same operating meaning. Customer contract definitions remain separately authoritative for that contract.
Minimum evidence: training, process definitions, tender terminology dictionary and controlled contract interpretation.

> **Audit prompt:** choose one term used in a security answer and ask three roles to explain it. Do their explanations lead to the same action?

4.1 - Organisational context

Working meaning: determine relevant external and internal issues that affect the ISMS's intended outcomes, including whether climate change is relevant.
Bid application: assess markets, customers, law, threat, technology, suppliers, workforce, remote operation, evidence maturity, financial appetite and climate-related disruption or requirements.
Controls and records: context register, management analysis, trigger review, risk and objective links, climate-relevance decision.

> **Audit prompt:** which context change most recently altered qualification, workspace, supplier, architecture or assurance?

4.2 - Interested parties and their requirements

Working meaning: identify interested parties relevant to the ISMS and determine their relevant requirements. Relevant parties may have climate-related requirements.
Bid application: customers, service users, employees, delivery, regulators, partners, certification bodies, insurers, shareholders and data subjects may create security needs or obligations.
Controls and records: interested-party register, source, requirement, owner, process effect and monitoring route.

> **Failure pattern:** the register lists everyone while no one can explain which requirement changed the ISMS.

4.3 - ISMS scope

Working meaning: define boundaries and applicability using context, interested parties, interfaces, dependencies and activities performed by other parties. Keep the scope as documented information.
Bid application: state which legal entities, locations, people, systems, remote work, pursuit activities and services are covered. Explain outsourced interfaces.
Controls and records: scope statement, organisational map, information-flow map, certificate wording and boundary rationale.

> **Audit prompt:** where does secure end-to-end bid management start and end, and what important information crosses the boundary?

4.4 - Establish and operate the ISMS

Working meaning: establish, implement, maintain and continually improve the ISMS and its processes and interactions.
Bid application: connect opportunity, capture, secure intake, risk, solution, writing, supplier, review, release, incident, handover and learning.
Controls and records: process architecture, owners, inputs, outputs, criteria, measures, records and improvement.

> **Failure pattern:** policies mirror clause numbers but the live pursuit follows private inboxes and individual memory.

5.1 - Leadership and commitment

Working meaning: top management is accountable for ISMS effectiveness, integration, resources, communication and improvement.

Bid application: leadership sets risk appetite, protects security gates, resolves resource conflict, accepts residual risk and prevents commercial urgency bypassing controls.
Evidence: decisions, objectives, resource allocation, management review, risk acceptance and response to incidents.

> **Audit prompt:** show a security decision that became difficult because revenue or deadline pressure pointed the other way.

5.2 - Information-security policy

Working meaning: establish a policy suitable to purpose, supporting objectives, including commitments to requirements and continual improvement; communicate and make it available appropriately.
Bid application: the policy should guide classification, access, supplier use, secure design, AI, incident, release and retention.
Evidence: approved policy, review, communication, awareness and decisions reflecting it.

> **Failure pattern:** the tender quotes the policy while the approved bid process contradicts it.

5.3 - Roles, responsibilities and authorities

Working meaning: assign and communicate security responsibilities and authority, including reporting on ISMS performance.
Bid application: define information owner, risk owner, security lead, bid manager, supplier owner, access approver, incident lead, reviewer, releaser and delivery owner.
Evidence: role and authority matrix, deputies, approvals, escalation and management reporting.

> **Audit prompt:** who may stop submission after a security incident, and who may override that decision?

6.1.1 - Risks and opportunities affecting the ISMS

Working meaning: address risks and opportunities arising from context and interested parties so the ISMS can achieve outcomes, prevent undesirable effects and improve.
Bid application: consider strategic information risk, process weakness, customer trust, supplier dependency, technology change and improvement opportunities.
Evidence: actions integrated into processes, evaluation of effectiveness and management decisions.

> **Failure pattern:** the risk register changes colour but no control, resource or decision changes.

6.1.2 - Information-security risk assessment

Working meaning: define and apply a consistent risk-assessment process with criteria, risk acceptance, identification, ownership, analysis and evaluation of confidentiality, integrity and availability risk.
Bid application: assess information assets, customer documents, solution data, identities, suppliers, AI, workspaces, submission and proposed services.
Evidence: method, criteria, asset and risk records, owners, consequence, likelihood, evaluation and repeatable results.

> **Audit prompt:** can another competent person apply the method to the same facts and reach a reasonably comparable decision?

6.1.3 - Information-security risk treatment

Working meaning: select treatment options and necessary controls, compare them with Annex A, produce the SoA, formulate a treatment plan and obtain risk-owner approval of the plan and residual risk.
Bid application: turn pursuit and service risk into specific organisational, people, physical and technological controls. Use non-Annex-A controls where necessary.
Evidence: treatment decisions, SoA, plan, owners, implementation status and residual-risk approvals.

> **Failure pattern:** every Annex A control is marked applicable without risk reasoning, or every control is marked implemented before evidence exists.

6.2 - Information-security objectives and planning

Working meaning: establish measurable objectives consistent with policy and requirements, monitor them and plan what, who, resources, timing and evaluation.
Bid application: reduce late security findings, close external access promptly, improve provider assurance, test recovery, improve promise handover or strengthen evidence.
Evidence: baseline, target, owner, measure, action, result and review.

> **Audit prompt:** which objective changed a leadership or resource decision this quarter?

6.3 - Planning ISMS changes

Working meaning: carry out changes in a planned manner.
Bid application: control new collaboration or AI platforms, supplier changes, scope expansion, revised risk method, acquisition, new sector or remote-work model.
Evidence: change proposal, impact, approval, pilot, communication, training, verification and review.

> **Failure pattern:** a new proposal platform is launched during a strategic bid without tested access, migration or fallback.

7.1 - Resources

Working meaning: determine and provide resources needed to establish, implement, maintain and improve the ISMS.
Bid application: security people, bid capacity, systems, devices, identity, monitoring, specialist advisers, provider assurance, testing and contingency.
Evidence: resource and capacity plans, approved budgets, system ownership and management decisions.

> **Audit prompt:** which required security control currently lacks enough people, time, money or technology to operate?

7.2 - Competence

Working meaning: determine competence, ensure people are competent through suitable education, training or experience, take action and evaluate it, retaining evidence.
Bid application: security architects, bid managers, writers, reviewers, suppliers, uploaders, auditors and risk owners need role-specific capability.
Evidence: competence matrix, practical assessment, supervised work, qualifications and effectiveness review.

> **Failure pattern:** training attendance is used as proof that a person can apply customer security requirements.

7.3 - Awareness

Working meaning: people understand policy, their contribution, benefits and consequences of nonconformity.
Bid application: people recognise classification, phishing, customer rules, AI boundaries, access expiry, incidents and release consequences.
Evidence: role briefings, practical behaviour, event reporting and interviews.

> **Audit prompt:** ask a writer what happens if they use an unapproved AI service with customer information.

7.4 - Communication

Working meaning: determine internal and external communications: what, when, with whom, how and by whom.
Bid application: customer clarifications, security changes, incidents, supplier requirements, access decisions, risk acceptance, release and handover.
Evidence: communication plan, authorised routes, retained messages, escalation and customer receipts.

> **Failure pattern:** a security commitment is made by phone and never reaches price, contract or delivery.

7.5.1 - Documented information: general

Working meaning: include information required by the standard and information the organisation determines necessary for ISMS effectiveness.
Bid application: maintain enough policies, process cards, risk and SoA records, access, supplier, incident, review, release and archive evidence.

> **Failure pattern:** the organisation writes a procedure for every clause while the most important live decision remains in chat.

7.5.2 - Creating and updating information

Working meaning: ensure appropriate identification, format, review and approval when creating or updating documented information.
Bid application: identify owner, date, status, classification, version and approver for policies, risk records, templates, evidence and final outputs.
Evidence: controlled metadata, approval and change history.

> **Audit prompt:** which version of the SoA and security response is authoritative, and how do you know?

7.5.3 - Controlling documented information

Working meaning: make information available where needed and protect it from loss of confidentiality, integrity or improper use. Address distribution, access, retrieval, storage, preservation, change, retention, disposal and external information.
Bid application: control source packs, customer property, workspace access, final files, audit evidence, external standards and secure disposal.
Evidence: permissions, baselines, archives, retention, deletion and external-document control.

> **Failure pattern:** the central library is available but contains expired certificates, uncontrolled downloads and no authoritative status.

8.1 - Operational planning and control

Working meaning: plan, implement and control processes needed to meet requirements and risk actions; establish criteria, control changes and retain evidence.
Bid application: opportunity class, security plan, workspace, risk gates, provider checks, design, review, release, incident and handover.
Evidence: plans, entry and exit criteria, controls, changes, exceptions and results.

> **Audit prompt:** which security control was strengthened because this pursuit was classified as Strategic?

8.2 - Operational information-security risk assessment

Working meaning: perform risk assessments at planned intervals and when significant changes occur, retaining results.
Bid application: reassess after sensitive data, new provider, architecture change, international remote work, incident, customer clarification or major negotiation.
Evidence: dated assessment, trigger, owner and revised decisions.

> **Failure pattern:** the enterprise risk assessment remains unchanged while the live solution and suppliers move substantially.

8.3 - Operational information-security risk treatment

Working meaning: implement the risk-treatment plan and retain results.
Bid application: configure access, sign supplier terms, implement monitoring, perform training, test recovery, close treatment actions and approve residual risk before release or operation.
Evidence: completed control records, tests, approvals and updated treatment status.

> **Audit prompt:** select one high risk and show the actual implemented treatment, not the planned task.

9.1 - Monitoring, measurement, analysis and evaluation

Working meaning: decide what to monitor and measure, methods, timing, responsibility, analysis and evaluation; retain evidence.
Bid application: risk, incidents, access, suppliers, recovery, bid-security findings, release, handover, customer perception and objectives.
Evidence: KPI definitions, data quality, trends, interpretation and decisions.

> **Failure pattern:** a green completion percentage conceals ineffective controls and missing data.

9.2.1 - Internal audit: general

Working meaning: conduct audits at planned intervals to determine conformity and effective implementation and maintenance.
Bid application: follow real information, risks and controls across the pursuit, including wins, losses and live work.
Evidence: audit plan, objective evidence, conclusions, findings and follow-up.

9.2.2 - Internal audit programme

Working meaning: plan and maintain an audit programme considering process importance and previous results; define criteria and scope, use objective auditors, report and act without undue delay.
Bid application: prioritise high-risk, changing or weak areas such as supplier access, AI, cloud, incident response, secure development and handover.
Evidence: risk-based programme, competence, independence, reports and closure.

> **Audit prompt:** why was this process audited now, and which evidence changed the next programme?

9.3.1 - Management review: general

Working meaning: top management reviews the ISMS at planned intervals for continuing suitability, adequacy and effectiveness.
Bid application: integrate security into commercial and operational governance rather than running a separate audit-season meeting.
Evidence: planned reviews, leadership attendance, current inputs and decisions.

9.3.2 - Management-review inputs

Working meaning: consider prior actions, context and interested-party change, performance, nonconformity, monitoring, audit, objectives, feedback, risk and treatment, and improvement.
Bid application: include customer security feedback, supplier change, incidents, risk, SoA, bid findings, evidence gaps, resources and delivery promises.

> **Failure pattern:** the review receives slides but no current risk or decision request.

9.3.3 - Management-review results

Working meaning: retain decisions on improvement and necessary ISMS changes.
Bid application: record what will stop, start, change, be funded, accepted or escalated.
Evidence: decision, owner, resource, date and follow-up.

> **Audit prompt:** which management-review decision changed the secure pursuit process?

10.1 - Continual improvement

Working meaning: continually improve ISMS suitability, adequacy and effectiveness.
Bid application: simplify controls, improve evidence, automate expiry, move assurance earlier, strengthen suppliers and remove waste.
Evidence: selected improvements, tested change, performance and sustained result.

> **Failure pattern:** improvement means adding forms without testing whether risk or customer confidence changes.

10.2 - Nonconformity and corrective action

Working meaning: react to nonconformity, control and correct it, deal with consequences, evaluate causes and similar issues, implement action, review effectiveness and change the ISMS where necessary.
Bid application: respond to access failures, disclosure, inaccurate claims, missed risk assessment, insecure supplier use, release defects or failed promise transfer.
Evidence: containment, correction, cause, action, effectiveness and updated risk or controls.

> **Audit prompt:** what changed in the system because the last security failure occurred, and what proves recurrence risk was reduced?

Annex A 93-Control Bid Crosswalk

TOOLKIT PURPOSE

Use this crosswalk after the organisation has determined its necessary controls through risk treatment. It is a completeness and implementation aid, not a declaration that all ninety-three controls are automatically required. The labels are deliberately paraphrased. Consult the authorised standards for exact wording and guidance.

A.5 - Organisational controls

A.5.1 Govern the information-security policy framework

A practical pursuit pack links the relevant policy rules at kick-off rather than attaching a forty-page policy nobody opens. Evidence may include approval, review history, staff awareness and decisions that follow the policy.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** Failure appears when the tender claims strong governance while the live bid uses personal storage, broad access and unapproved tools. The policy exists, but the operating route teaches something else.

