

Information Security Management System (ISMS) — a practical implementation guide

[Czytaj po polsku](#)

An Information Security Management System (ISMS, known in Polish as SZBI) brings together leadership, people, procedures and technology to protect information across an organisation. This guide explains how to turn written commitments into working controls and evidence.

Prepared by DATPOL · updated 5 October 2026. For public authorities, their associated organisations and businesses. This British English edition concerns organisations operating in Poland; it does not claim compliance with UK legislation. Suggested schedules, risk scales and review intervals are organisational examples unless a specific legal requirement is identified. This is not an individual compliance assessment.

1. What is an ISMS?

An ISMS is an agreed, documented and continually improved approach to information security. It covers electronic records, paper documents, conversations, staff knowledge and information handled by partners. It combines responsibilities, processes and technical measures.

Its central objectives are **confidentiality** — access by authorised parties; **integrity** — protection against unauthorised alteration; and **availability** — information and services being usable when required. Accountability and trustworthy sources also matter.

For example, a member of staff must access the correct case file, an invoice payment account must not be altered fraudulently, and a council must continue serving residents after a server failure. Each objective requires different controls.

2. ISMS, ISO 27001, KRI, KSC, NIS2 and GDPR

- **ISO/IEC 27001:2022** specifies requirements for a risk-based ISMS. Certification is a separate process: an organisation can implement an ISMS without a certificate. Certification has a defined scope and does not guarantee that incidents will never occur. [ISO source](#).
- **Polish KRI:** section 19 of the regulation of 21 May 2024 provides for an ISMS in bodies performing public tasks. Section 19(2)(14) requires an internal information security audit at least annually. Its reference to an ISMS based on PN-ISO/IEC 27001 and related standards should not be confused with a blanket requirement to buy certification. [KRI source](#).
- **KSC and NIS2:** Poland's KSC amendment implementing NIS2 entered into force on 3 April 2026. Determine obligations for the specific legal entity, activities and statutory classification. Do not assume every school, municipal company or associated body has the same status. [Ministry source](#).
- **GDPR** addresses personal data; an ISMS also protects other information. Coordinate controls and evidence, but do not treat one programme as automatic compliance with the other. [GDPR, particularly Articles 32–34](#).

At the review date: official guidance identifies 3 October 2026 for registration of the relevant group and 3 April 2027 for implementing new duties for entities meeting the criteria when the amendment entered into force. The first date has already passed. Check whether entry is automatic or application-based and verify your own status. Transitional arrangements do not remove earlier KRI or data-protection obligations. [Official timetable](#); [KSC duties and criteria](#).

3. Define scope, services and accountability

Identify organisational units, sites, staff, remote working, applications, suppliers and business processes. Explain exclusions. A scope described simply as “all IT” can overlook paper archives, contractors and hosted services.

For a municipality with 25 office staff, assess the council office, school, nursery, childcare centre, cultural centre, cemetery and community premises separately. Shared IT support does not automatically create a single data controller or transfer directors' responsibilities. Common standards can help, provided ownership remains explicit.

- **Leadership:** approves scope, resources, priorities and risk acceptance.

- **ISMS coordinator:** maintains the programme, records and reviews.
- **Process owners:** define information needs and the consequences of disruption.
- **IT and suppliers:** implement agreed controls and provide operational evidence.
- **Data protection officer:** retains their independent data-protection role; they do not automatically become the IT administrator or owner of the whole ISMS.
- **Staff:** follow practical rules and report concerns through a familiar channel.

4. Inventory: what are you protecting?

Cover endpoints, servers, phones, networks, applications, licences, accounts, certificates, domains, backups, archives and external services. Record ownership, location, purpose, information category, dependencies, support expiry and maintenance responsibility. Include CCTV, access control and building automation.

An inventory agent can discover equipment and installed software. It cannot independently establish business criticality, lawful processing grounds or licence entitlement. Compare installations with contracts and purchasing evidence. Assign a register owner and update records when assets are acquired, changed or retired.

5. Information classification and everyday work

Use understandable categories such as public, internal and confidential. Define permitted storage, sharing, encryption and disposal for each. This internal scheme does not replace statutory classified-information categories.

