Apptega

GUIDE

ISO/IEC 27001:2022

Enterprise Compliance Guide (ISMS)

For organizations that need a practical, implementable path to establish, certify, and continuously improve an Information Security Management System (ISMS) aligned to ISO/IEC 27001:2022

Current as of October 14, 2025

Purpose

Turn ISO/IEC 27001:2022 into a working ISMS that can be implemented by teams and verified by auditors. The guide explains why each requirement matters, how to design processes that naturally emit evidence, which artifacts to collect, and how to run the ongoing loop (monitor → audit → management review → corrective action) to achieve and sustain certification.

How to use this guide

1. Stand up the foundation with the 90-Day Quick-Start and complete the System Description (2B.2).
2. Implement Clauses 4–10 using the consistent pattern in Section 4 (Intent • Minimums • Implement • Evidence • Acceptance • Common Failures • Internal QA • Docs).
3. Set quantitative thresholds in Organization-Defined Parameters (Section 6), store proof in the Evidence Register (Section 7), and run the Quarterly Operating Calendar (Section 8A).
4. Use Audit Readiness Gates (Section 13) and Evidence Packaging Rules (Section 7A) before Stage 1 and Stage 2.

Who Should Use This Guide

Executive Sponsor, ISMS Manager, CISO/CIO/CTO, Risk Lead, SecOps/Detection/IR, IAM, Platform/Cloud/IT, Network, AppSec/SDLC, Data Governance/Privacy, Legal & Compliance, TPRM/Procurement, Internal Audit, Business/System Owners, Facilities, PMO.

What “Good” Looks Like

- Scope, boundaries, dependencies, and exclusions are explicit, version-controlled, and match deployed reality; exclusions have rationale, compensating controls, and expiry.
- Risk drives control selection; exceptions are rare, time-boxed, and reviewed in Management Review.
- Evidence comes from normal operations (tickets, pipelines, logs, reviews) and is traceable requirement → process → record; sampling is documented and reproducible.
- The operating loop is visible: KRIs trend, internal audits re-perform real work, Management Reviews make decisions and fund actions, and CAPAs prove effectiveness.
- Supplier/shared responsibility is explicit; contracts include notice and telemetry/export rights; notices trigger actions with proof.
- Change management is complete for 100% of production changes (approvals, tests/scans, rollback); emergency changes have PIR ≤72h.
- Backup/DR targets (RPO/RTO) are defined; restore tests run; failed restores trigger CAPA and successful re-test.
- •dentity & Access shows SSO/MFA coverage, quarterly access recerts, leaver deprovision ≤24h (target), and tested break-glass.
- Logging & Detection ingests ≥95% required sources, runs benign detection drills, and monitors ingestion health.
- ODPs/metrics have owners, thresholds, cadence, and breach handling.

1. Introduction

ISO/IEC 27001:2022 certification requires an operating system of security, not a static document set. Auditors confirm that your ISMS understands business context and obligations, selects and operates risk-based controls, monitors performance, escalates to leadership, and improves with verified corrective actions. This guide structures each process so it creates auditable proof by default and organizes evidence the way auditors consume it during Stage 1 and Stage 2.

1A. 90-Day Quick-Start (ISMS stand-up → certification readiness)

Days 1—15: Foundation

- Approve ISMS Policy and risk appetite; appoint Executive Sponsor and ISMS Manager.
- Draft scope/boundary and diagrams; create Interested Parties & Obligations Register.
- Start Risk Register and Evidence Register; publish Incident and Change processes.
- Enforce MFA for admin/remote; centralize identity, control-plane, workload, and app logs.

Days 16—45: Core Loop

- Finalize risk criteria and taxonomy; complete initial risk assessment.
- Set ISMS objectives/KRIs with targets; baseline asset/config inventory.
- Implement JML access lifecycle and quarterly recerts; define vulnerability SLAs + re-scan policy.
- Establish backup/restore cadence with integrity checks; inventory suppliers and responsibility matrices.

Days 46—90: Prove Operation

- Limited-scope internal audit with re-performance (one restore, one detection drill, one access recert).
- Management Review with decisions and funded actions.
- Record nonconformities and CAPAs with effectiveness windows.
- Publish ISMS Manual v1; lock Stage 1/Stage 2 timing and scope.

2. ISMS Scope & Boundary

- **Intent:** Define what the ISMS governs and why, so controls are applied consistently and auditable.
- **Minimums:** Approved scope statement; interfaces/dependencies; exclusions (with rationale & expiry); version-controlled diagrams.
- **Implement (how).** Write a plain-language scope naming services, locations, systems, data flows, and interfaces (enterprise IT, cloud providers, processors). Maintain boundary & data-flow diagrams matched to deployments; add review triggers (region/architecture change; new customer SOW). Record exclusions with risk acceptance, compensating controls, and a review date.
- **Evidence:** Approved scope; diagrams with last review date; dependency register; change logs.
- **Acceptance:** Scope and diagrams current; exclusions justified and time-boxed; dependencies explicit and monitored.
- **Common Failures:** Stale diagrams; hidden shared services; exclusions without treatment.
- **Internal QA:** Annual refresh and on material change.
- **Docs:** ISMS Scope Statement; Architecture & Data Flow Diagrams.