A.5.2 Assign security roles and accountabilities

Use a role and authority matrix showing deputies and escalation. Retain risk ownership, access approval, security review and release decisions.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** The common failure is a RACI crowded with contributors and empty of decision rights. When the security lead is absent, nobody knows who may accept residual risk or stop submission.

A.5.3 Separate incompatible duties

Separate author from independent reviewer where possible; separate commercial model ownership from final approval; require a second person to verify portal contents; prevent workspace administrators from approving their own privileged access.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** Failure occurs when the same person grants access, uploads the file and confirms that the upload was correct. The process may be fast. It cannot independently detect its own mistake.

A.5.4 Make managers responsible for secure behaviour

Evidence is visible in workload decisions, corrected unsafe practice, role briefings, removal of unapproved tools and action after near misses.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

WATCH FOR A manager who signs the policy and then asks a writer to use a personal account because the approved platform is slow has issued the real instruction.

A.5.5 Maintain contact with competent authorities

A bid-stage incident plan should state who decides whether to contact law enforcement, regulators, the NCSC, a contracting authority or another competent body, and how evidence is preserved.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

WATCH FOR Do not search for the correct authority during the first hour of a serious incident. Equally, do not notify externally without defined authority and competent legal or regulatory assessment.

A.5.6 Use relevant security communities and specialist groups

For pursuit teams this may support current knowledge on public-sector security expectations, cloud risk, vulnerability disclosure, supplier assurance or secure development. Record how information is assessed before it changes the ISMS.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

WATCH FOR Membership logos are not threat intelligence. The control works when useful external knowledge changes a risk, design, training or response.

A.5.7 Operate a threat-intelligence process

A high-risk technology bid may need current knowledge about sector attacks, exploited vulnerabilities, supplier compromise, phishing campaigns or threats to the proposed platform. The output may change treatment, architecture, monitoring or bid/no-bid.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

WATCH FOR Copying a weekly threat bulletin into a folder is collection, not intelligence. Ask what changed because the organisation learned it.

A.5.8 Build security into project and pursuit management

Use security gates, risk actions, secure workspaces, design reviews, supplier checks, incident routes, release criteria and handover. Scale depth to the opportunity.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

WATCH FOR The failure pattern is familiar: the security questionnaire lands with IT three days before submission, after solution and price have already been fixed.

A.5.9 Maintain an inventory of information and supporting assets

For a pursuit, inventory source documents, workspaces, datasets, pricing models, credentials, devices, providers, AI tools, final files and archives. Link classification, owner, retention and access.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

WATCH FOR A file cannot be protected or deleted reliably when the organisation does not know that a partner downloaded it or that a local copy exists.

A.5.10 Define acceptable use

Make bid-specific restrictions visible at kick-off and in provider briefs. Provide a workable authorised route.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** A prohibition that requires three days to obtain secure file transfer will be tested by a deadline in three hours. Acceptable use must be supported by usable systems.

A.5.11 Recover or account for assets at the end of access

Remove guest access, recover loan devices and tokens, transfer records, confirm deletion of controlled copies and preserve continuing obligations.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** The control fails when a consultant leaves the project but retains downloaded tender material because offboarding only disabled the corporate account.

A.5.12 Classify information by consequence and requirement

Bid classifications may distinguish public notices, internal strategy, customer-confidential material, personal data, privileged legal advice and restricted technical information. Map customer labels to internal handling.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** Everything marked Confidential creates noise. Nothing marked Confidential creates exposure. The label should change access, transfer, storage, retention or review.

A.5.13 Label information so people can handle it correctly

Provide clear instructions for inherited customer labels and for files that cannot carry visible markings, such as pricing workbooks or portal fields.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** A label is ineffective when external contributors do not understand it or when it remains after a document has been properly sanitised for public use.

A.5.14 Control information transfer

Define approved routes, recipient checks, encryption where needed, access expiry, transfer records, supplier rules and incident response. Verify unusual destinations and high-risk attachments.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** The ordinary failure is the correct file sent securely to the wrong Martin. Technology helps; recipient and purpose checks still matter.

A.5.15 Establish access-control principles

In the bid room, access should follow role, question, information class and campaign stage. Customer or legal restrictions may require tighter boundaries.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** Broad access granted because the deadline is near becomes the permanent position unless expiry and review are designed.

A.5.16 Manage identities through their lifecycle

Link onboarding and offboarding to the pursuit roster, partner status and role changes. Control shared and non-human identities separately.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** A dormant guest account is not harmless because the partner has stopped attending meetings. The identity remains a route until the system closes it.

A.5.17 Protect authentication information

Avoid credentials in bid documents, chat or shared spreadsheets. Use approved password or secrets management and separate emergency recovery.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** The portal password taped into the upload checklist may solve availability for one afternoon and create an accountability problem for months.

A.5.18 Provision, review and remove access rights

For live pursuits, review guest and privileged access at gates, after supplier change, at submission and at closure. Retain approval and review evidence.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** The access list should show why a person still needs the information, not merely that the platform allows them to see it.

A.5.19 Manage security risk in supplier relationships

Bid-related suppliers include freelance writers, designers, hosting providers, proposal platforms, data-room services, AI tools and delivery partners.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** The failure is approving a supplier because another department already uses it, without examining the different information and purpose in the pursuit.

A.5.20 Put security requirements into supplier agreements

Requirements must be understood by both parties and reconciled with the prime bid. Retain signed terms and approved exceptions.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** A one-hour customer notification cannot be supported by a supplier contract allowing notice within twenty-four hours unless another control closes the gap.

A.5.21 Address security across the ICT supply chain

In a bid, ask how proposed platforms, libraries, hardware, telecommunications and managed services are sourced, supported, changed and monitored.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** A supplier certificate gives assurance within scope; it does not reveal every component dependency or guarantee future availability.

A.5.22 Monitor supplier performance, assurance and change

Reassess when ownership, location, subprocessors, architecture, control scope or customer requirements change. Update bid claims accordingly.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** The provider approved last year may no longer deliver the same service. Current tender evidence needs a current provider position.

A.5.23 Govern acquisition, use and exit from cloud services

This applies to the offered solution and to cloud tools used to produce the bid. The same SaaS platform may have different risks under different use cases.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** Cloud certification does not configure the tenant. A secure provider can host an insecurely managed customer environment.

A.5.24 Prepare for information-security incidents

The pursuit incident plan should include misdirected files, compromised accounts, malicious tender content, supplier incidents and portal disruption.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** A phone tree last checked three years ago is not preparation. Test a realistic bid-stage scenario and record what failed.

A.5.25 Assess events and decide whether they are incidents

Record the decision and authority. Not every suspicious event is a confirmed incident, but uncertainty may still require containment.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** The control fails when every event is ignored until harm is proven, or when every anomaly triggers the same crisis response.

A.5.26 Respond to incidents under controlled authority

Bid operations should know who may stop submission, revoke access, contact the customer and approve recovery. Supplier routes must align.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** Urgency is not permission for five people to investigate the same account and destroy the evidence trail.

A.5.27 Learn from incidents

Feed learning into qualification, supplier onboarding, workspace rules, AI use, review and handover. Share only the detail needed for action.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** A lessons report stored in a restricted incident folder does not improve bidding unless controlled changes reach the people and process.

A.5.28 Collect and preserve evidence

Relevant evidence may include logs, emails, file versions, access records, devices, screenshots and timelines. Use competent support for serious cases.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** Casual copying, editing or opening of evidence may change metadata or integrity. The first person curious about the incident should not become the forensic method.

A.5.29 Maintain security during disruption

A bid team working through platform outage still needs controlled files, identities, communications and release. The fallback should not be personal email and unmanaged storage.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** Continuity that preserves productivity but abandons confidentiality or integrity has solved only one part of the problem.

A.5.30 Ensure ICT can support continuity requirements

For critical pursuits and services, identify collaboration, identity, communication, backup, portal and provider dependencies. Test restoration and alternate routes.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** A backup that has never been restored is a hope stored on another system.

A.5.31 Identify and comply with legal, regulatory and contractual duties

The register should connect obligations to controls, owners, evidence and change monitoring. Tender and contract requirements belong in the same operational route.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** Copying a generic list of laws into the ISMS is not compliance. Show which duty changed a process, retention rule, notification route or design.

A.5.32 Protect intellectual-property rights

Bid teams should control reuse of customer content, competitor material, licensed standards, images, source code and partner evidence. Define rights in external contributor agreements.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** A previous customer's diagram remains protected even after the company name is removed.

A.5.33 Protect records

Bid records include released submissions, approvals, risk decisions, receipts, clarifications, incidents, contracts and audit trails. Ensure readability and retrieval over the period.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** Keeping every draft forever is not records protection. It can conceal the authoritative record and extend unnecessary exposure.

A.5.34 Protect privacy and personal information

Bids involve CVs, references, user data, demonstrations and customer datasets. Align privacy roles with security controls and customer commitments.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** A security answer can be technically strong and still fail because personal data was collected or reused without a valid and transparent basis.

A.5.35 Obtain independent review of information security

Use internal audit, external specialists, certification audits, technical assurance or peer review. Findings should reach management and corrective action.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** The architect explaining that their own design is secure is useful input. It is not independent assurance.

A.5.36 Check compliance with security policies and standards

Sample live pursuits: access, classification, AI use, supplier onboarding, retention and release. Distinguish approved exception from silent bypass.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** The audit should not begin and end with whether a policy was signed. Follow the information through the actual work.

A.5.37 Maintain clear operating procedures where needed

Bid procedures may cover secure intake, guest access, incident reporting, portal submission, evidence sanitisation, archive and disposal. Keep them accessible at the point of work.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** A procedure written for an auditor and unavailable during the deadline is not an operating procedure. Equally, do not write thirty pages where a controlled checklist will do.

A.6 - People controls

A.6.1 Screen people proportionately

confirm named personnel and external contributors meet tender conditions before relying on them. Protect screening evidence and track expiry or role change.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** the response says everyone is screened while freelance or acquired personnel sit outside the process.

A.6.2 Put security duties into employment and engagement terms

ensure temporary bid roles and seconded staff receive obligations that fit the information they handle.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** a contractor signs an NDA but has no duty to use approved devices, report incidents or delete working copies.

A.6.3 Build awareness, education and training around real work

brief customer handling, phishing, AI, classification, remote work, supplier exchange and submission incidents at kick-off. Test understanding with practical scenarios.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** annual training is complete, but nobody recognises that a prompt can disclose customer-confidential information.

A.6.4 Use a fair disciplinary process

distinguish deliberate misuse, repeated disregard, competence gap and system design failure. Apply consequence without using one individual to hide systemic causes.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** every event produces generic retraining, or the first person to report a near miss is punished and reporting stops.

A.6.5 Control duties after role change or departure

when a person leaves the pursuit, remove access, preserve records, confirm confidentiality and redirect customer communications.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** employment access ends, but guest accounts, local downloads and customer portal invitations remain.

A.6.6 Use confidentiality agreements where appropriate

agreements should cover customer information, partner material, pricing, intellectual property, duration, permitted disclosure and return or deletion.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** the NDA names the wrong entity, excludes subcontractors or conflicts with the customer's tender conditions.

A.6.7 Secure remote working

define device, network, screen privacy, printing, travel, location, support, storage and disposal rules. Consider cross-border work and customer restrictions.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** the policy assumes a private home office while staff routinely work in trains, hotels and shared spaces.

A.6.8 Make event reporting easy and immediate

include misdirected messages, suspicious portal emails, lost devices, malware, unapproved AI use and supplier concerns. Provide a route outside the affected system.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** staff delay because they cannot decide whether the event is serious enough. Assessment belongs to the incident process, not the frightened individual.

A.7 - Physical controls

A.7.1 Establish physical security boundaries

identify where sensitive documents, devices and discussions are permitted. A serviced office boundary may rely partly on provider controls.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** the restricted bid room has a locked door while printed drafts sit in the open shared printer area.

A.7.2 Control physical entry

manage visitors, external reviewers, cleaners and delivery partners around bid information. Remove temporary access after the session.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** a meeting-room booking grants building access long after the confidential review ended.

A.7.3 Secure offices, rooms and facilities

choose rooms suitable for sensitive reviews and calls. Do not place war-room boards where public visitors can see them.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** the secure video call is held beside a glass wall displaying the customer name, price and win strategy.

A.7.4 Monitor physical areas where justified

monitoring may protect secure offices, archives, device stores or data-centre facilities supporting the proposed service.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** cameras exist, but footage is unavailable, clocks are wrong or nobody reviews alerts after an access event.

A.7.5 Protect against physical and environmental threats

consider home offices, serviced premises, print rooms, data centres and the availability of the bid process during severe weather.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** continuity assumes access to an office that sits inside the same flood zone as the primary equipment.

A.7.6 Control work in secure areas

brief participants before restricted reviews or customer data-room work. Remove materials afterwards.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** the room is secure, but a participant photographs the whiteboard to work from home.

