Statement of Applicability (SoA)

Note
One row per Annex A control of ISO/IEC 27001:2022. For each row, record whether the control applies, why you include it (risk, law, contract) or why not, how far it is implemented (implemented / partly implemented / planned / not implemented) and where the evidence is. Short titles and explanations are our own words; the wording of your licensed copy of the standard is authoritative.

ISO/IEC 27001:2022 Annex A

A.5 Organizational controls

Control	What it is about	Applicable	Justification	Status	Evidence
A.5.1 Security policy and topic policies	Everyone involved should know which security rules apply and who put them into force. A short policy signed by management forms the umbrella; below it, topic policies cover individual areas such as access, remote maintenance or backup. How to check: every policy has an approval, the date of its last review and evidence that the people concerned know it.				
A.5.2 Assigning ISMS responsibilities	Every security task has a named person who has taken it on. Typical roles in a mid-sized company are the information security officer, OT owners and risk owners; a RACI matrix shows at a glance who decides, who contributes and who is informed. Check that the appointments are in writing and that the people know about them.				
A.5.3 Segregation of duties	Separate conflicting activities (requesting/approving, changing/reviewing); in small teams, document compensating controls.				
A.5.4 Management responsibilities	Security only works when supervisors model it and expect it. Managers explain the applicable rules to their team, watch that they are followed day to day and address breaches. How to check: briefings are documented, and managers can name the key rules for their area.				
A.5.5 Authority contacts and reporting channels	Define in advance the contacts and reporting channels for the police (ZAC), BSI, the data protection authority and, where applicable, the NIS2 reporting office.				
A.5.6 Liaison with expert groups and networks	Maintain membership of industry or security networks (e.g. Alliance for Cyber Security, associations) to exchange information.				

Control	What it is about	Applicable	Justification	Status	Evidence
A.5.7 Threat intelligence	Knowing the current threat situation lets you react in time. Define sources (BSI warnings, vendor advisories, ICS advisories, industry networks), name who reviews them and record which action follows from a relevant alert. A short monthly situation report to management makes the work visible.				
A.5.8 Security built into projects	Build security requirements into every project, e.g. with a checklist at the start of projects for new plants or IT systems.				
A.5.9 Inventory of information and systems	You can only protect what you know about. Keep an inventory that shows information holdings, IT systems and production equipment together, and give each entry a responsible person. How to check: new and retired systems appear promptly, and a comparison with a network scan or the license portal finds no major gaps.				
A.5.10 Usage rules for information and devices	Staff need clear guidance on what is and is not allowed with company devices and information. A short usage policy covers, for example, private use, permitted cloud and AI services and the handling of mobile devices. Have staff confirm they have read it, and agree any monitoring with data protection and the works council.				
A.5.11 Return of equipment on leaving	On leaving or contract end, reclaim devices, keys, badges and data – using a checklist in the leaver process.				
A.5.12 Protection classes for information	Not every piece of information needs the same protection. Define a few easy-to-understand protection classes (for example public, internal, confidential, strictly confidential) and describe for each class what it means for storage, sharing and destruction. Check that the owners have actually classified their information.				
A.5.13 Making the protection class visible	Anyone holding a document or storage medium should see at once how sensitive its content is. Proven methods are markings in document templates, labels in email and office tools, and stickers on storage media. Spot check: do confidential documents in circulation carry the right marking?				
A.5.14 Secure data exchange	Information should stay protected on its way to customers, suppliers or authorities. Define which channels are allowed for each protection class, such as encrypted email, a data room or an exchange platform for CAD data, and agree the exchange with important partners by contract. How to check: confidential data does not leave unencrypted by email or through private services.				
A.5.15 Access principles	Every person should have exactly the access their task requires, and no more. Record these principles (need to know, least privilege, roles rather than individual rights) in a policy that applies equally to office IT and production. The technical implementation is covered by A.5.18 and A.8.3.				