Staff should know whether they may send a document through a personal messenger, use a private USB drive or enter case information into a public AI service. Identify approved tools and an exception process. If a rule cannot realistically be followed, improve the workflow rather than merely requesting another signature.

6. Assess risk step by step

1. Select a service or asset and identify its owner.

- 2. Describe a scenario: threat, weakness and organisational consequence.
- 3. Account for controls that actually operate.
- 4. Assess likelihood and impact using a documented method.
- 5. Choose treatment: reduce, avoid, share or knowingly accept the risk.
- 6. Assign delivery ownership, resources, deadline and completion evidence.
- 7. Reassess residual risk and obtain an authorised decision.

A 1–5 scale and multiplied score can assist prioritisation, but the number cannot replace reasoning. Consider residents, personal safety, service continuity, confidentiality, finances and obligations. Review risk after significant changes and incidents as well as on a planned cycle.

Illustrative risk-register entry

Field	Example
Process and owner	Payroll; payroll manager
Scenario	A compromised administrator account permits encryption of the server and connected backups
Impact	Delayed salary processing and possible disclosure of staff information
Treatment	MFA, separate administrator accounts, isolated backup and recovery exercise
Evidence and decision	Configuration checks, successful application test and documented residual-risk acceptance with review date

7. Documentation that supports action

A practical set includes the policy, scope, responsibilities, asset register, risk method and register, treatment plan, access rules, backup procedures, change and patch processes, incident management, continuity, supplier requirements and user guidance. Include a register of legal and contractual obligations and an audit and training plan.

Give documents an owner, version, approval, review date and intended audience. A completed leaver-access checklist provides stronger operational evidence than a general statement that accounts are protected. For an ISO 27001 implementation, prepare a Statement of Applicability with justified control decisions; check full requirements against a current, lawfully obtained copy of the standard.

8. Access, MFA and remote administration

Use individual accounts and task-appropriate privileges. Separate administration from everyday work. Prioritise MFA for email, remote access, administration and backup systems, and test recovery and emergency-access arrangements.

Process owners authorise access. Staff departure or role change triggers removal or adjustment. Reviews must include suppliers, service accounts, API keys and obsolete integrations. Supplier access needs a defined scope, expiry and activity record. Store credentials in an appropriate secrets system, never in a public knowledge base or an ordinary support ticket.

9. Patching, segmentation and physical security

Prioritise fixes according to exposure and potential impact. Changes need ownership, verification and a rollback plan. Unsupported systems require replacement decisions or documented compensating controls with review dates.

Separate administrative systems from guest Wi-Fi, cameras and technical devices. Permit communication according to service needs. Assess server-room access, power, temperature, water ingress and appropriate fire protection. Select measures through risk assessment and design: buying a camera or door lock does not establish compliance with all KSC duties.

10. Backups and continuity

The service owner defines RPO, the tolerable period of lost data, and RTO, the target recovery time. Protect backups against failure or compromise of production. The 3-2-1 approach is useful guidance, not a universal statutory prescription or proof that a backup design works.

Recovery testing should restore data, configuration and dependencies, start the application and complete an agreed business task. A matching archive checksum verifies file integrity, not service usability. Record achieved

recovery objectives, limitations and corrective action. Plan degraded operations too: communication with residents, manual intake and later reconciliation.

11. Logs, SOC and automation

A SOC supports event monitoring, alert analysis, escalation and agreed response. Define its visibility, operating hours, escalation recipients and authority. A continuously running platform is different from a staffed 24/7 analyst service.

Check log-source coverage, time synchronisation, access and justified retention. No alerts can mean missing data. Automated blocking needs approved rules, exceptions, an audit trail and an unblock procedure. AI output supports investigation; it is not independent proof of an incident or a compliance decision. Keep organisational data within the agreed environment and processing scope.

12. Incident management

Provide one simple reporting channel. The responder records timing, symptoms, affected services and actions, then escalates appropriately. Authorised personnel contain the incident and preserve evidence. Do not direct ordinary users to delete files, reinstall systems or send confidential information to private addresses.