A.7.7 Keep desks and screens clear when needed

lock screens, clear meeting rooms, collect printouts and avoid sensitive wall displays between sessions.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** the final PDF is protected while reviewer notes and CV printouts remain beside the office kitchen.

A.7.8 Site and protect equipment

position screens away from public view, secure network equipment and protect devices used for restricted work.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

WATCH FOR a laptop used for pricing is left beside an unlocked street-level window during an overnight render.

A.7.9 Protect assets used away from premises

laptops, phones, printouts and encrypted media used by remote or travelling bid teams need defined handling and incident response.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

WATCH FOR the device is encrypted, but the notebook beside it contains portal credentials and customer names.

A.7.10 Control storage media

prohibit or control USB use for customer packs, offline contingencies and print production. Encrypt and inventory where necessary.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

WATCH FOR an encrypted drive is secure in transit but nobody can identify which version of the bid it contains.

A.7.11 Protect supporting utilities

consider office power, home connectivity, data-centre utilities and submission-day alternatives.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

WATCH FOR the backup internet router exists in a cupboard with an expired SIM and no charged battery.

A.7.12 Secure power and communications cabling

usually relevant to controlled facilities, data centres, print rooms or service environments rather than every home office. Supplier assurance may carry much of the control.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

WATCH FOR the control is marked not applicable solely because cabling is outsourced, without assessing provider and physical dependency.

A.7.13 Maintain equipment securely

ensure critical laptops, scanners, secure printers, network and service equipment are maintained and that repair does not expose customer data.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

WATCH FOR a faulty laptop containing tender material is sent to an unapproved repair shop without controlled deletion or custody.

A.7.14 Dispose of or reuse equipment safely

wipe devices used by temporary teams, return leased equipment and control printer or storage components that retain data.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

WATCH FOR an old multifunction printer leaves the office with scanned security schedules still on its internal storage.

A.8 - Technological controls

A.8.1 Secure user endpoint devices

require managed devices for sensitive work, control local storage and provide a lost-device route.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** a secure cloud workspace is accessed from an unsupported personal laptop that keeps local copies.

A.8.2 Control privileged access

control workspace administrators, cloud engineers, portal managers and emergency accounts.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** the person administering the bid room can read all pricing and approve their own access indefinitely.

A.8.3 Restrict information access

separate pricing, legal, personal and restricted technical material while preserving necessary integration.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** a link setting of anyone in the organisation quietly overrides the role design.

A.8.4 Protect source code

relevant where the solution includes software demonstrations, code samples or development. Share extracts only through approved routes.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** a developer uploads proprietary code to a public repository to help the proposal team review it.

A.8.5 Use secure authentication

protect collaboration, portals, cloud services and privileged functions. Test external-user routes as well as employee access.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** MFA protects employees but not guest accounts, which hold the customer data.

A.8.6 Manage capacity

test collaboration, logging, storage, support, network and proposed service capacity, including peak review and submission periods.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** the security monitoring promise works at normal volume but drops logs during the customer's peak scenario.

A.8.7 Protect against malware

scan tender packs, macros, archives, partner files and production assets; maintain endpoint and email protection.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** staff disable macro security globally because one customer pricing workbook needs signed macros.

A.8.8 Manage technical vulnerabilities

confirm vulnerabilities and patch position for the proposed service and the tools handling customer information.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** the tender promises thirty-day remediation while a critical unsupported component has no supplier patch route.

A.8.9 Control configuration

preserve approved baselines for cloud tenants, bid workspaces, endpoints and demonstrations.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** a platform is secure by policy but a new workspace inherits public sharing from a marketing template.

A.8.10 Delete information securely

close campaign workspaces, remove partner copies, delete demonstration data and retain only authorised records.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** the team removes the folder link but provider backups and downloaded copies remain outside the deletion plan.

A.8.11 Mask sensitive data where useful

create demonstrations with masked or synthetic customer data and redact CVs or case evidence.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** names are removed while rare attributes still make individuals identifiable.

A.8.12 Prevent inappropriate data leakage

protect customer data, pricing, architecture and personal information; tune controls so urgent legitimate transfers have a secure route.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** DLP blocks the final approved upload and the team bypasses it through personal email because no exception route exists.

A.8.13 Back up information

protect source packs, working baselines, pricing, final files and critical service data. Keep backup access and retention controlled.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** automatic sync copies corruption everywhere and is mistaken for a recoverable backup.

A.8.14 Provide processing redundancy where required

consider identity, collaboration, connectivity, monitoring and proposed customer service. Redundancy depth follows consequence.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** the design claims high availability while both primary and backup depend on the same region or identity service.

A.8.15 Create and protect logs

workspace access, privileged actions, file events, portal activity and service security logs may support assurance and incident response.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** logs exist but are overwritten before the contract notification period or cannot be linked to unique users.

A.8.16 Monitor systems and activity

explain coverage, hours, thresholds, responsibilities and customer reporting. Price the service.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** the tender says continuous monitoring while alerts are reviewed next working day.

A.8.17 Synchronise clocks

critical for incident timelines, access records, submissions, evidence and distributed services.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** three systems record the same event in different time zones and the team cannot establish whether notification was on time.

A.8.18 Restrict powerful utility programs

limit administrative, diagnostic or extraction utilities used in demonstrations and support.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** a convenient export utility allows a contractor to download the complete customer dataset outside normal access restrictions.

A.8.19 Control software installation

prevent unapproved converters, browser extensions, plugins and AI tools from entering the pursuit environment.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** a designer installs a free PDF tool that uploads documents for processing.

A.8.20 Secure networks

address office, remote, cloud and customer connectivity; identify who owns each segment.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** the proposal describes encrypted application traffic but ignores an unmanaged wireless network used by the delivery team.

A.8.21 Define security for network services

include VPN, connectivity, DNS, firewall, managed network and customer links in supplier and service design.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** availability and incident obligations in the bid exceed the telecommunications provider agreement.

A.8.22 Segregate networks where risk requires

distinguish development, production, customer, administrative and guest environments.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** a demonstration environment shares credentials and connectivity with production because separation was considered too expensive.

A.8.23 Filter access to harmful web content

protect endpoints used for tender research and file acquisition while maintaining a controlled exception route.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** filtering is absent on contractor devices or so restrictive that users switch to personal equipment.

A.8.24 Use cryptography under controlled policy

support data in transit and at rest, secure transfer, backups and customer solutions. State boundaries and key ownership.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** the answer says AES-256 without explaining where encryption applies or who controls the keys.

A.8.25 Operate a secure development lifecycle

show governance from requirements and threat modelling through coding, testing, release, vulnerability and maintenance.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** the company has a secure development policy for its product but the bid relies on unmanaged scripts outside that lifecycle.

A.8.26 Define application security requirements

derive requirements from customer, risk, privacy, architecture, authentication, logging, resilience and provider obligations.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** security requirements are added after the application design and treated as optional hardening.

A.8.27 Use secure architecture and engineering principles

document trust boundaries, defence in depth, least privilege, secure defaults, resilience and shared responsibility.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** the architecture diagram uses security icons but has no design principles or threat assumptions.

A.8.28 Apply secure coding practices

verify that proposed development teams and subcontractors follow controlled practices.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** the tender quotes secure coding guidance while code review is optional and secrets appear in repositories.

A.8.29 Test security during development and acceptance

specify static and dynamic testing, vulnerability assessment, penetration testing, remediation and acceptance criteria.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** a penetration test is promised annually, but no test occurs before go-live and critical findings have no release threshold.

A.8.30 Control outsourced development

align subcontractor methods, code access, vulnerability, IP, evidence and customer flow-down.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** the prime promises a secure lifecycle that does not apply to the offshore component team.

A.8.31 Separate development, test and production

control environments, identities, data and deployment paths; use representative but protected test data.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** live customer data is copied into development because the demonstration needed realistic examples.

A.8.32 Control system and service changes

connect customer clarification, architecture change, provider update and price movement to risk, design, evidence and approval.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** a late feature is added to strengthen the bid but bypasses security testing and supplier review.

A.8.33 Protect test information

prefer synthetic or masked data; control access, copies and retention for demonstrations and validation.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** a sample customer dataset becomes permanent development content after the tender ends.

A.8.34 Protect operational systems during audit or testing

coordinate penetration tests, demonstrations, evidence collection and customer assurance with owners, windows, scope and recovery.

MINIMUM PROOF an approved owner, a risk or requirement link and objective evidence that the control operates.

> **WATCH FOR** an assurance test is run against production during a critical submission or service period without approved safeguards.

APMP-Aligned Lifecycle and ISMS Control Map

TOOLKIT PURPOSE

The APMP Winning Business Ecosystem describes the pursuit across pre-bid and capture, bid and proposal, post-bid and proposal, and implementation. This map preserves that professional lifecycle while placing information-security management where risk becomes real.

Stage 1 - Pre-bid and capture

Opportunity identification

APMP-aligned activity: understand markets, customers, routes, history and possible opportunities.

ISMS control: context, interested parties, information sources, asset ownership, lawful research, threat and supplier awareness.

When: continuously and when a new lead appears.

Minimum record: source, customer, likely information involved, route, owner, confidence and next action.

> **Security test:** has customer or competitor information been gathered through a permitted route and classified correctly?

Qualification

APMP-aligned activity: decide bid, no-bid, partner or defer using fit, return, competition, resource and risk.

ISMS control: risk criteria, information sensitivity, legal and contractual requirements, supplier dependency, capacity, authority and residual-risk boundaries.

When: after initial triage and again after material change.

Minimum record: criteria, rationale, information risks, owner, conditions, approval and re-gate trigger.

> **Security test:** would the organisation still pursue if headline value were removed and only the information, obligations and delivery exposure remained?

Capture strategy

APMP-aligned activity: build customer insight, competitive position, solution direction, partners, evidence and win themes.

ISMS control: source discipline, confidentiality, access boundaries, secure collaboration, early risk assessment, supplier assurance and information-flow design.

When: after qualification and through solicitation release.

Minimum record: known, inferred and unknown information; source; handling; stakeholders; solution concepts; suppliers; security actions and decisions.

> **Security test:** which insight is sensitive, who may use it and what decision did it change?

Pre-solicitation readiness

APMP-aligned activity: assemble people, tools, content, partners and response capability.
ISMS control: competence, managed devices, approved tools, role-based access, provider terms, workspace, incident route and continuity.
When: before expected release for strategic pursuits or immediately after qualification for short routes.
Minimum record: secure workspace, team roster, access, deputies, approved providers, handling rules and first forty-eight-hour plan.

> **Security test:** can every named person work securely at the time they are needed?

Stage 2 - Bid and proposal

Solicitation receipt and analysis

APMP-aligned activity: review solicitation, instructions, evaluation, deadlines and compliance.
ISMS control: controlled source receipt, malware handling, classification, customer property, access, document baseline, risk trigger and legal requirements.
When: immediately after receipt.
Minimum record: native file set, issue status, classification, access, integrity, amendments, security requirements and kill sheet.

> **Security test:** can the team prove which customer file and instruction set governed the response?

Bid planning

APMP-aligned activity: establish milestones, responsibilities, reviews, resources and internal dates.
ISMS control: security plan, information flows, risk assessment, treatment actions, access lifecycle, supplier review, incident and protected contingency.
When: after triage and requirements baseline; revise after material change.
Minimum record: campaign plan, risk owners, security gates, provider actions, assurance and release criteria.

> **Security test:** does the plan put controls before the information or commitment becomes difficult to change?

Solution and proposal development

APMP-aligned activity: develop solution, price, content and evidence.
ISMS control: secure design, risk treatment, SoA relevance, provider responsibility, controlled sources, personal data, AI use, version and material change.
When: from design input through approved content.
Minimum record: security requirements trace, risk and treatment, architecture, cost ledger, evidence, controlled drafts and promise register.

> **Security test:** do architecture, price, supplier agreements and narrative describe the same control environment?

Reviews

APMP-aligned activity: use strategy, solution, Pink, Red, Gold or equivalent reviews.
ISMS control: competent and independent assurance, secure reviewer access, verification, validation, finding severity, closure and residual-risk approval.
When: at defined maturity while meaningful change remains possible.
Minimum record: purpose, entry criteria, reviewer brief, evidence, findings, closure and decision.

> **Security test:** what security conclusion can the evaluator reach from the response, and what remains unsafe to believe?

Release and submission

APMP-aligned activity: complete production, final checks, upload and receipt.
ISMS control: approved source, hidden-content and metadata checks, file integrity, authorised identity and device, manifest, contingency, incident route and secure archive.
When: after content and risk approval, before protected contingency is consumed.
Minimum record: exact released files, approvals, manifest, hashes where used, portal verification and receipt.

> **Security test:** did the portal receive exactly the files that were authorised, through an approved route, without exposing more information than required?

Stage 3 - Post-bid and proposal

Clarification and evaluation support

APMP-aligned activity: respond to questions, presentations and demonstrations.
ISMS control: submitted baseline, secure communication, information minimisation, risk and design impact, authority and new commitment control.
When: from submission until the result and contractual position are final.
Minimum record: customer request, impact, response, approvals, changed promises and receipt.