2A. Interested Parties & Obligations Register — Purpose & Use

- **Purpose.** Translate external promises (contracts, SLAs, laws, policies) into concrete control work.
- **How to use.** Record each obligation, mapped control(s) or gap, owner, cadence, and evidence path. Review on schedule and whenever a new SOW/regulation lands. Gaps become dated actions or exceptions.
- **What auditors expect.** Each obligation points to a control or a time-boxed action with an evidence path.

2B. System Description Kit (Scaffold & Template)

- **Purpose:** Establish a single, authoritative description of the services/systems in scope so scope, risks, controls, and evidence stay anchored to reality.
- **How to use:** Complete the Scaffold (2B.1) to agree on structure and depth; then fill the Template (2B.2) with concrete facts (names, regions, owners, data classes, SLAs). Keep 2B under change control; when architecture, regions, data handling, or suppliers change, update 2B and link the change tickets. Use the worked example in Section 16 to calibrate tone and detail.
- **Evidence & Acceptance:** The System Description must match deployed reality and identity/network boundaries; name owners for components and data stores; trace key dependencies (IdP, cloud services, processors); link to diagrams/evidence paths; and show a visible “last reviewed” date.

2B.1 Scaffold (Authoritative Outline)

1. Services in scope (names, versions, deployment model, customers, critical transactions)
2. System components (infrastructure/regions, platforms/services, applications/microservices)
3. People and roles (internal; external/managed; subservice/processor organizations)
4. Processes (JML, change, operations, IR, DR/BCP, vulnerability/config, SDLC, privacy)
5. Data flows and stores (inbound, processing, outbound; classification; retention/deletion)
6. Boundaries and dependencies (tenants/accounts/segments; DR posture; key third parties)
7. Commitments and system requirements (objectives, SLOs, legal/contractual)
8. Clause/Annex coverage map (pointers into this Guide)
9. Complementary user/entity responsibilities (if applicable)
10. Changes during the period (date, impact, mitigation)
11. Subservice/processor organizations (treatment; evidence held; monitoring)
12. Limitations and exclusions (rationale; compensating controls)

2B.2 System Description — Fill-in Template (Ready to copy)

1. System Name & Scope

System name

Services included (names, versions)

Customer segments / primary use cases

In scope summary (services, components, locations):

Out of scope (and why):

2. Architecture & Components

Hosting model (cloud/on-prem/hybrid) and regions/tenancy

Core infrastructure (VPCs/VNETs, networks, load balancers)

Applications / microservices (name → purpose → owner)

Data stores (type/classification → region → owner):

3. People & Roles

Internal roles (SecOps, IAM, Platform/Cloud, AppSec, IT Ops, IR)

External parties / managed services (name → services → contract/SLA)

Subservice/processor orgs (name → service relied on → treatment)

4. Processes & Procedures

Access lifecycle (JML) summary

Change management approach (tickets, approvals, CI/CD, rollback)

System operations (monitoring, detection/response, vulnerability mgmt)

Backup/restore & DR approach (RTO/RPO, test cadence)

Privacy operations (if in scope)

5. Data Flows & Stores

Inbound data sources (from whom/what)

Processing steps (high level)

Outbound/data sharing (to whom/what)

Retention & deletion rules (by data class)

6. Boundaries & Dependencies

Physical/logical boundaries (tenants, accounts, network segments)

Multi-region / DR posture

Key dependencies (identity provider, cloud services, third-party APIs)

7. Commitments & System Requirements

ISMS objectives & KPIs/KRIs

Principal service commitments (security, uptime/SLOs, data handling)

Applicable laws/regs/contractual requirements

8. Coverage Map (Clauses/Annex)

Clauses 4—10 overview → see Section

Annex A Organizational/People/Physical/Technological summaries → see Section

9. Complementary User/Entity Responsibilities

Customer or internal unit responsibilities required for commitments

10. Changes During the Period

Change description

Effective date

Risk/control impact

Mitigation

11. Subservice/Processor Organizations (Detail)

Name

Service relied on

Treatment

Evidence held (certifications/assurance/bridge letter/controls tested)

Monitoring approach (reviews, KPIs, notices)

12. Limitations & Exclusions

Explicit limitations and rationale

Compensating controls

13. Evidence Cross-References (paths)

Link each section to artifacts in the Evidence Register.

14. Approval & Versioning

Owner

Reviewers

Approved date	Next review

3. Roles & Responsibilities (RACI)

Program Area	Accountable	Responsible	Consulted	Informed
ISMS scope & boundary	Executive Sponsor	ISMS Manager	Legal, Product	Control Owners
Risk assessment & treatment	CISO	Risk Lead	Control Owners	Executives
Access & identity	CISO	IAM Lead	HR, Audit	All users
Logging & operations	CISO	SecOps Lead	Platform/Cloud	Product
Change management	CTO	Platform Eng Lead	AppSec, QA	Product
Business continuity/DR	CIO	IT Ops Lead	SecOps, Product	Executives
Data protection & privacy	CISO/CPO	Data Owner/Privacy Eng	AppSec, Legal	Product
Supplier & processors	CFO	TPRM Lead	Security, Legal	Business Units
Internal audit & reviews	CEO	IA Lead	ISMS Manager	Executives

3A. Program Operating Model (Decision Rights & Escalations)

- **Scope/system changes:** Executive Sponsor (A); ISMS Manager (R).
- **Risk exceptions & expiry:** CISO/CTO (A); Control Owner (R).
- **Supplier treatment & clauses:** Executive Sponsor (A); TPRM/Security (R).
- **Escalations:** Red KRIs twice consecutively → Management Review; expired exceptions → alternate control in 48h and report at next review.