Combine technical classification with assessment of KSC, personal-data and contractual reporting duties. Do not apply one deadline to every notification. Identify recipients, the event that starts the relevant clock, deputies and approval responsibilities. Closure includes confirmed recovery, cause analysis and completed corrective actions.

13. Suppliers, cloud and external processing

Assess supplier access, processing locations, subcontractors, support, response times, backup responsibilities and data export at contract end. Agree incident notification and evidence of service delivery. "Secure cloud" does not identify who restores an accidentally deleted register.

Before adopting remote management or an AI model, establish what information it receives, the processing basis and safeguards. Do not combine independent customers' information in a shared account without an agreed separation and access model.

14. People and training

Induction should cover authentication, email, reporting concerns, documents and devices. Managers also need decision exercises: who authorises taking a system offline, communicates with residents and approves degraded operations?

Short refreshers and scenario exercises reveal behaviour better than attendance records alone. Teach staff to verify changes to bank details through a known independent channel. Encourage prompt, honest reporting of mistakes.

15. An illustrative first 90 days

A starting plan, not a guaranteed delivery time

Period	Work	Output
Days 1–15	Scope, ownership, units, urgent gaps and requirements	Approved programme and service owners
Days 16–30	Inventory, risks, accounts, backups and suppliers	Registers and prioritised actions
Days 31–60	Procedures, controls, monitoring and training	Implementation evidence and outstanding gaps
Days 61–90	Recovery exercise, incident exercise, audit and management review	Test results, decisions and corrective plan

Complex estates, public procurement and missing records may extend implementation. Address the most serious risks and maintain an honest gap list. Do not declare completion while basic tests or accountable owners are missing.

16. Effectiveness and audit readiness

Define measures with clear denominators: critical services supplying logs, privileged accounts protected by MFA, recoveries checked at application level and overdue risk actions. “All agents online” ignores equipment that was never inventoried.

Audits need criteria, scope, competence and impartiality. Vulnerability scans and penetration tests support technical assurance but do not replace an ISMS audit. Leadership reviews results, incidents, risks and resources, assigns actions and checks completion. Monthly operational and quarterly risk reviews are possible starting points; determine actual frequency from needs and applicable obligations.

17. Acceptance checklist

- Approved scope, responsibilities and deputies.
- Current asset, service, owner and supplier registers.
- Documented legal applicability and obligations.
- Risk register and agreed treatment plan.
- Tested access provisioning and removal.
- Recovery reports for selected services, including limitations.
- Tested escalation and out-of-hours contact where required.
- Log-source coverage and SOC response authority.
- Staff understanding and exercise evidence.
- Audit results, management decisions and dated corrective actions.

18. Common questions

Can we simply buy policies? Policies need to reflect the real environment, have owners and be used in practice.

Does buying a SOC deliver an ISMS? It covers part of the technical and operational work, not the organisation's entire governance.

Does certification prove compliance with every law? No. Scope, criteria and validity matter; legal duties require separate assessment.

Does a small body need a large team? Resources should match risk. Shared or external support is possible, but accountability and availability must be explicit.

What does implementation cost? It depends on units, services, infrastructure condition and gaps. Separate assessment and documentation from licences, replacements, monitoring, tests, training and ongoing maintenance. A cheap document pack does not describe the cost of operational readiness.

19. Preparing a discussion with DATPOL

Bring site and user numbers, critical services, IT-support arrangements, backup information and known issues. These support agreement on assessment, priorities and technical work covering networks, server rooms, physical protection, recovery and monitoring integrations. Tasks, service hours and responsibilities must be agreed contractually.

[SOC monitoring and response](#) · [LCPD server-room construction and modernisation](#) · [DATPOL24 contact and service requests](#). Do not submit passwords, full configurations or residents' information through a public form.

Related guides

- [What to prepare before connecting a public authority to a SOC](#)
- [How to document a backup recovery test](#)
- [How to compare an indoor server room with a container solution](#)
- [How to prepare a business for an audit without disrupting operations](#)

Revision #2

Created 2026-10-05 12:33:32 UTC by Administrator DATPOL

Updated 2026-10-05 12:33:32 UTC by Administrator DATPOL