> **Security test:** did a short answer create an unpriced security or incident obligation?

Negotiation and best-and-final offer

APMP-aligned activity: protect position, respond to customer need and revise the offer where permitted.
ISMS control: risk reassessment, security design change, supplier and price alignment, legal review, authority and revised release.
When: whenever the process permits negotiation or revision.
Minimum record: objectives, red lines, concessions, risk effect, revised baseline and formal confirmation.

> **Security test:** which control, resource or residual risk changed when price or contract changed?

Award, loss or cancellation

APMP-aligned activity: transition, debrief, analyse and close.
ISMS control: information retention and deletion, access removal, customer communication, incident review, corrective action, knowledge and secure handover.
When: immediately on formal notice and at planned review points.
Minimum record: result, security closure, archive, access removal, handover or learning.

> **Security test:** what information remains, why is it retained and who can still reach it?

Stage 4 - Implementation and contract learning

Mobilisation

APMP-aligned activity: launch the contract, deploy resources and align to the statement of work.
ISMS control: security promise register, access provisioning, screening, provider activation, architecture, risk treatment, incident readiness, testing and customer dependencies.
When: before contract start and through acceptance.

Minimum record: accepted security commitments, controls, owners, evidence, open risks and customer decisions.

> **Security test:** does the secure organisation described in the tender exist on day one?

Contract operation

APMP-aligned activity: manage deliverables, terms, change, reporting, invoices and relationships.
ISMS control: operational controls, monitoring, incidents, supplier performance, vulnerability, access, continuity, customer feedback and change.
When: throughout delivery.
Minimum record: control operation, reports, incidents, changes, audits, nonconformities and evidence.

> **Security test:** which security promise is currently difficult to deliver, and what controlled decision has followed?

Closeout and future opportunity

APMP-aligned activity: close the contract, capture lessons, archive and maintain the relationship.
ISMS control: exit, access removal, deletion, records, customer permission, risk update, evidence renewal and improvement.
When: at planned review, contract end and before future pursuits.
Minimum record: exit evidence, retained records, updated evidence cards, corrective actions and future opportunity inputs.

> **Security test:** what current security evidence did delivery create, and where can the next bid find it without exposing customer information?

The integrated six-gate route

Gate 0 - Market and route relevance. Decide whether the market and information environment belong inside strategy and risk appetite.

Gate 1 - Opportunity qualification. Decide bid, conditional bid, partner, defer or no-bid with information-security risk visible.

Gate 2 - Strategy and secure-solution commitment. Approve customer strategy, security design direction, providers and commercial boundaries.

Gate 3 - Response readiness. Confirm controlled sources, workspace, risk assessment, treatment, people, evidence and plan.

Gate 4 - Secure release. Authorise exact files after requirements, risk, evidence, price, provider and security assurance are complete.

Gate 5 - Result and transition. Mobilise, negotiate, investigate, learn, close access or retain records through the appropriate route.

Timing rules

- Put classification and access before broad distribution.
- Put risk assessment before secure architecture becomes fixed.
- Put supplier agreement before supplier capability becomes a promise.
- Put commercial reconciliation before security controls become contractual.
- Put independent assurance before production.
- Put incident and portal rehearsal before the final day.

- Put access removal and retention decisions at campaign closure.
- Put learning where the next risk and design decision can use it.

The Working Secure-Pursuit Process Pack

TOOLKIT PURPOSE

These are tool specifications, not mandatory templates. Build them in systems people already use where possible. Each field should support a decision, control or record. Remove fields without purpose. Add any required by customer, law, contract, risk, certification scope or scale.

Tool 1 - ISMS scope and secure-pursuit boundary

Purpose: define what the ISMS covers and how bid management fits.
Fields: legal entity; products and services; locations and remote work; information and systems; approved providers; start and end of the pursuit process; interfaces; interested parties; obligations; certification scope; approval and review trigger.

> **Control note:** describe outsourced activity and dependencies. Outsourcing does not remove risk ownership.

Tool 2 - Context and interested-party register

Purpose: keep relevant changes and requirements connected to action.
Fields: issue or party; source; requirement or consequence; process affected; risk or opportunity; owner; monitoring route; action; date; climate relevance where applicable.

> **Control note:** delete generic entries that do not affect a process, objective, scope or decision.

Tool 3 - Information and supporting-asset inventory

Purpose: know what must be protected across the pursuit.
Fields: asset ID; information or supporting asset; owner; location; provider; classification; confidentiality, integrity and availability need; access; retention; backup; disposal; linked process and risk.

> **Control note:** include local, downloaded, physical and supplier-held copies where material.

Tool 4 - Information-security risk register

Purpose: apply the approved method and retain risk decisions.
Fields: asset or activity; risk event; threat and vulnerability; consequence; existing controls; likelihood; impact; level; owner; acceptance criterion; treatment option; necessary controls; action; residual risk; approval; reassessment trigger.

> **Control note:** use one risk statement clear enough that another competent person can challenge the reasoning.

Tool 5 - Statement of Applicability

Purpose: record necessary controls, Annex A comparison, implementation and exclusions.
Fields: control reference; organisational description; included or excluded; justification; risk or requirement source; implementation status; owner; evidence; policy or process; action and review date.

> **Control note:** include necessary controls outside Annex A. An excluded Annex A control needs reason, not convenience.

Tool 6 - Risk-treatment plan

Purpose: turn risk decisions into funded work.
Fields: risk; treatment; control; action; owner; resource; dependency; target; acceptance criteria; verification; residual-risk decision; status.

> **Control note:** a planned action should have an implementation output and evidence, not only a completion date.

Tool 7 - Secure opportunity gate

Purpose: decide whether to pursue work with information and security exposure visible.
Identity: customer, route, lot, dates, value, owner and source.
Security triage: information classes; customer handling; personal data; security schedules; certifications; locations; providers; remote work; technical novelty; incident and continuity obligations.
Assessment: strategic fit; customer; capability; evidence; information risk; supplier; technology; legal; commercial; capacity and delivery.
Decision: bid, conditional bid, partner, defer or no-bid; conditions; owner; authority; re-gate trigger.

Tool 8 - Secure capture record

Purpose: control customer insight and pre-tender information.
Fields: source; date; classification; known, inferred or unknown; stakeholder role; permitted use; customer outcome; security requirement; competitor or incumbent information; design implication; partner; action; owner; expiry or review.

> **Control note:** lawful access does not automatically permit reuse in another opportunity.

Tool 9 - Tender baseline and handling record

Purpose: preserve authoritative customer inputs and establish security controls at receipt.
Fields: file or message; native source; issue status; date; classification; owner; malware check; authoritative location; working location; access group; amendment; integrity check; retention and customer rule.

> **Control note:** preserve native files. Label superseded material without destroying audit history.

Tool 10 - Security requirements trace

Purpose: connect customer and legal security requirements to risk, design, evidence and handover.
Fields: unique ID; exact source; requirement; type; mandatory or scored; information or system; risk; design response; control; provider; evidence; cost; owner; final response location; verification; change and handover.

> **Control note:** include security schedules, contracts, portal instructions and clarifications, not only scored questions.

Tool 11 - Pursuit access register

Purpose: authorise, review and remove access.
Fields: identity; organisation; role; information or workspace; requestor; approver; access level; privileged status; device or location conditions; start; expiry; review; removal; exception and evidence.

> **Control note:** connect the register to team and supplier status so withdrawal or role change creates an action.

Tool 12 - Supplier and cloud assurance record

Purpose: assess and control external services affecting the bid or offered solution.
Fields: provider; service; owner; criticality; information; location; subprocessors; certification and scope; security evidence; contract controls; incidents; continuity; exit; customer requirements; approval; monitoring and review.

> **Control note:** an existing corporate supplier still needs assessment for the proposed use and data.

Tool 13 - AI use register

Purpose: govern AI systems and opportunity-specific use.
Fields: system and service tier; owner; use case; data class; provider terms; retention and training; region; access; sources; human owner; prohibited use; disclosure requirement; testing; incident route; review.

> **Control note:** record meaningful use and risk. Do not create a list of ordinary spelling tools that obscures material processing.

Tool 14 - Secure solution design record

Purpose: control security architecture and transfer into price, answer and delivery.
Inputs: customer requirements, risk, information flow, legal and privacy obligations, provider limits, threat, business continuity and commercial boundaries.
Outputs: architecture; trust boundaries; access; data lifecycle; logging; incident; continuity; development; providers; customer dependencies; measures; evidence and open decisions.
Controls: review, verification, validation, risk treatment, change and approval.

Tool 15 - Security cost ledger

Purpose: ensure controls and services are resourced and priced.
Fields: requirement or risk; control; one-off and recurring resource; provider cost; volume assumption; customer dependency; contract treatment; measure; evidence; owner; decision.

> **Control note:** compare every material security promise with the commercial model before release.

Tool 16 - Security evidence card

Purpose: support accurate, controlled reuse of security proof.
Fields: claim; source; owner; entity and scope; date and period; method and sample; result; independent assurance; confidentiality; permission; limitation; review date; current status; approved use.

> **Control note:** certificate scope, penetration-test scope and performance scope are separate things.

Tool 17 - Security answer plan

Purpose: define the answer's job and safe inputs before writing.
Fields: question and score; required components; direct response; security design; risk and controls; customer consequence; evidence; provider; price; boundaries; commitments; classification; permitted tools; owner; reviewers; word allocation and gaps.

> **Control note:** provide minimum necessary information to contributors and external writers.

Tool 18 - Assurance and review record

Purpose: create objective review and closure.
Header: purpose, maturity, criteria, scope, classification, reviewers, competence, independence and secure handling.
Finding: requirement or risk; evaluator conclusion; evidence; severity; owner; action; affected outputs; verifier; closure; residual risk.

> **Control note:** score or assess confidence before editing language.

Tool 19 - Secure release and submission record

Purpose: authorise and prove release of exact files.
Criteria: baseline current; requirements verified; risk treatment current; SoA claims accurate; certificates and evidence checked; providers and price aligned; findings closed; hidden content removed; files inspected; portal rehearsed.
Manifest: lot; file; format; size; classification; approved source; hash where used; upload and verifier.
Receipt: status; reference; time; uploader; second checker; incident or exception.

Tool 20 - Security promise and handover register

Purpose: transfer tender security commitments into mobilisation and contract control.
Fields: promise; source; requirement; control; risk; owner; start date; measure; evidence; resource; provider; customer dependency; incident route; contract location; mobilisation action; acceptance and status.

> **Control note:** extract commitments during development and confirm them against the submitted baseline.

Tool 21 - Information-security event and incident record

Purpose: report, assess and control events and incidents.
Fields: reporter; time; event; information; systems and people; classification; initial containment; assessment; incident decision; severity; owner; customer and authority communication; evidence; recovery; lesson and corrective action.

> **Control note:** the reporting form should be accessible through a route that still works when the affected system does not.

Tool 22 - Nonconformity and corrective-action record

Purpose: correct failure and remove causes.
Fields: requirement not met; evidence; consequence; containment; correction; similar-risk check; cause analysis; action; owner; resource; date; ISMS and SoA effect; effectiveness method; result and closure authority.

> **Control note:** human error is incomplete where the system made the event likely or difficult to detect.

Tool 23 - KPI definition card

Purpose: ensure security measures support decisions.
Fields: name; purpose; definition; numerator; denominator; source; owner; frequency; target or threshold; segmentation; limitations; data-quality check; action trigger and reporting route.

Tool 24 - Internal audit pack

Plan: objective, scope, criteria, risk basis, sample, auditor, competence, independence, methods and timetable.
Evidence: people, records, observations, trails and control tests.
Finding: requirement, objective evidence, classification, owner and follow-up.
Report: conformity, effectiveness, strengths, systemic themes, actions and conclusion.

Tool 25 - Management-review pack

Inputs: prior actions; context; interested parties; objectives; performance; incidents; audit; risk and treatment; SoA; providers; resources; feedback; nonconformity and improvement.
Outputs: decisions on scope, policy, objectives, risk, controls, resources, suppliers, processes, certification and improvement.
Record: decision, rationale, owner, resource, date and follow-up.

The pack test

Choose one high-risk opportunity. Can the tools trace customer information and security commitments from source, through risk and treatment, into design, price, response, release, submission and delivery? If the answer requires duplicate data entry across ten disconnected spreadsheets, integrate before adding another template.

The Risk and Statement of Applicability Workshop

TOOLKIT PURPOSE

Use this workshop to build or refresh the risk-treatment and SoA position around end-to-end bid work. It assumes the organisation has approved risk criteria. If criteria do not exist, stop and define them first.

Participants

Keep the group small enough to decide. Include:

- ISMS or security lead;
- bid-process owner;
- information or service owner;
- technology and access owner;
- commercial or finance lead;
- delivery or solution lead;
- supplier owner where relevant;
- privacy, legal or continuity competence as needed;
- one person close to ordinary bid work.

The meeting needs risk owners or people able to obtain their decision. A room of advisers can analyse without accepting anything.