4. Standards & Practices (ISO Clauses 4—10)

This section turns Clauses 4–10 into an operating model. For each clause you'll find why it exists (Intent), what must exist (Minimums), how to run it (Implement), what proof to keep (Evidence), the acceptance criteria auditors apply (Acceptance), where programs fail (Common Failures), how to self-check (Internal QA), and which documents bind it (Docs). Operate to cadence, and update artifacts when context changes.

4.1 Context of the Organization (Clause 4)

Intent: Align the ISMS with business, technology, and regulatory context.

Minimums: Context analysis; interested parties; obligations; scope and diagrams under change control.

Implement: Publish a Context Report (mission, threat drivers, tech stack, regulatory footprint). Maintain Interested Parties & Obligations and show linkages to controls or dated actions. Keep boundary/data-flow diagrams with "last reviewed" and change links.

- **Evidence:** Context report; obligations register; approved scope; diagrams; change logs.
- **Acceptance:** Registers current; scope/exclusions reviewed annually and on change; diagrams match deployed systems.
- **Common Failures:** Outdated diagrams; obligations not mapped.
- **Internal QA:** Annual refresh + trigger-based updates.
- **Docs:** ISMS Scope Statement; Interested Parties Register.

4.2 Leadership (Clause 5)

Intent: Leadership sets direction, resourcing, and decision rights.

Minimums: Policy and objectives; roles/authorities; resources; communications.

Implement: Approve policy/risk appetite; set objectives; publish governance calendar; define exception rules; review KRI pack and decide (approve/deny/accept risk/fund).

- **Evidence:** Signed policy; RACI; governance minutes with decisions/owners; budget/resource tickets; policy communications.
- **Acceptance:** Reviews executed; actions closed; exceptions time-boxed with compensating controls.
- **Common Failures:** Objectives unfunded; exceptions without expiry.
- **Internal QA:** Quarterly sample of decisions → action proof.
- **Docs:** ISMS Policy; Governance Charter.

4.3 Planning — Risks, Opportunities, Objectives (Clause 6)

Intent: Risk-based control selection and measurable objectives.

Minimums: Risk method; register with owners; treatment or exception; objectives with targets.

Implement: Use a taxonomy (identity, logging, vulnerability/config, DR, supplier, privacy, change). Rank and treat; time-box exceptions; set objectives/KRIs with baselines and trends; require change-impact analysis for material moves.

- **Evidence:** Risk register; treatment plan; exception ledger; objective dashboards with actions.
- **Acceptance:** High risks have dated treatments; residual risk within appetite; objectives drive decisions.
- **Common Failures:** Static register; vanity metrics.
- **Internal QA:** Monthly risk review; quarterly objective review.
- **Docs:** Risk Management Procedure; Objectives & Key Results.

4.4 Support — Resources, Competence, Communication, Documented Information (Clause 7)

Intent: Ensure people, skills, and documents support the ISMS.

Minimums: Role competence; training and verification; controlled documents; communications.

Implement: Define role rubrics; run onboarding + annual refresh with assessments/ demos; implement document lifecycle with approvals/versioning; execute communications plan for policy and incidents.

- **Evidence:** Training rosters + assessments; competence verifications; approved docs with version history; comms logs.
- **Acceptance:** ≥98% training completion; critical roles verified; documents current and access-controlled.
- **Common Failures:** Shadow SOPs; expired **Docs:**
- **Internal QA:** Quarterly doc-control audit; semiannual competence sampling.
- **Docs:** Competence & Training Plan; Document Control SOP.

4.5 Operation — Risk Treatment, Outsourcing, Change (Clause 8)

Intent: Operate selected controls; manage suppliers; control change; respond to incidents.

Minimums: Implement control themes; manage supplier responsibility; r un change process; handle incidents with AARs.

Implement: Execute Annex A themes (Section 5). Maintain supplier matrices and contract clauses (notice SLAs, telemetry/export rights, audit/assurance, sub-processor flow-down). Run change process linking tickets → approvals → tests/ scans → rollback. Operate IR timelines and AARs.

- **Evidence:** Control configs; supplier matrices/due diligence; change records with approvals/tests/rollback; incident tickets/AARs.
- **Acceptance:** Treatments delivered; 100% production changes show approvals/ tests/rollback (emergency PIR ≤72h); supplier duties evidenced; incidents show containment, RCA, actions.
- **Common Failures:** Console changes; vendor gaps; controls with no telemetry.
- **Internal QA:** Quarterly attack or restore drill; supplier review with actions.
- **Docs:** Operational Procedures; Supplier Responsibility Matrix; Change Policy; Incident Response.