Control	What it is about	Applicable	Justification	Status	Evidence
A.5.16 Identity lifecycle	Every action in a system should be traceable to a person or a known technical account. Define how accounts are created, changed and deleted, and record exceptions such as shared accounts on operator panels deliberately. How to check: there are no active accounts of people who have left and no accounts without a responsible person.				
A.5.17 Handling authentication data	Passwords, tokens and keys must not fall into the wrong hands. Set rules for issuing, storing and changing them, provide a password manager and replace preset passwords on machinery before commissioning. Spot-check whether credentials are lying around openly on notes or in files.				
A.5.18 Granting and recertifying rights	Rights are created only on request with approval and are removed once they are no longer needed. The responsible people confirm at fixed intervals whether the rights granted still fit; on leaving or a change of role, rights are withdrawn promptly. How to check: request and approval can be traced, and the last recertification is documented.				
A.5.19 Managing supplier risks	Suppliers with access to your data, systems or machinery bring their own risks. Group them by importance, define for each tier which security evidence you expect, and take this into account when selecting them. A supplier register with tier and date of the last assessment makes the status verifiable.				
A.5.20 Security clauses in supplier contracts	What is in the contract can be enforced later. Depending on the service, agree with important suppliers on, for example, rules for remote maintenance, deadlines for reporting incidents, confidentiality and the right to request or audit evidence. Check that the contracts of critical suppliers contain these points.				
A.5.21 Origin and support of ICT components	Consider risks from hardware and software supply chains, e.g. origin of components, update supply, SBOM for machinery.				
A.5.22 Keeping track of supplier performance	A good contract is of little use if nobody checks whether it is being kept. Assess critical suppliers at fixed intervals based on disruptions, reports or certificates, and review changes to their services before you adopt them. The result and consequences of each assessment belong in the supplier register.				
A.5.23 Selecting, running and leaving cloud services	Regulate the selection, use, configuration and exit of cloud services – including shared responsibility with the provider.				
A.5.24 Incident readiness	When an incident occurs, nobody should have to work out first who does what. Set roles, reporting channels, escalation levels and an up-to-date contact list in advance, and include scenarios for production, such as the outage of a line. How to check: the procedure is described and has been rehearsed at least once.				

Control	What it is about	Applicable	Justification	Status	Evidence
A.5.25 **Triage of reported events**	Not every report is an incident, but every report deserves a decision. Define criteria for classifying reported events, for example affected systems, protection class of the data or impact on production. Record the decision with its reasons so it can be traced later.				
A.5.26 **Handling incidents**	In an emergency, what counts is limiting the damage quickly and resuming operations safely. Keep short playbooks ready for common scenarios such as ransomware or compromised accounts, covering containment, clean-up and restart. Document during handling what was decided and when.				
A.5.27 **Incident follow-up**	Every incident reveals a weakness that can be closed. After relevant incidents, discuss in the team what went well, what did not and why, and carry the findings over into actions, the risk assessment or training. How to check: the debriefs have produced actions with a deadline and an owner.				
A.5.28 **Securing evidence**	Traces of an attack are quickly wiped out, for example by a restart or a reinstallation. Decide in advance who secures logs, storage media and system images, how the handover is documented and when an external forensics partner is called in. This keeps evidence usable for insurers, authorities or courts.				
A.5.29 **Protection in emergency operation**	Emergency operation means improvising, and that is exactly when gaps appear. Plan which protective measures must still apply during a disruption, for example no unsecured emergency access and no switching off of logging, and which fallback solutions are available for this. Check in emergency exercises whether this is adhered to.				
A.5.30 **IT and OT recovery readiness**	Derive recovery objectives (RTO/RPO) for IT and OT systems, prepare contingency plans and test them regularly.				
A.5.31 **Legal register and contractual duties**	You should always know which laws, regulations and contracts create security obligations for you. A legal register lists them with source, relevance to your company and responsible person, for example GDPR, NIS2, customer contracts and export control. Review it at least once a year and whenever new laws or major customers arrive.				
A.5.32 **Licenses and know-how protection**	Respecting the rights of others and protecting your own knowledge go together. Manage licenses centrally, prevent the installation of unlicensed software, and mark your own know-how such as designs or formulations as worth protecting. An annual comparison of license holdings and installations shows whether things match.				
A.5.33 **Keeping records safe**	Evidence such as logs, contracts, test reports or approvals must still be complete and unaltered years later. For each type, define where it is kept, who may access it and how long it is retained, and make sure it stays backed up and readable throughout that time. Spot check: can an older record be found quickly, and is it intact?				