Preparation

Bring:

- approved scope and process map;
- information and asset inventory;
- context and interested-party requirements;
- customer and contractual security requirements;
- current risk method and criteria;
- existing risk register;
- current SoA;
- incidents, near misses, audit and customer feedback;
- supplier and cloud inventory;
- planned process or technology change.

Choose a representative pursuit. A Strategic consortium bid usually reveals more than a tidy low-risk quotation.

Session 1 - Establish the information route

Draw the pursuit from opportunity source to archive and handover. Mark where information enters, changes owner, crosses a boundary, is copied, leaves the organisation or becomes a contractual promise.

Ask:

1. What information exists here?
2. Who owns it?
3. Which confidentiality, integrity and availability needs apply?
4. Which legal, customer or supplier rule applies?
5. Which system, person, location or provider supports it?
6. What would make the consequence material?

Do not discuss controls for every box yet. Understand the route.

Session 2 - Write usable risk statements

Use a structure:

> **WORKING WORDS**
>
> [Information or process] may suffer [loss of confidentiality, integrity or availability] because [threat and vulnerability or condition], leading to [consequence for customer, organisation or another party].

Examples:

> **WORKING WORDS**
>
> Customer-confidential architecture may be disclosed to unauthorised partner personnel because guest access is inherited from a broad group and has no automatic expiry, leading to tender breach and loss of customer trust.

> **WORKING WORDS**
>
> The final pricing schedule may be corrupted or replaced because production and upload use uncontrolled local copies, leading to submission of an unapproved commercial offer.

> **WORKING WORDS**
>
> The bid process may become unavailable during the final review because collaboration and identity depend on one cloud service with no tested fallback, leading to missed deadline and lost opportunity.

Avoid cyber attack, human error and data breach as complete statements.

Session 3 - Verify existing controls

For each risk, identify controls currently relied upon and ask for evidence.

- Is the control implemented across the actual route?

- Does it cover external users and remote work?
- Who owns it?
- What evidence shows operation?
- What incident or exception shows its limit?
- Has the control changed since the last assessment?

Do not credit a policy where the live process bypasses it. Do not ignore a working control because it lacks a polished document.

Session 4 - Assess and evaluate

Apply approved likelihood and impact criteria. Record uncertainty. Identify risk owner.

Compare with acceptance criteria. Avoid averaging away a severe impact merely because likelihood is judged low without evidence.

Where customer or legal requirements impose a control, risk acceptance may not remove the obligation.

Session 5 - Select treatment

Choose avoid, reduce, share or retain, or another organisationally approved option. Identify necessary controls without beginning from Annex A.

For each treatment, record:

- intended effect;
- control or change;
- owner;
- resource;
- evidence;
- target date;
- residual risk;
- reassessment trigger.

Ask whether the control is organisational, people, physical, technological or a combination.

Session 6 - Compare against Annex A

Use Annex A as a completeness check. For each necessary control:

- Is there an equivalent Annex A reference?
- Has another relevant Annex A control been missed?
- Is an additional control outside Annex A needed?
- Does the current SoA include the control and correct justification?
- Does implementation status match reality?

Do not add a control solely because it exists in the list. Do not exclude one without reasoning.

Session 7 - Update the SoA

For each entry confirm:

- included or excluded;
- inclusion or exclusion justification;
- risk, legal, contractual or business source;
- implementation status;
- owner;

- evidence;
- treatment action;
- review date.

Check that necessary non-Annex-A controls are present.

Session 8 - Risk-owner approval

Risk owners approve treatment plans and residual risk. Escalate beyond tolerance. Record any condition or expiry.

A risk accepted for one short pursuit should not silently become a permanent enterprise position.

Two-hour version

0-15 minutes: scope, criteria and representative information flow.
15-45 minutes: write and refine the five most material risks.
45-70 minutes: verify current controls and rate risk.
70-95 minutes: select treatment and controls.
95-110 minutes: Annex A comparison and SoA update.
110-120 minutes: owners, resources, approvals and next review.

Quality checks

- Every risk has a named owner.
- Every high risk changes action or authority.
- Existing controls have evidence.
- Treatment actions have resources and acceptance criteria.
- Annex A comparison is visible.
- SoA status matches implementation.
- Residual risk is approved.
- Reassessment triggers are defined.
- The live bid plan contains the actions.

Friday test

Select one risk rated low and one rated high. Ask a person not in the workshop to explain why. If the evidence and criteria do not permit them to follow the reasoning, improve the record before the score becomes institutional memory.

Secure-Pursuit Audit Question Bank

TOOLKIT PURPOSE

Use these questions as routes through evidence, not as a script. Select samples and follow contradictions. Ask people to show work. A confident yes proves little until the trail reaches a record, action and result.

Trail 1 - Context, scope and leadership

1. What products, services, locations, remote work and pursuit activities sit inside the ISMS scope?
2. Which outsourced activities materially affect the scope?
3. Which internal issue changed secure bid work during the past year?
4. Which external issue changed it?
5. How was climate-change relevance determined?
6. Which interested party most recently created or changed a security requirement?
7. How is that requirement monitored?
8. What does top management do that demonstrates accountability beyond signing policy?
9. Which security objective is currently most important?
10. Which resource or commercial decision followed its performance?
11. Who owns information risk during a live pursuit?
12. Who may accept residual risk?
13. Who may stop release or submission?
14. How is an override recorded?
15. What happens when the bid manager and security lead disagree?

Trail 2 - Risk assessment, treatment and SoA

1. What risk method and criteria apply?
2. How are confidentiality, integrity and availability considered?
3. Select one risk. Which information and process are involved?
4. What threat and condition create the exposure?
5. Which consequence and affected party were considered?
6. Which existing controls were verified?
7. Who owns the risk?
8. How was likelihood and impact determined?
9. Which acceptance criterion applies?
10. What treatment option was selected?
11. Which controls were determined necessary?
12. How was Annex A used to check completeness?
13. Which necessary control sits outside Annex A?
14. Show the SoA inclusion or exclusion justification.
15. Does implementation status match evidence?

16. Who approved the treatment and residual risk?
17. Which action remains open?
18. How is effectiveness assessed?
19. When was the risk last reassessed?
20. What event would trigger early reassessment?

Trail 3 - Opportunity and capture

1. How did the opportunity enter the pipeline?
2. What sensitive or restricted information was involved before the notice?
3. How was source and permitted use recorded?
4. What security requirement could have caused no-bid?
5. Which certificate, clearance, provider or data condition was tested?
6. How did information risk affect opportunity class?
7. Which security cost or resource entered qualification?
8. What evidence supported the score?
9. Was a partner or cloud service assumed before assurance?
10. Which capture information was known, inferred or unknown?
11. How were stakeholder and competitor details protected?
12. Which insight changed security design?
13. What happened when the formal solicitation contradicted capture?
14. When was the pursuit re-gated?
15. How was an unsuccessful opportunity closed securely?

Trail 4 - Tender intake and workspace

1. Who received the tender and preserved the native files?
2. How were malware, macros or unusual formats handled?
3. Which classification and customer handling rules applied?
4. Where is the authoritative source baseline?
5. Who can access it and why?
6. How are external users approved?
7. Which identity, device and location conditions apply?
8. How are access expiry and removal triggered?
9. How are amendments and clarifications baselined?
10. What prevents unapproved local copies becoming authoritative?
11. Which backup or recovery route exists?
12. When was it tested?
13. How are confidential calls, screens, printouts and meeting rooms controlled?
14. How will the workspace close after submission or loss?
15. Which audit logs are retained and who reviews them?

Trail 5 - Security requirements and design

1. Select one security requirement from the customer's source.
2. Where was it interpreted and approved?
3. Which risk and design input does it create?
4. What information flow and trust boundary are involved?

5. Which customer, supplier and bidder responsibilities apply?
6. What alternatives were considered?
7. Which security architecture or control was selected?
8. How was it verified against requirements?
9. How was it validated under realistic conditions?
10. What fails first under doubled volume or loss of a key provider?
11. Which residual risk remains?
12. Which treatment and SoA controls apply?
13. Where is the control priced?
14. Which evidence supports it?
15. What changed after clarification or review?
16. Who approved the change?
17. Can delivery use the design output?
18. Which customer dependency is stated?
19. Which incident and recovery action exists?
20. Does the narrative describe the same service?

Trail 6 - People, suppliers, cloud and AI

1. How was competence defined for the selected role?
2. Which screening or clearance applies?
3. What security duties sit in terms or agreements?
4. What live-pursuit awareness was provided?
5. How is remote work controlled?
6. How can the person report an event?
7. What happens after role change or departure?
8. Select a supplier. What information or service does it control?
9. How was the supplier selected and assured?
10. Which customer requirements flowed into the agreement?
11. What incident and notification terms apply?
12. How are supplier changes monitored?
13. What exit or deletion route exists?
14. Select a cloud service. Who owns configuration, access, logging, backup and deletion?
15. Which data classes may enter it?
16. Select an AI use. Which provider terms and sources apply?
17. Who is accountable for the output?
18. What is prohibited?
19. How would a provider incident affect the bid or proposed service?
20. What evidence led to the latest re-evaluation?

Trail 7 - Writing, evidence and assurance

1. What was the security answer intended to prove?
2. Which sources were approved?
3. How was information minimised for contributors?
4. Which personal or customer data was used?
5. How was classification preserved in extracts and drafts?
6. Did AI or an external writer contribute?

7. Which source supports the main security claim?
8. Is certificate scope accurate?
9. Which claims use absolute language?
10. Who approved technical and contractual truth?
11. Which provider confirmed the commitment?
12. Where is the commitment priced?
13. What review purpose and entry criteria applied?
14. Were reviewers competent and sufficiently independent?
15. Which critical or major finding was raised?
16. What evidence proved closure?
17. What was validated rather than only read?
18. Which residual risk was accepted?
19. Did hidden comments, metadata or attachments remain in final files?
20. Can the released text be traced to the approved source?

Trail 8 - Release, submission and archive

1. Which release criteria applied?
2. Who authorised the exact files?
3. What security exception remained?
4. Which account and device were used to submit?
5. Was portal access rehearsed?
6. Did the manifest contain every required file and field?
7. How was file integrity checked?
8. Who independently verified portal contents?
9. Which receipt or evidence remains?
10. What contingency route existed?
11. How would a compromised account change the decision?
12. Were live working copies restricted after release?
13. How were clarifications controlled against the submitted baseline?
14. Which information is retained and for how long?
15. Which copies were deleted or returned?
16. When was external access removed?
17. How is the archive protected and retrievable?
18. What evidence would support a challenge or incident reconstruction?
19. How is customer information separated from reusable knowledge?
20. What is the secure closure record?

Trail 9 - Incident, continuity and handover

1. How can staff report an event during a system outage?
2. Who assesses whether it is an incident?
3. Which severity criteria apply?
4. Who may contain access or stop submission?
5. How is evidence preserved?
6. Which customer and authority notification routes apply?
7. When was the incident plan exercised?
8. Which weakness did the exercise reveal?

9. What continuity route protects confidentiality, integrity and availability?
10. When was backup restoration tested?
11. Which single supplier or identity dependency remains?
12. After award, how are security promises extracted?
13. Who accepts them in delivery?
14. Which control must be implemented before contract start?
15. Which promise was disputed?
16. How was it resolved?
17. How are access and information moved from pursuit to operation?
18. What customer dependencies remain open?
19. Which performance evidence will return to future bids?
20. What incident or nonconformity changed the process?

Trail 10 - Monitoring, audit, management review and improvement

1. What question is the selected security KPI intended to answer?
2. Is its definition stable and complete?
3. Which data source and owner apply?
4. What limitation exists?
5. What decision followed the latest result?
6. How is control effectiveness distinguished from completion?
7. How is customer perception monitored?
8. Why was this area selected for internal audit?
9. What criteria and scope applied?
10. Was the auditor competent and sufficiently independent?
11. What objective evidence supports the finding?
12. How was correction separated from corrective action?
13. Did cause analysis move beyond human error?
14. Where else could the issue occur?
15. How was effectiveness defined?
16. Which risk, SoA entry or process changed?
17. Did management review receive context, risk, incidents, audit, objectives and provider information?
18. Which decision and resource followed?
19. How was action completion verified?
20. Which recent improvement removed work while maintaining or improving security?

Auditor's discipline

- Ask for current examples rather than normally.
- Follow one awkward trail deeply.
- Distinguish absence of evidence from evidence of absence.
- Protect sensitive audit information.
- State criteria before findings.
- Do not advise so extensively that independence disappears.
- Test effectiveness, not only document presence.
- Report strengths accurately as well as failures.
- Follow up until material corrective action is shown to work.

Realistic Security Scenario Playbook

TOOLKIT PURPOSE

These scenarios are ordinary on purpose. Most information-security failures in bids begin as plausible decisions made by busy people. Use four horizons: now, before the next irreversible decision, before submission or delivery, and after the result.

Scenario 1 - The tender pack contains a malicious macro

The pricing workbook opens with a warning. A colleague says macros must be enabled or the formulas will not work.