4.6 Performance Evaluation — Monitoring, Internal Audit, Management Review (Clause 9)

Intent: Prove performance, independently verify, and make decisions.

Minimums: KRI set; internal audit program; management review cadence and inputs/outputs.

Implement: Track KRIs that move risk (MFA, log coverage, patch SLAs, EDR health, restore success, change completeness, supplier review currency). Internal audit re-performs real work. Management Review decides and funds actions.

- **Evidence:** KRI dashboards; audit plans/reports/workpapers; review minutes with actions.
- **Acceptance:** Reviews on schedule; audits cover full scope annually; actions close with proof; trend-driven changes.
- **Common Failures:** Metrics without thresholds; “note-taking” reviews.
- **Internal QA:** Second-eye on workpapers; KRI trend analysis.
- **Docs:** Monitoring & Measurement Procedure; Internal Audit Procedure; Management Review SOP.

4.7 Improvement — Nonconformity & Corrective Action (Clause 10)

Intent: Fix causes and prevent recurrence.

Minimums: Nonconformity handling; corrective action; effectiveness verification.

Implement: Each CAPA links root cause → actions → dated evidence → effectiveness proof (metric moved or re-test passed for a verification window) → docs/training updated. Severity drives timeline (Major ≤30d, Medium ≤45d, Low ≤60d).

- **Evidence:** CAPA register; verification proof; updated documents/training.
- **Acceptance:** Actions meet timelines; verification shows improvement; recurrence declines.
- **Common Failures:** Closing without verification; permanent “temporary” exceptions.
- **Internal QA:** Quarterly review of repeats/overdues.
- **Docs:** Nonconformity & Corrective Action Procedure.

5. Annex A Control Themes — Narrative Implementations

These narratives operationalize the highest-leverage security domains so control operation naturally emits auditable proof. They are tool-agnostic but evidence-specific. Update narratives when platforms change; reset targets in ODPs (Section 6); run targeted re-tests to prove effectiveness.

5A. Identity & Access

Implement: IdP-backed SSO; MFA for admin/remote; RBAC aligned to job functions; JIT elevation; quarterly access recerts; automated leaver deprovision; tested break-glass with logging.

- **Evidence:** IdP MFA export; IGA recert attestations & revocations; deprovision logs; break-glass test runs.
- **Acceptance:** MFA 100% admin/remote; recerts 100% quarterly; leaver ≤24h; break-glass success with audit trail.
- **Common Failures:** Local accounts; stale privileged access; recerts rubber-stamped.
- **Internal QA:** Monthly MFA coverage review; quarterly recert sample deep-dive.

5B. Logging & Detection

Implement: Required sources—IdP, cloud control plane, workloads, apps, EDR, network egress. Maintain a SIEM onboarding matrix; alerts for auth anomalies, control-plane changes, malware/EDR events, exfil indicators; monthly ingestion health checks; quarterly benign detection drill.

- **Evidence:** Onboarding matrix; ingestion coverage %; drill transcript (generated event → alert timestamp); on-call tickets.
- **Acceptance:** ≥95% required sources ingested; benign drill alerts within MTTA targets; documented routing/escalation.
- **Common Failures:** Unmonitored sources; disabled detections; missing ingestion health.
- **Internal QA:** Monthly ingestion audit; quarterly drill.

5C. Vulnerability & Configuration Management

Implement: Scan cadence (cloud/hosts/containers/apps); SLAs (Critical ≤7d; High ≤15d); verification re-scans; baseline configurations and drift monitoring; SBOM intake to backlog.

- **Evidence:** Scan reports; SLA dashboards; re-scan proof; baseline/diff reports; backlog links.
- **Acceptance:** ≥95% SLA adherence; baseline drift remediated within windows.
- **Common Failures:** Exceptions without expiry; re-scan not proving fix.
- **Internal QA:** Weekly SLA review; monthly spot re-scan.

5D. Backup/Recovery & DR

Implement: Classify systems; set RPO/RTO; encrypted/immutable backups; quarterly restore tests with integrity checks; annual DR exercise with measured outcomes and AAR.

- **Evidence:** Backup configs; restore logs; DR AAR with timings; remediation tickets.
- **Acceptance:** Restores complete within RTO/RPO; failed restores drive CAPA and successful re-test.
- **Common Failures:** Untested restores; scope mismatch.
- **Internal QA:** Quarterly critical restore test; annual DR.

5E. Change Management

Implement: ITSM change tickets linked to commits/PRs; CI/CD gates for tests/scans; approvals by risk; rollback plans; emergency PIR ≤72h; post-deploy monitoring checks.

- **Evidence:** Ticket → commit → approval → gate results → deploy record → rollback artifacts; PIRs.
- **Acceptance:** 100% production changes show approvals/tests/rollback; emergency PIRs timely.
- **Common Failures:** Console/“hotfix” changes; missing rollback.
- **Internal QA:** Monthly random sample (≥10 changes).

5F. Supplier/Processor Governance

Implement: Tiering; responsibility matrices (You/Provider/Shared); contract clauses (notice SLAs, telemetry/export rights, audit/assurance, sub-processor flow-down, off-boarding). Onboarding due diligence; periodic reviews; action tracking; incident/change notices processed.

- **Evidence:** Matrices; due diligence files; notices and actions; assurance artifacts (certs/reports).
- **Acceptance:** Tier-1 reviews current; notices acted within SLA; matrices current and consistent with operations.
- **Common Failures:** Blind trust in provider; missing telemetry rights.
- **Internal QA:** Quarterly Tier-1 review; annual clause audit.

5G. Control Test Procedures (CTPs) Starter Pack — Purpose & Use

- **Purpose:** Lightweight, consistent spot-checks for high-risk controls.
- **How to use:** Run quarterly: MFA coverage; access recerts; patch SLAs + re-scans; log coverage + benign alert drill; restore proof; change completeness; supplier oversight. Save inputs/outputs to Evidence paths.
- **What auditors expect:** Completed runs with outcomes and tickets for failures.

6. Organization-Defined Parameters (ODPs) & Metric Definitions

Parameter	Target	Owner	Review
MFA coverage (admin/remote)	100%	IAM Lead	Monthly
Access review completion	100% quarterly	IAM Lead	Quarterly
Log coverage (required sources)	≥95%	SecOps Lead	Monthly
Critical/High vuln SLAs	7/15 days met ≥95%	SecOps Lead	Weekly
EDR healthy coverage	≥98%	SecOps Lead	Weekly
Backup/restore tests (critical)	≥1 per quarter	IT Ops Lead	Quarterly
Change completeness (approvals+tests+rollback)	100% of prod changes	Platform Eng Lead	Monthly
Incident MTTA/MTTR	≤15 min / improving	SecOps/IR Lead	Monthly
Supplier review currency	100% Tier-1 ≤12 months	TPRM Lead	Quarterly
Privacy request timeliness (if applicable)	100% within legal timeline	Privacy Eng	Monthly

6A. Metrics & Evidence Map

Metric	Clause/Theme	Source	Owner	Evidence Path	Review
MFA Coverage %	Annex A (Access)	IdP	IAM Lead	ISMS/MFA/	Monthly
Access Recert %	7, Annex A	IGA	IAM Lead	ISMS/Access/	Quarterly
Log Coverage %	9, Annex A	SIEM	SecOps	ISMS/Logging/	Monthly
Patch SLA %	8–9, Annex A	Vuln Mgmt	SecOps	ISMS/Vuln/	Weekly
EDR Healthy %	Annex A	EDR console	SecOps	ISMS/EDR/	Weekly
Restore Success %	8–9, Annex A	Backup	IT Ops	ISMS/Recovery/	Quarterly
Change Completeness %	8, Annex A	ITSM/CI/CD	Platform Eng	ISMS/Change/	Monthly
Supplier Review Currency %	8, Annex A	TPRM	TPRM	ISMS/TPRM/	Quarterly

6B. Exception Governance Policy — Purpose & Use

- **Purpose:** Keep risk deviations visible, temporary, and controlled.
- **How to use:** When a control misses its target, open an exception with risk statement, scope, compensating controls, owner, approver, and expiry. Track on the ledger and review at each Management Review until closed or renewed with new justification. Expired items auto-escalate.
- **What auditors expect:** A current ledger with approvals, expiries, evidence of closure or renewal, and references in Management Review minutes.

7. Evidence Register (Authoritative Artifacts)

Artifact	Clauses/ Annex	Path	Owner	Format	Last Updated	Verifier	Next Review
ISMS Policy & Scope	4–5	ISMS/Policy/	ISMS Mgr	PDF			
Context & Interested Parties	4	ISMS/Context/	ISMS Mgr	PDF			
Obligations Register	4	ISMS/ Obligations/	Legal/ Compliance	CSV/PDF			
Architecture & Data Flows	4, 8	ISMS/Arch/	Eng Lead	PDF			
Risk Method & Register	6	ISMS/Risk/	Risk Lead	CSV/PDF			
ISMS Objectives & KRIs	6, 9	ISMS/Metrics/	ISMS Mgr	CSV/PDF			
Document Control Records	7	ISMS/Docs/	Quality	CSV/PDF			
Training & Competence	7	ISMS/Training/	L&D	CSV/PDF			
Control Implementations	Annex A	ISMS/ Controls/	Control Owners	PDF/ JSON			
Logging & Monitoring	9, Annex A	ISMS/ Monitoring/	SecOps	PDF/CSV			
Incidents & AARs	8, 10	ISMS/IR/	IR Lead	PDF/CSV			
Supplier Matrices & Reviews	8, Annex A	ISMS/TPRM/	Procurement	PDF/ XLSX			
Internal Audit Program & Reports	9, 10	ISMS/Audit/	IA Lead	PDF			
Management Review Minutes	9	ISMS/MR/	Exec Sponsor	PDF			
Corrective Action Records	10	ISMS/CAPA/	ISMS Mgr	CSV/PDF			

7A. Evidence Packaging Rules — Purpose & Use

- **Purpose:** Make evidence easy to trace from requirement to record.
- **How to use:** Store artifacts under the Evidence Register path using the naming scheme. For sampled areas (e.g., access recerts), package the population export, sampling method, and sampled items. Screenshots show date/time and source path; exports contain filters and time ranges.
- **What auditors expect:** Consistent filenames, a single place to find proof, and sampling packs that reproduce the selection.