Now: preserve the native file, isolate and scan it using the approved environment. Confirm whether the macro is signed, expected and required. Do not disable protection across the device.

Before use: involve competent IT or security support, compare with the portal source and seek customer clarification if integrity is uncertain. Provide a contained environment where the workbook can operate safely.

Before submission: verify that the completed file retains required functionality and no security workaround remains on the device.

Afterwards: update unusual-file handling and record any event or near miss.

Scenario 2 - A partner asks for full workspace access

The consortium architect says granular access will delay work and requests the whole bid room.

Now: identify the work package and information actually required. Do not grant full access by urgency.

Before access: complete provider assurance, terms, identity, device and location checks. Create named least-privilege access with expiry.

Before review: confirm the partner can reach necessary inputs and that the prime can integrate outputs without disclosing pricing, legal advice or personal data unnecessarily.

At closure: remove access, obtain return or deletion evidence where required and evaluate the relationship.

Scenario 3 - A director forwards a restricted document to personal email

The corporate service is unavailable and the director wants to continue from home.

Now: contain the transfer, assess whether the message left organisational control and activate the event-reporting route. Preserve evidence.

Before work continues: provide an approved alternative, reset credentials or secure the information as needed. Decide whether customer notification is required.

Before release: verify no uncontrolled copy influenced the final baseline and that the director's access route is safe.

Afterwards: examine availability, manager behaviour and exception design. Do not close with a reminder email alone.

Scenario 4 - The certificate scope does not cover the proposed service

The bidder has a valid ISO/IEC 27001 certificate, but the scope covers software development at one site. The tender is for a managed service delivered by another entity.

Now: stop the blanket certification claim. Verify entity, scope, locations and current status.

Before response approval: decide what assurance genuinely transfers, what additional evidence can be provided and whether future scope extension is only a plan.

Before submission: describe certification accurately and ensure all schedules use the same wording.

After the result: consider whether business strategy justifies extending scope; do not alter certification solely to repair one sentence.

Scenario 5 - The AI assistant invents an incident statistic

A fluent draft states that the organisation has experienced no material security incidents in five years. Nobody knows the source.

Now: quarantine the claim and search every location where it may have propagated.

Before review: inspect prompt, retrieval and source records. Replace the statement with verified evidence or remove it.

Before submission: run a bounded check for numbers, absolute claims, certificate status and incident language. Obtain named factual attestation.

Afterwards: improve source markers, refusal behaviour, user competence and AI-use controls. Test effectiveness with representative work.

Scenario 6 - A customer clarification requires thirty-minute notification

The current incident process uses four hours for initial assessment and the critical supplier allows twenty-four hours.

Now: do not confirm from memory. Assess the requested definition, clock and scope.

Before answering: involve security, legal, supplier, operations and finance. Design an achievable acknowledgement, assessment and notification route or seek clarification.

Before final commitment: update risk, supplier terms, resource, price, incident procedure and promise register.

After award: exercise the route before service start.

Scenario 7 - A reviewer downloads the data room to work offline

The reviewer is authorised but will be travelling without stable connectivity.

Now: determine classification, device, location and customer restrictions. Remove the copy if the route is not approved.

Before review: provide managed offline access or an approved contingency pack with encryption, expiry and clear scope where risk permits.

Before closure: reconcile comments into the authoritative version and confirm deletion of local material.

Afterwards: decide whether offline review is a recurring business need requiring a formal control.

Scenario 8 - A supplier changes cloud region during the bid

The SaaS provider announces that new customers will be hosted in another region. The tender requires UK processing.

Now: identify which data and service are affected and whether existing tenants differ from new ones.

Before solution freeze: obtain provider evidence, contract position and subprocessor information. Reassess privacy, security, customer requirements and exit alternatives.

Before submission: change provider, negotiate a suitable region, redesign the use or disclose an accurate boundary. Update risk, SoA, architecture and price.

Afterwards: strengthen supplier-change monitoring and notification requirements.

Scenario 9 - A laptop is lost on the train during final review

The device is managed and encrypted. It contains cached customer documents and an active collaboration session.

Now: report, revoke sessions, locate or wipe the device, assess exposure and preserve the timeline. Do not assume encryption ends the event.

Before work resumes: provide a replacement through the controlled route, review identities and confirm authoritative files remain intact.

Before submission: check whether customer notification or risk acceptance is required and whether the incident affected file integrity or availability.

Afterwards: review travel, session, local caching and incident-response controls.

Scenario 10 - Red review adds a new monitoring service

Reviewers say the security response lacks detection. The writer adds continuous monitoring and a dedicated analyst.

Now: mark the change as design and commercial, not editorial.

Before closure: confirm tool, coverage, staffing, provider, alert response, evidence and cost. If the service is not real, remove it.

Before release: update architecture, risk treatment, SoA, pricing, supplier agreement, incident process and promise register.

Afterwards: measure how often late reviews create unpriced security design and move the relevant assurance earlier.

Scenario 11 - The portal is impersonated

A message appearing to come from the procurement portal asks the uploader to sign in through a new link because the deadline has changed.

Now: do not use the link. Verify through the known portal address and published support route. Report the event.

Before submission: review account activity, reset or revoke credentials if exposure occurred and confirm the authoritative deadline. Alert the team through controlled communication.

Afterwards: update phishing scenarios, domain verification, portal bookmarks and event intelligence. Consider whether other bidders or customer contacts need notification through the proper route.

Scenario 12 - Delivery rejects a security promise after award

The tender commits to monthly access certification across all subcontractors. Delivery says its provider platform cannot produce the data and the cost was not included.

Now: compare submitted wording, provider agreement, price and contract. Escalate before the first report is due.

Before mobilisation acceptance: add a workable process and resource, negotiate through the proper route or resolve the contractual position. Assign owner and evidence.

Before service start: test the certification report and supplier response.

Afterwards: raise nonconformity where appropriate and change promise extraction, provider approval and commercial reconciliation.

Scenario 13 - The internal audit finds the SoA overstated

Several controls are marked fully implemented because policy documents exist, but sampled bids show inconsistent operation.

Now: correct misleading status and assess affected risks. Do not create retrospective evidence.

Before certification audit: prioritise material gaps, implement controls, update treatment actions and obtain residual-risk decisions. Verify live operation.

Afterwards: improve SoA ownership, evidence links, control-effectiveness review and management oversight.

Scenario 14 - Severe weather closes the primary office on submission day

The plan assumes the bid team will gather in the secure war room. Travel is suspended and power is intermittent.

Now: activate the tested continuity route. Confirm people, identities, secure devices, authoritative files, communication and submission authority.

Before upload: use approved remote locations and backup connectivity. Maintain classification, access, independent verification and incident reporting.

Afterwards: assess climate relevance, office concentration, utilities, home-working readiness and whether the fallback preserved all three security properties.

Scenario method

For any new scenario, answer:

1. What information and service are affected?
2. Which confidentiality, integrity and availability consequences matter?
3. What must be contained now?
4. What is the next irreversible decision?
5. Which roles and authorities are required?
6. Which customer, legal or supplier clock applies?
7. What evidence must be preserved?
8. Which design, risk, SoA, price or commitment changes?

9. What proves recovery?
10. What must change before recurrence?

Ninety-Day Implementation Calendar

TOOLKIT PURPOSE

This calendar is a practical implementation sequence, not a guarantee of certification in ninety days. Existing maturity, scope, audit availability, risk and certification-body timing differ. One accountable implementation lead should coordinate the build without becoming owner of every control.

Week 1 - Decide why and where

Leadership: agree business case, intended outcomes, sponsor, authority, resources and certification intention.
Process: draft scope; identify services, locations, remote work, pursuit stages, technology, suppliers and interfaces.
Evidence: charter, resource decision, draft scope and selected live proving pursuits.
Friday question: what should become safer, easier or more predictable because the ISMS exists?

Week 2 - Understand context and requirements

Review strategy, customers, law, contracts, threat, technology, workforce, suppliers, privacy and climate relevance. Identify interested parties and their relevant requirements.
Evidence: context and interested-party registers, climate decision, legal and contractual obligations, monitoring owners.

> **Live test:** which issue from the current bid was absent from the workshop?

Week 3 - Map information and process

Map opportunity, capture, intake, workspace, risk, design, writing, review, submission, incident, handover and closure. Map information flows, trust boundaries and supporting assets.
Evidence: process architecture, information-flow map, asset inventory, owners and interfaces.

> **Live test:** follow one customer file and one security promise through the route.

Week 4 - Leadership, policy and objectives

Approve a usable policy. Define roles, risk and release authority, deputies and escalation. Set a small number of measurable security objectives.
Evidence: policy, authority matrix, objectives, leadership communication and first operating decisions.

> **Live test:** use the authority matrix when a genuine disagreement occurs.

Week 5 - Risk method and criteria

Define risk assessment, acceptance criteria, impact and likelihood, ownership, review and uncertainty. Train the people who will apply it using one live scenario.
Evidence: approved method, criteria, exercise and competence record.

> **Live test:** can two competent people reach comparable reasoning from the same facts?

Week 6 - Assess risk and build the SoA

Identify and evaluate risks. Verify existing controls. Select treatment, compare with Annex A and create the SoA and treatment plan. Obtain owner approval.

Evidence: risk register, SoA, treatment plan, residual-risk decisions and priority actions.

> **Live test:** select one exclusion and one partly implemented control. Can both be defended?

Week 7 - Control identities, information and workspace

Implement classification, labelling, access, identity lifecycle, authentication, transfer, customer property, secure workspace, backup, remote work and physical handling.

Evidence: access register, handling rules, workspace configuration, recovery test and closure route.

> **Live test:** onboard and remove one external contributor.

Week 8 - Suppliers, cloud and AI

Tier providers by risk. Review agreements, assurance, cloud responsibility, subcontractors, incident, continuity and exit. Establish approved AI use, data boundaries and accountability.

Evidence: provider records, contracts, cloud register, AI use register and monitoring plan.

> **Live test:** follow one provider claim from evidence to tender answer and price.

Week 9 - Secure design and content production

Implement security requirements trace, design, risk-treatment integration, cost ledger, evidence cards, secure writing, claims control and material-change assessment.

Evidence: solution record, architecture, validation, commercial reconciliation, evidence and answer plans.

> **Live test:** run one difficult-day scenario and trace the result into price and narrative.

Week 10 - Assurance, release, incident and handover

Define review purposes, competence, findings, closure, release, manifest, portal, incident, archive and security promise handover. Rehearse a portal or incident failure.

Evidence: review record, release criteria, submission manifest, incident exercise and handover acceptance.

> **Live test:** ask delivery to explain three security promises before award.

Week 11 - Competence, awareness and measures

Assess role competence. Provide practical learning and evaluate it. Define a minimum balanced scoreboard and data-quality checks.

Evidence: competence matrix, assessments, awareness, KPI cards and first results.

> **Live test:** ask what decision each measure would cause if it turns red.

Week 12 - Internal audit and corrective action

Conduct risk-based internal audits across live and completed work. Raise precise findings. Contain and correct issues. Begin cause-based corrective action with effectiveness criteria.

Evidence: audit programme, plans, reports, findings, actions and follow-up.

> **Live test:** verify a control in operation rather than accepting a document.

Week 13 - Management review and readiness

Present context, requirements, objectives, performance, incidents, audit, risks, treatment, SoA, providers, resources and improvement. Top management decides and funds action.

Complete readiness assessment. Stabilise the system and plan certification or further implementation.

Evidence: management review, decisions, readiness report, evidence index and open-action plan.

Final question: can a competent person operate the system next week without the implementation lead translating it?

Operating cadence after day ninety

Daily during live bids: control new information, access, changes, incidents and blocked security decisions.

At each gate: review risk, treatment, providers, evidence, resource and acceptance criteria.

Weekly: review high-risk pursuits, external access, supplier actions, vulnerabilities, evidence gaps and approaching irreversible dates.

Monthly: review objectives, incidents, near misses, measures, treatment, providers, competence and corrective action.

Quarterly or planned interval: conduct management review at suitable depth, revisiting context, interested parties, scope, climate relevance, risk, SoA and improvement.

Annually and after material change: review scope, policy, risk method, audit programme, continuity, provider strategy, retention and certification arrangements.

Control Plans by Opportunity and Information Class

TOOLKIT PURPOSE

The same ISMS should not force every pursuit through identical control depth. Define classes before the deadline. Each class should state mandatory controls, permitted simplifications, escalation and evidence. Reclassify when new information changes risk.

Class 1 - Public-information quotation

The customer asks for a short quotation using public requirements. No personal data, customer-confidential material, novel technology or critical supplier is involved.

Minimum controls: opportunity record; source baseline; approved workspace; named owner; price and factual approval; managed device; final release; receipt and archive.

Permitted simplification: short risk check, combined review and simple access list.

Escalate when: contract introduces unusual security duties, customer provides non-public data, remote external contributors join or the service itself has significant security consequence.

Class 2 - Standard confidential tender

The pack is customer-confidential and contains commercial or operational information. The response uses employee profiles and current corporate evidence.