7B. Evidence Retention Matrix

Category	Examples	Minimum Retention	System of Record / Path	Owner
Policies & Governance	Policy library, governance charter, RACI	3 years	ISMS/Policy/	ISMS Mgr
Context & Scope	Scope, diagrams, change log	3 years	ISMS/Context/, ISMS/Arch/	ISMS Mgr
Risk Management	Risk register, treatments	3 years	ISMS/Risk/	Risk Lead
Document Control	Approvals, versions	3 years	ISMS/Docs/	Quality
Training & Awareness	Completion, assessments	2 years	ISMS/Training/	L&D
Access & Identity	JML, recerts, MFA exports, break-glass logs	2 years	ISMS/Access/, ISMS/MFA/	IAM
Logging & Detection	Onboarding matrix, alert samples, SIEM exports, drills	18–36 months	ISMS/Monitoring/	SecOps
Vulnerability Mgmt	Scans, SLAs, re-scans	2 years	ISMS/Vuln/	SecOps
Change Management	Tickets, PRs, pipelines, PIRs	2 years	ISMS/Change/	Platform Eng
Availability/DR	Backups, restore proofs, DR plans/AARs	3 years	ISMS/Recovery/, ISMS/DR/	IT Ops
Supplier & Processors	Due diligence, notices, bridge letters	3 years	ISMS/TPRM/	Procurement
Incidents & CAPA	Timelines, AARs, verification	3 years	ISMS/IR/, ISMS/CAPA/	IR/ISMS
Internal Audit & MR	Workpapers, minutes, trackers	3 years	ISMS/Audit/, ISMS/MR/	IA/Exec Sponsor

8. Continuous Monitoring (KRIs, Alerts, Automation) — Purpose & Use

- **Purpose:** Keep a short list of risk indicators that trigger action before issues become findings.
- **How to use:** Assign each KRI an owner, threshold, alert path, and auto-action. Review per the Operating Calendar. Any breach opens a ticket with a due date and appears in Management Review. Automate enforcement for recurring tasks (exception-expiry reminders, CI/CD gates).
- **What auditors expect:** KRI trends, breach tickets with outcomes, and proof that repeated breaches lead to CAPA or design change.

KRI	Threshold	Owner	Alert	Auto-Action
MFA gaps (admin/remote)	Any	IAM	Pager	Block or time-boxed exception
Unmanaged accounts	>0	IAM	Ticket	Disable pending review
Critical log source failure	Any	SecOps	Pager	Fix ≤24h; track ticket
Critical/High patch SLA late	>5%	SecOps	Weekly	Exec review + plan
Backup restore failure	Any	IT Ops	Pager	RCA + retest
Change without approval	Any	Platform Eng	Ticket	PIR + CAPA
Supplier notice overdue	Any beyond SLA	TPRM	Email	Vendor escalation + CISO notify

8A. Quarterly Operating Calendar — Purpose & Use

- **Purpose:** Create a predictable rhythm so the ISMS doesn’t drift between audits.
- **Cadence:**
  - Week 1 — Access reviews; EDR coverage; log source health
  - Week 2 — Patch SLA review; exception ledger; Tier-1 supplier review
  - Week 3 — Detection drill (generate→collect→alert); one critical restore test
  - Week 4 — Internal audit slice; prepare Management Review
  - Annual — DR exercise; pen-test cycle; policy refresh; privacy/DPIA refresh (if applicable)

9. Internal Audit Program — Purpose & Use

- **Purpose:** Independently verify that the ISMS operates as described and controls work.
- **How to use:** Annual plan covering Clauses 4–10 and major Annex A themes. Methods: interviews, document review, re-performance (restore, benign detection trigger, access recert run-through), and sampling (≥10 items or ≥10%). Classify findings (major/minor); require RCA/CAPA; close only after effectiveness verification.
- **What auditors expect:** Plan, scope, workpapers, findings, and proof that prior findings were verified as effective.

10. Management Review — Purpose & Use

- **Purpose:** Give leadership a recurring forum to decide, accept, and fund based on ISMS performance.
- **How to use:** Present KRI dashboard, exception ledger, audit results, incidents/AARs, supplier notices, and context changes. Record decisions with owners/dates (accept risk with expiry; fund logging; revise patch target). Track follow-through to closure.
- **What auditors expect:** Minutes that clearly show decisions and actions, with links to tickets or artifacts.