Minimum controls: classification; role-based workspace; guest approval; requirements trace; risk assessment; evidence and claims check; supplier review; final hidden-content and metadata check; access removal and retention.

Escalate when: personal data becomes extensive, architecture is shared, data crosses borders or a critical security schedule appears.

Class 3 - Personal-data-rich pursuit

The bid uses CVs, user data, case records, research datasets or a demonstration involving personal information.

Minimum controls: privacy and security assessment; data minimisation; lawful and transparent use; restricted access; masking or synthetic data where possible; transfer and retention; incident and deletion evidence.

Escalate when: special-category or criminal-offence data, vulnerable people, large scale, automated decision-making, re-identification risk or international transfer is involved.

Class 4 - Security-sensitive technical tender

The customer provides network diagrams, vulnerabilities, configurations, system access or security architecture. The offered service includes technical security controls.

Minimum controls: restricted technical workspace; strong identity and managed endpoints; privileged-access control; threat and vulnerability review; secure architecture; provider assurance; technical validation; incident and evidence handling; secure release.
Escalate when: national-security, defence, critical infrastructure, live credentials, exploitable vulnerability or customer operational access is involved. Apply customer classification and handling schemes exactly.

Class 5 - Consortium or supplier-dependent pursuit

Several legal entities need information and contribute to the offered service.
Minimum controls: role and information boundaries; supplier tiering; agreements; identity and device conditions; least-privilege access; secure transfer; joint design and claim approval; incident alignment; access removal and deletion.
Escalate when: a partner controls critical data, privileged access, certification, source code, monitoring or mobilisation. A partner change triggers risk and design reassessment.

Class 6 - Cloud- or AI-intensive pursuit

The bid process or solution relies materially on SaaS, cloud infrastructure, AI, automation or outsourced technology.
Minimum controls: service owner; approved use; provider and subprocessor review; regions; data classes; identity; configuration; logging; retention; training use; output verification; shared responsibility; incident and exit.
Escalate when: customer-confidential or sensitive personal data enters the service, models generate security decisions, provider terms change, or service availability is critical to submission or delivery.

Class 7 - Strategic or regulated pursuit

The contract could materially affect organisational stability, public safety, regulated services, vulnerable users or reputation.
Minimum controls: enhanced leadership gate; formal information-risk assessment; risk-owner decisions; deeper supplier and technical assurance; independent review; incident and continuity rehearsal; commercial security ledger; secure mobilisation and post-award monitoring.
Permitted simplification: very little around critical controls. Administrative form can still be streamlined.
Escalate when: residual risk exceeds tolerance, required evidence is absent, pre-contract activity is necessary, or the organisation would need to become materially different to deliver.

Class 8 - Urgent or disrupted pursuit

The response period is unusually short or normal systems, people or premises are unavailable.

> **Non-negotiable controls:** authoritative source; qualification; classification; secure access; factual and commercial ownership; security risk decision; release authority; exact file verification; incident reporting.
> **Simplify first:** meeting ceremony, duplicate trackers, low-value graphics and optional content.
> **Do not simplify first:** customer handling, provider truth, price-security reconciliation, critical review, identity and submission verification.

Escalate when: there is insufficient time for a legal, technical or risk decision, the secure route is unavailable or final authority cannot be obtained. No-bid or customer clarification may be the secure control.

Information handling overlay

Apply a simple handling overlay across opportunity classes.
Public: approved for public release. Integrity and source still matter.
Internal: ordinary business information not intended for public release. Use approved systems and access.
Customer Confidential: information provided or created under customer confidentiality. Restrict to the named purpose and team; control external transfer and retention.
Restricted: high-consequence technical, personal, legal, national-security or commercially sensitive information requiring explicit access, stronger transfer, monitored use and planned disposal.

Map customer labels to the internal scheme. The customer's requirements take precedence for their information.

Classification decision card

Record:

- opportunity and owner;
- opportunity class;
- information classes;
- reasons and sources;
- mandatory controls;
- approved simplifications;
- escalation thresholds;
- reviewer and release authority;
- reclassification trigger;
- closure and retention.

The purpose is not to make every bid strategic. It is to stop a low-value opportunity with severe information exposure being treated as routine because the sales number is small.

Role-by-Role Secure-Pursuit Guide

TOOLKIT PURPOSE

Job titles vary. Combine roles in small organisations, but preserve ownership, authority and sufficient challenge.

Top management

Owns: ISMS effectiveness, scope, policy, objectives, risk appetite, resources and management review.

Enter: strategic qualification, high residual risk, resource conflict, major incident, certification and material change.

> **Do not:** delegate security accountability to the ISMS manager or bypass release because the deadline is close.

Evidence: decisions, resources, objectives, review and risk acceptance.

ISMS or information-security manager

Owns: ISMS coordination, risk method, SoA governance, monitoring, audit support and security integration.

Enter: scope, risk, high-risk pursuits, provider or technology change, incidents, assurance and improvement.

> **Do not:** become owner of every risk or complete records after business decisions have already happened.

Bid-process owner

Owns: design, performance and improvement of secure end-to-end pursuit processes.

Enter: process design, objectives, repeated failures, interface disputes, management review and change.

> **Do not:** confuse ownership of the process with factual ownership of every tender statement.

Bid or proposal manager

Owns: integration of the live campaign, including source baseline, workspace, plan, risk actions, access, reviews, release and closure.

Enter: from triage through archive and handover.

> **Do not:** accept unowned security claims, informal access or private customer communications.

Information owner

Owns: classification, acceptable use, access, retention and risk decisions for assigned information.

Enter: at receipt, sharing, material change, release and disposal.

> **Do not:** assume technology ownership equals information ownership.

Information-security risk owner

Owns: understanding, treatment and residual-risk acceptance within authority.
Enter: assessment, treatment, material change, exception and management review.

> **Do not:** sign risks without authority over the business consequence or treatment resource.

Capture or opportunity lead

Owns: lawful customer insight, source discipline, pre-tender information and security implications.
Enter: before formal solicitation and at strategy reset.

> **Do not:** represent rumour as customer requirement or retain sensitive intelligence in personal notes.

Solution or security architect

Owns: coherent, secure and deliverable service design, trust boundaries, shared responsibility, verification and change.
Enter: before full writing and remain through negotiation and mobilisation.

> **Do not:** approve architecture detached from provider evidence, price, risk or customer dependency.

Commercial or finance lead

Owns: security-control cost, pricing, assumptions, cash, provider charges and commercial approval.
Enter: qualification, design, risk treatment, late change, negotiation and handover.

> **Do not:** cut controls without tracing risk and contractual consequence.

Privacy, legal or contracts adviser

Owns: competent advice on relevant privacy, legal and contractual issues within authority.
Enter: qualification, requirements, data use, supplier terms, incident, negotiation and retention.

> **Do not:** arrive as a late signature after the operational model has already assumed the answer.

Subject-matter expert

Owns: technical or operational truth, constraints, evidence and approval.
Enter: requirements, risk, design, writing, review and handover.

> **Do not:** approve a polished answer without checking the control works in the actual service.

Bid writer

Owns: responsive and accurate communication from controlled sources.
Enter: answer planning through approved content.

> **Do not:** invent controls, use unapproved tools, expand evidence beyond scope or convert aspiration into promise.

Reviewer or assurance lead

Owns: objective evaluation against defined criteria, risk and intended customer confidence.
Enter: when entry criteria are met and change remains possible.

> **Do not:** begin with grammar, use insecure review tools or close findings without evidence.

Production and submission owner

Owns: final formatting, hidden-content checks, file integrity, manifest, portal and receipt.
Enter: during planning and rehearsal, not only at the deadline.

> **Do not:** alter approved security content or use an unassessed converter.

Supplier or partner manager

Owns: selection, agreement, access, assurance, performance, change and exit of external providers.
Enter: capability-gap identification through handover and service operation.

> **Do not:** treat a logo, certificate or old relationship as current capacity and commitment.

Technology, cloud or AI owner

Owns: approved platforms, configuration, data classes, access, provider terms, logging, incident and exit.
Enter: procurement, change, new use case, integration and incident.

> **Do not:** imply that enterprise licensing guarantees security or truth.

Incident lead

Owns: event assessment, containment, response coordination, evidence, recovery and communication governance.
Enter: preparation, exercise, suspected event and post-incident review.

> **Do not:** let the bid deadline determine whether a security incident is serious.

Internal auditor

Owns: objective evidence and conclusions against defined criteria.
Enter: according to the risk-based programme and after material change or failure.

> **Do not:** audit only documents or design the full corrective action and then verify it personally.

Delivery or mobilisation lead

Owns: acceptance and operation of security commitments after award.
Enter: qualification, design, pre-release validation, award and contract performance.

> **Do not:** meet the security answer for the first time during handover.

The five-question responsibility test

1. Who performs the activity?
2. Who owns the result or risk?
3. Who supplies facts or approval?
4. Who must be informed?
5. Who may stop, override, accept or release?

Where one name fills every field, design the least burdensome independent challenge that still protects the customer and organisation.

The Secure Pursuit Clock

TOOLKIT PURPOSE

This clock assumes a twenty-working-day tender. Adjust to the actual procurement, opportunity class and risk. Do not turn the example into a rule that overrides customer dates.

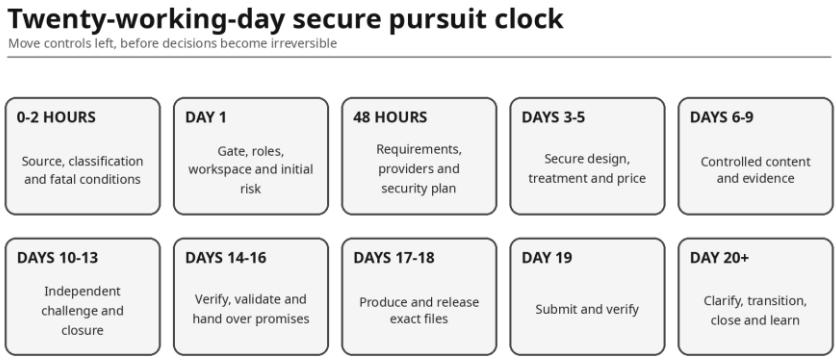

Figure 11 - The secure pursuit clock places information-security decisions before they become irreversible.

The first two hours

Preserve the notice and native files. Confirm source, deadline, clarification deadline, lots, portal, customer handling and first owner. Scan or isolate unusual files. Identify information classes, personal data, security schedules and conditions that may prevent participation.

Establish the authoritative source location. Do not distribute the pack widely before access and handling are known.

Output: controlled source pack, initial classification, first security kill-sheet items, owner and triage time.

By the end of day one

Complete rapid qualification. Review security requirements, certificate or clearance conditions, customer information, provider dependencies, technical novelty, locations, remote work, legal exposure, incident timing and delivery capacity.

Decide bid, conditional bid, hold, partner or no-bid. Appoint bid, security, solution and commercial owners. Establish the secure workspace, access groups, incident route and decision log.

Output: gate decision, workspace, team roster, initial risk, security requirements and immediate actions.

The first forty-eight hours

Baseline customer documents and amendments. Build the security requirements trace. Begin contract, privacy and supplier review. Identify information assets, trust boundaries and initial risks. Set security gates, evidence requests, review purposes, provider actions, release route and protected contingency.

Transfer capture information only through approved sources and discard assumptions contradicted by the solicitation.

Output: usable baseline, security matrix, risk-assessment plan, access register, supplier actions, review calendar and clarification list.

Days three to five - decide the secure design

Agree design inputs, information flows, shared responsibility, identity, access, data lifecycle, logging, incident, continuity, providers and customer dependencies. Assess risks and select treatment. Compare controls against Annex A and update the SoA where the pursuit changes the ISMS.

Build cost from the same design. Identify evidence and validation.

Output: reviewed security design, current risk and treatment, provider position, priced controls, evidence plan and answer positions.

Days six to nine - build controlled content

Develop answers from controlled sources and approved design. Limit information to contributors' need. Track AI and external-provider use. Extract claims and commitments. Verify certificate and evidence scope. Keep narrative, architecture, price and supplier agreements aligned.

Run an outline or Pink review where useful. Close clarifications and reassess material changes.

Output: complete answer logic, current evidence, controlled drafts, promise register, owned gaps and revised risk decisions.

Days ten to thirteen - challenge while change remains possible

Run security solution, technical and evaluator-style reviews. Test the difficult day. Classify findings. Treat any new monitoring, service level, provider or control as a design and price change.

Close critical and major findings with evidence. Obtain residual-risk decisions. Do not allow review material to escape the controlled environment.

Output: assurance findings, approved changes, updated risk and SoA position, reconciled price and residual-risk list.

Days fourteen to sixteen - verify and validate

Verify requirements, claims, certificates, providers, architecture, data, access, incident timing, continuity, price and cross-document consistency. Validate through rehearsal, tabletop, test or service walkthrough where proportionate.

Extract final security promises and obtain delivery and supplier acceptance. Approve content baseline.

Output: technically and commercially approved content, validation evidence, promise register and production baseline.

Days seventeen to eighteen - produce and release

Complete formatting, accessibility, hidden-content and metadata checks, file naming, size and manifest. Compare produced documents with approved source. Test portal access and authorised devices. Prepare hashes or other integrity checks where proportionate.

Hold final release review. Confirm risk, evidence, providers, price, exact files, contingency and authority. This is not a late opportunity to invent stronger security claims.

Output: released file set, manifest, approval and upload readiness.

Day nineteen - submit under control

Upload before the internal deadline using named authorised access and an approved device. One person uploads; another verifies. Preserve receipts, portal status, timestamps and incident evidence.

If the portal fails, follow the rehearsed route. If a security event occurs, protect information and account integrity before urgency drives the wrong action.

Output: verified submission and controlled archive baseline.

Day twenty and after - remain accountable

Monitor customer messages. Control clarification, presentations and negotiation against the submitted baseline. Every new security commitment receives appropriate technical, risk, provider and commercial approval.

Remove unnecessary live access. Preserve required records. Prepare conditional routes for award, loss, delay and incident.

Output: post-submission control and secure campaign closure plan.

Within one working day of the result

If successful, open mobilisation and transfer security promises, risk, providers, access and customer dependencies. If unsuccessful, retain the record, remove access, return or delete information and separate legal review from learning. If delayed, review continuing access, supplier commitments and data retention.

Within thirty days

For a win, compare security assumptions with mobilisation reality, test critical controls and resolve disputed promises. For a loss, analyse evaluator feedback and evidence gaps without retaining customer information unnecessarily.

Within ninety days

Review decision quality, incidents, access closure, provider performance, review effectiveness, customer perception and delivery of security promises. Feed systemic findings into risk assessment, audit, corrective action and management review.

The clock test

At any moment the bid manager should answer:

- What is the next irreversible security decision?
- Which information and risk are involved?
- What evidence is missing?
- Who owns the decision?
- When does delay remove safe options?
- Which control must not be traded away?
- What will the customer or delivery team experience if the decision is wrong?

The Minimum Useful Security Scoreboard

TOOLKIT PURPOSE

Measures should help somebody decide. Start small. Define them properly. Add a measure only when the organisation knows what question it answers and what action may follow.

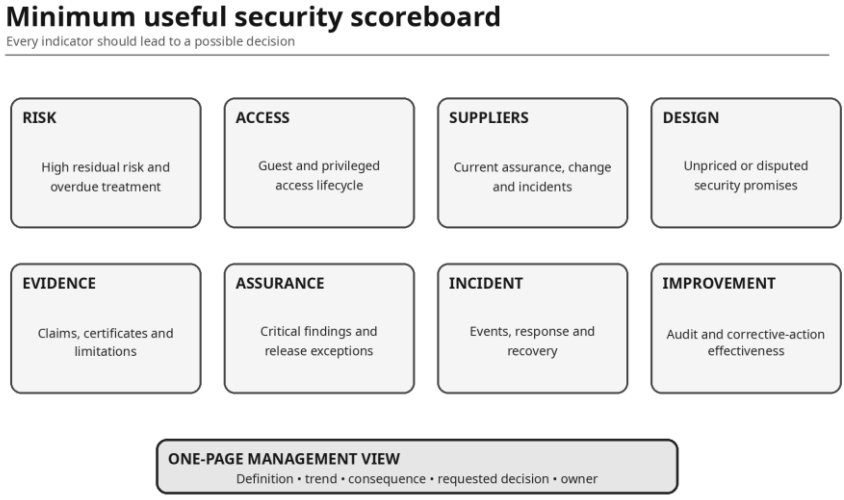

Figure 12 - The minimum useful security scoreboard connects evidence and trend to a management decision.

Risk and treatment position

Track high and above-tolerance risks, overdue treatment, residual-risk approvals, reassessment after change and SoA controls whose implementation status is uncertain.

Decision: fund, redesign, accept, stop or escalate treatment.

> **Do not:** count all risks equally or reward owners for lowering scores without changing exposure.

Customer and pursuit security

Track sensitive pursuits correctly classified, security requirements identified within target time, customer handling exceptions, security clarifications, assurance requests and evaluator feedback.

Decision: change triage, customer communication, requirements analysis, evidence or opportunity class.

Identity and access lifecycle

Track guest and privileged accounts with owner and expiry, overdue access review, time to remove access after role or campaign end, orphaned identities and emergency-access use.

Decision: automate, clarify ownership, change approval or strengthen review.

> **Quality check:** sample whether reviewed access still has genuine business need.

Supplier, cloud and AI assurance

Track critical providers assessed before use, current agreements and evidence, material provider changes, overdue re-evaluation, incidents, unresolved shared responsibilities and unapproved tools or use cases.

Decision: improve selection, terms, monitoring, configuration, exit or permitted-use rules.

> **Do not:** mark provider assurance complete because a questionnaire was returned.

Secure design and commercial coherence

Track material security requirements without design owners, late security design changes, unpriced controls, provider commitments not reflected in agreements, unresolved customer dependencies and security promises disputed by delivery.

Decision: move security and commercial involvement earlier, redesign review entry criteria or requalify pursuits.

Evidence and claim integrity

Track expired or out-of-scope certificates, unsupported security claims, evidence items with unclear owner or limitation, repeated customer requests and factual corrections after review.

Decision: narrow claims, create evidence, improve source control or stop reuse.

Assurance and release

Track critical and major security findings by stage, recurrence, closure time, risk acceptance, reviews held without entry criteria, post-freeze security changes and release exceptions.

Decision: change reviewer competence, timing, independence, design maturity or authority.

> **Do not:** celebrate fewer findings without checking later incidents and evaluator feedback.

Submission and information closure

Track portal and account incidents, file-integrity defects, wrong or missing uploads, use of contingency, receipt verification, access removal, customer-information deletion and archive completeness.

Decision: improve rehearsal, device and identity readiness, manifest, retention or closure ownership.

Incident and continuity readiness

Track events and incidents by type and consequence, reporting time, containment, notification, repeat cause, exercise results, backup restoration, recovery performance and untested critical dependencies.

Decision: change control, resource, exercise, provider or recovery design.

> **Do not:** use zero reported incidents as the only sign of security.

Competence and secure behaviour

Track role competence, practical assessment, missing deputies, event-reporting awareness, repeated bypass, unsafe workload and learning effectiveness.

Decision: train, supervise, redesign tools, change authority, add resource or stop assigning the work.

Audit, corrective action and improvement

Track audit coverage based on risk, nonconformities, repeat findings, aged actions, corrective-action effectiveness, management-review completion and improvements that remove unnecessary work.

Decision: escalate, resource, simplify, verify or close.

The one-page management view

For each selected indicator show:

- definition;
- current position;
- trend;
- target or threshold;
- interpretation;
- risk or customer consequence;
- requested decision;
- owner and due date.

Keep detailed evidence behind the page. Do not fill it with green arrows.

A practical starting set might be:

1. high residual risks and overdue treatment;
2. external access closed within target;
3. critical providers with current assurance;
4. security requirements and design completed before content freeze;
5. unpriced or disputed security promises;
6. critical review findings closed before release;
7. security incidents and serious near misses;
8. backup or continuity tests passed;
9. corrective actions shown effective;
10. customer or delivery security feedback requiring decision.

The scoreboard is useful when leadership can look at it and decide what must change before the next pursuit reaches the same point.

SOURCES AND PROFESSIONAL NOTES

This book is practical implementation commentary. It does not reproduce the text of ISO/IEC 27001 or ISO/IEC 27002 and cannot replace authorised standards, competent professional advice, customer documents, law or organisational judgement.

At the date of publication, the principal certifiable requirements discussed were ISO/IEC 27001:2022 together with ISO/IEC 27001:2022/Amd 1:2024. The amendment introduced climate-change consideration into the organisational-context and interested-party requirements. ISO/IEC 27002:2022 remained the current control-guidance standard supporting implementation of information-security controls. ISO/IEC 27005:2022 provided guidance on information-security risk management.

The Annex A labels and descriptions in this book are paraphrased for implementation learning. The authorised standard remains decisive. The organisation determines necessary controls through risk treatment, compares those controls with Annex A and records the position through the Statement of Applicability. Annex A is not a declaration that every listed control is automatically required.

The APMP alignment is based on the public description of the APMP Winning Business Ecosystem and related professional resources. APMP terminology is used to explain lifecycle alignment. This book is independent and is not approved, issued or endorsed by APMP.

Primary and official standards references

1. International Organization for Standardization and International Electrotechnical Commission, **ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements**. Obtain an authorised copy through ISO, IEC or an authorised national standards body.
2. ISO and IEC, **ISO/IEC 27001:2022/Amd 1:2024 - Climate action changes**.
3. ISO and IEC, **ISO/IEC 27000:2026 - Information security, cybersecurity and privacy protection - Information security management systems - Overview**.
4. ISO and IEC, **ISO/IEC 27002:2022 - Information security controls**.
5. ISO and IEC, **ISO/IEC 27005:2022 - Guidance on managing information security risks**.
6. ISO and IEC, **ISO/IEC 27007:2020 - Guidelines for information security management systems auditing**.
7. ISO and IEC, **ISO/IEC 27006-1:2024 - Requirements for bodies providing audit and certification of information security management systems**.
8. ISO/IEC JTC 1/SC 27 public articles and guidance concerning Annex A, risk treatment and the Statement of Applicability.
9. ISO official information on the ISO/IEC 27000 family of standards and ISO/IEC 27001 certification.

Professional and UK assurance references

10. Association of Proposal Management Professionals, **Winning Business Ecosystem**, public lifecycle description and related professional resources.
11. United Kingdom Accreditation Service, public guidance on accreditation of management-system certification bodies and information-security management-system certification.
12. United Kingdom Accreditation Service, **UKAS CertCheck**, for verification of relevant accredited certificates where applicable.

13. National Cyber Security Centre, public guidance on cyber-security risk management, supply-chain security, incident management, cloud and supplier assurance.
14. Information Commissioner's Office, public guidance on security, data protection by design and default, encryption and personal-data obligations.
15. Applicable laws, regulations, customer security policies, procurement documents, contracts, classification schemes and sector guidance in the jurisdiction and service concerned.

Current related standards

The wider ISO/IEC 27000 family continues to evolve. Depending on scope and customer need, organisations may also need current standards and guidance concerning cloud security, privacy information management, cyber incident management, network security, secure development, business continuity, supplier relationships and sector-specific requirements.

Do not rely on a list printed in 2026 as permanently current. Maintain a controlled standards and obligations register. Record edition, source, owner, relevance, review date and change action.

Intellectual property and independent status

Bid Security by Design is an independent publication. It is not affiliated with, sponsored by or endorsed by ISO, IEC, APMP, UKAS, the NCSC, the ICO, any certification body, the UK Government or any contracting authority.

ISO and IEC standards, APMP materials and third-party marks remain the property of their respective owners. References are provided for professional orientation and further study. Readers should consult current authorised and official material.

CLOSING FIELD ORDER

FINAL DISPATCH

Information security in bidding is not a folder marked Confidential.

It is the decision not to enter work the organisation cannot protect. It is the partner who receives only what they need. It is the risk owner who signs a residual risk after understanding it. It is the writer who stops when evidence ends. It is the architect who knows who creates the first administrator account. It is the pricing lead who gives every control a commercial home. It is the reviewer who checks scope before grammar. It is the uploader using the right identity, device and file. It is delivery receiving the same security promise the evaluator read.

ISO/IEC 27001 provides the management discipline. Annex A provides a reference set for control completeness. ISO/IEC 27002 provides deeper implementation guidance. APMP provides a professional view of the pursuit lifecycle.

None removes judgement.

Build the ISMS around real information. Put a live pursuit through it. Follow one file, one identity, one supplier, one risk and one promise until the route either holds or breaks.

Where it breaks, do not add theatre.

Correct the exposure. Understand the cause. Change the system. Test it again.

Qualify with security visible. Capture lawfully. Classify before sharing. Assess risk before design hardens. Price the control. Write from evidence. Review independently. Release exact files. Respond to incidents. Remove access. Handover every promise. Learn before the next notice arrives.

The customer may never see most of the control environment.

They will see the consequences when it is absent.

ISO/IEC 27001 • SECURE PURSUITS • OPERATING EVIDENCE

Security is not a policy appendix. It is part of the pursuit.

Most bid teams treat security as a questionnaire exercise. This field manual shows how to build ISO/IEC 27001 into the real pursuit: qualification, capture, bid room control, solution design, writing, review, submission, clarification and handover.
It connects clauses 4 to 10, Annex A thinking and APMP-aligned practice to everyday bid work, turning security from theatre into a controlled operating system. With crosswalks, role guides, audit questions, scenario playbooks and a ninety-day implementation route, it helps teams protect information, strengthen trust and produce more disciplined bids.

- Clause-to-bid crosswalks
- Annex A control guidance
- Audit and review toolkits
- Ninety-day implementation plan

Hayden Fay

Published by Bid Champions Ltd