11. Corrective Action (RCA/CAPA) — Purpose & Use

- **Purpose:** Stop recurrence by fixing causes, not just symptoms.
- **How to use:** Open a CAPA when a control fails, a KRI repeatedly breaches, or an audit/incident finds a gap. Record root cause, corrective/preventive actions, and the effectiveness test (metric or re-test and verification window). Close only when the agreed test passes; otherwise revise and continue. Severity sets the deadline (Major ≤30d; Medium ≤45d; Low ≤60d).
- **What auditors expect:** A CAPA register with evidence, results of effectiveness checks, and fewer repeats over tim

12. Change Management for Security-Impacting Changes — Purpose & Use

Purpose

Prevent security regressions by ensuring every production change that can affect confidentiality, integrity, or availability is risk-assessed, approved, validated, reversible, monitored, and evidenced.

Scope

All production changes to infrastructure, platforms, applications, data processing logic, identities/permissions, security tooling, logging/telemetry, backup/DR, network exposure, cryptographic material, data lifecycle rules, and third-party/service configurations that alter the effective security posture. Includes emergency changes and supplier-initiated changes that impact your controls.

Definitions

- Security-impacting change — change that alters risk profile or controls.
- Emergency change — required to restore service or mitigate an active threat; abbreviated approvals with mandatory PIR ≤72h.
- Rollback plan — tested path to restore the prior known-good state.

Principles

No unapproved production change. Risk drives approvals and gates; higher impact → stronger evidence. Author ≠ approver. Tested, reversible, observable before live. Emergencies permitted but must pass PIR and effectiveness check. Treat supplier changes as your own when they affect your risk.

Roles & Decision Rights

- Accountable: CTO (product/app), CIO (IT), CISO (security controls).
- Responsible: Platform/Cloud Lead, App/Service Owner, Security Eng (for control changes), Data Owner (for data rules).
- Approvers: Risk-tiered per 12A.
- Consulted: SecOps/IR, IAM, Privacy, QA, TPRM.
- Informed: Business/System Owners, Support, PMO.

Triggers (examples)

Identity/MFA/RBAC; network ingress/egress/exposure; encryption/KMS/keys/certs; logging scope/pipelines/retention; EDR/monitoring policies; vulnerability/config baselines; CI/CD or runtime guards; backup/restore/DR design; data retention/deletion; supplier or hosting moves; customer-visible security features.

Mandatory Artifacts (attach to the change record)

Impact analysis; risk score and tier; approvals (who/when); tests/scans/gate results; rollback plan; deployment record (time, scope, owner); monitoring checks/alerts; PIR for emergencies; links to updated diagrams/docs where applicable.

Process Outcomes (acceptance criteria)

- 100% of production changes show approvals, tests/scans, and rollback artifacts.
- Emergency changes have PIR ≤72h with actions tracked to closure.
- Material control or boundary changes update diagrams and the System Description (2B) within 14 days.
- Random samples reconstruct traceability: ticket → commit/PR → approvals → gates → deploy → monitor → rollback (if invoked).
- Deviations create exceptions with expiry and compensating controls.

12A. Change-Impact Matrix

- Internet exposure ↑ → update detections; review log scope; focused test.
- Baseline configuration change → staged rollout; drift monitoring; rollback verified.
- Identity/MFA change → break-glass test; access review ≤14 days.
- Backup architecture change → restore test ≤7 days.
- Data processing rule change → reconciliation/approval checks.

13. Audit Readiness Gates (Stage 1 / Stage 2) — Purpose & Use

- **Stage 1 — Design Gate:** Policies, scope, risk method, objectives, procedures, Annex A rationale complete; Evidence Register navigable.
- **Stage 2 — Operation Gate:** Two periods of KRI trends; internal audit with re-performance; one full Management Review with decisions; sampling packs for high-risk areas; exceptions ledger current.

14. Evidence Sampling Plans (Internal QA) — Purpose & Use

- **Purpose:** Demonstrate effectiveness across typical cases without reviewing everything.
- **How to use:** Define populations, sample sizes, and acceptance criteria for access, logging/detection, vulnerability SLAs, change completeness, restores, supplier reviews. Package the population export and sampled records together with results and follow-ups.

15. Common Pitfalls & Anti-Patterns

- Scope and diagrams lag actual environment changes.
- Regulatory/contractual obligations not mapped to controls or evidence.
- Access recertifications incomplete or overdue.
- MFA carve-outs exist but aren’t justified, tracked, or time-boxed.
- Logs are generated but not centralized, alerting, or monitored for health.
- Console/direct changes bypass change management and CI/CD gates.
- Backup/restore tests skipped or lack proof of successful recovery.
- CAPAs closed without verified effectiveness (metric improvement or re-test).
- “Temporary” exceptions become permanent due to missing expiries and reviews.

16. Completed Example System Description (Worked Example)

1. System Name & Scope

- **System name:** Atlas Analytics Platform (AAP)
- **Services included (names, versions):** Atlas API v3, Atlas Web v2, Atlas Jobs v1 (ETL), Atlas Admin v1
- **Customer segments / primary use cases:** Mid-market SaaS/e-commerce; ingest events, build dashboards, export insights
- **In scope summary (services, components, locations):** Production and staging in AWS (us-east-1, eu-west-1); EKS; S3; Aurora-Postgres; MSK; Redis; Okta; CloudWatch; Datadog; GitHub Actions
- **Out of scope (and why):** Corporate IT endpoints and productivity suites (separate Corporate ISMS); legacy Atlas v1 export tool (read-only, decommissioning in progress—no customer data changes)

2. Architecture & Components

- **Hosting model and regions/tenancy:** Multi-tenant SaaS; dedicated VPC per region; customer data segregated by tenant IDs and KMS keys; optional single-tenant VPC-link
- **Core infrastructure:** VPCs, ALB (web/API), private NLB (internal), NAT, Transit Gateway
- **Applications/microservices:** atlas-web (UI), atlas-api (ingestion/query), atlas-jobs (Spark ETL), atlas-admin (admin UI)
- **Data stores:** S3 (raw, parquet), Aurora-Postgres (metadata), Redis (cache), MSK (streams)

3. People & Roles

- **Internal:** SecOps, IAM, Platform/Cloud, App Eng, IT Ops, IR
- **External:** MSP-SOC (24×7 monitoring), Cloud provider (AWS), IdP (Okta)
- **Subservice/processor orgs:** Payment provider (customer billing), Email provider (system notices)

4. Processes & Procedures

- **JML:** HRIS → IdP → IGA → leaver deprovision ≤24h target
- **Change:** ITSM + PR links; CI/CD gates; approvals by risk; rollback plans; emergency PIR ≤72h
- **Operations:** SIEM with required sources; weekly patch SLAs; EDR health; benign detection drill
- **Backup/DR:** Daily encrypted S3 backups; quarterly restore tests; annual DR exercise
- **Privacy:** DSR workflow via ticket; data retention rules by classification

5. Data Flows & Stores

- **Inbound:** Customer event SDKs; admin console inputs
- **Processing:** Ingest → queue → ETL → store → query
- **Outbound:** Dashboards; CSV/warehouse exports; webhooks
- **Retention/deletion:** Raw events 90 days; aggregated 24 months; tenant wipe ≤30 days after termination

6. Boundaries & Dependencies

- **Tenants/accounts/segments:** Prod/stage VPCs; separate AWS accounts; per-region KMS
- **DR posture:** Cross-region snapshots; RPO 1h; RTO 8h
- **Dependencies:** IdP Okta; AWS; MSP-SOC; Email provider; Payment provider

7. Commitments & System Requirements

- **ISMS objectives & KRIs:** MFA 100% admin/remote; log coverage ≥95%; patch SLAs ≥95%; quarterly restores
- **Service commitments:** 99.9% monthly uptime; data encrypted in transit/at rest; DSRs within legal timelines
- **Laws/regs/contracts:** Customer MSAs; applicable privacy laws based on customer location

8. Coverage Map (Clauses/Annex)

Clauses 4–10 → Sections 2, 3, 4, 8–11; Annex A themes → Section 5

9. Complementary User/Entity Responsibilities

Customers manage endpoint security, user hygiene, and API keys in their environment.

10. Changes During the Period

Migrated audit logs to new SIEM pipeline (2025-07-10) — improved coverage; updated detections

11. Subservice/Processor Organizations (Detail)

- **MSP-SOC** — monitoring (carve-out); evidence: contract, runbooks, monthly reports
- **Email provider —** transactional emails (inclusive); evidence: security whitepaper, SOC report

12. Limitations & Exclusions

No on-prem deployments supported; compensating controls not applicable

13. Evidence Cross-References (paths)

- SIEM onboarding matrix → ISMS/Monitoring/Onboarding_Matrix.csv
- Change sample pack → ISMS/Change/Q3_Sample.zip

14. Approval & Versioning

Owner: ISMS Manager • Reviewers: CISO, CTO • Approved: 2025-09-30 • Next review: 2026-01-15

17. Self-Assessment & Leadership Attestation

Record Status (C/PC/NC) per clause/theme with owner, evidence link, action ID, due date. Leadership attests that scope is complete; “C” entries have current evidence; PC/NC items have owners/dates; exceptions have compensating controls and expiry.

Signature

Name/title

Date

18. References

ISO/IEC 27001:2022 — Information security management systems — Requirements

ISO/IEC 27002:2022 — Information security controls

ISO/IEC 27005:2022 — Information security risk management

Apptega Product Features

- 16+ Security Frameworks
- One-Click Reporting
- Automated Alerts & Notifications
- API & Application Connectors
- Automated Framework Crosswalking
- Real-Time Compliance Scoring
- Restricted Auditor View
- Single Sign-On Connectivity
- Policy & Plan Templates
- Automated Risk Assessments
- Document Repository for Artifacts
- Multi-Tenant Environment

Apptega

About Apptega

A perennial G2 leader across various cybersecurity categories, Apptega is the cybersecurity and compliance platform purpose-built for security providers who are growing lucrative security practices, creating stickier customer relationships, and winning more business from competitors.

With Apptega's end-to-end platform, IT providers can:

1. Build continuous compliance offerings that set them apart, retain customers, and grow their ARR.
2. Build and manage world-class cybersecurity and compliance programs for their clients.
3. Increase the capacity and efficiency of their existing team so they can service 2–3× more customers.
4. Assess, measure, and manage their own security programs against a standard set of industry-leading frameworks.

To learn more, visit apptega.com

Visit apptega.com