Control	What it is about	Applicable	Justification	Status	Evidence
A.5.34 Data protection in the ISMS	Data protection and information security interlock and should not be planned separately. Involve the person responsible for data protection in risk assessment and measures, and link the record of processing activities with the asset inventory. How to check: data protection requirements appear in the ISMS policies and risk register.				
A.5.35 Outside view of the ISMS	Those who run their own ISMS easily overlook weaknesses. Have it reviewed at planned intervals and after major changes by people who have not worked on it themselves, for example through an external audit or a penetration test. Results and follow-up actions belong in the management review.				
A.5.36 Checking day-to-day rule compliance	Rules only work if they are followed in daily practice. Check this regularly in three ways: managers look closely in their area, the information security officer takes samples, and technical checks reveal deviations in configurations. Deviations found are handled like nonconformities.				
A.5.37 Written operating instructions	Important procedures should still work when the experienced person is absent. Write down the steps for backup, restoration, user administration or restarting a machine so that a competent stand-in can carry them out. Check that the instructions are current and kept where they are needed in an emergency.				

A.6 People controls

Control	What it is about	Applicable	Justification	Status	Evidence
A.6.1 Screening of candidates	Trust in new staff should rest on verified information, not just on a good impression. Depending on how sensitive the position is, decide which lawful checks take place, such as certificates, references or, for special roles, a certificate of good conduct. Document that the check took place before the person started work.				
A.6.2 Security duties in the employment contract	Anyone who works for you should know from day one which security duties come with the job. Include these duties, such as confidentiality, compliance with policies and reporting of incidents, in the employment contract or a supplementary agreement. Check that the current contract template covers this and also applies to temporary agency workers.				
A.6.3 Building security know-how	Staff should be able to recognize threats and act correctly. Plan training by target group, from short e-learning in the office and briefings at shift handover to specialist training for administrators and automation staff. How to check: participation rates are evidenced, and phishing exercises show progress.				
A.6.4 Dealing with rule violations	Define a fair process for handling rule violations, agreed with HR and the works council.				

Control	What it is about	Applicable	Justification	Status	Evidence
A.6.5 Leaving and changing roles	Not all duties end on the last working day. On leaving or changing roles, explain which duties continue to apply, for example confidentiality, and have this confirmed. At the same time, rights that are no longer needed are withdrawn through the leaver or mover process.				
A.6.6 Securing confidentiality by contract	Before confidential information leaves the company, what the recipient may do with it should be settled in writing. Use reviewed templates for staff, service providers and partners, keep an overview of the agreements concluded and adapt the templates when your protection needs change. Spot check: is there an agreement in place for current projects with external parties?				
A.6.7 Home office and mobile working	Set rules for working from home and on the move (VPN, screen lock, handling of printouts).				
A.6.8 Simple reporting channels for staff	The earlier someone reports something suspicious, the smaller the damage. Provide a simple route known to everyone, such as a phone number, a mailbox or a report button, and thank people for every report, including false alarms. How to check: when asked, staff can say how they would report something.				

A.7 Physical controls

Control	What it is about	Applicable	Justification	Status	Evidence
A.7.1 Security zones on site	A site is easier to protect when it is clear which protection applies where. Divide it into zones, such as public area, office building, production, server room and control room, and describe how the boundaries are secured. A site plan with the zones marked is good evidence.				
A.7.2 Entry control and visitors	Only authorized people should get into each zone. Control entry with key or badge systems, register visitors and escort them in protected areas. How to check: the list of entry permissions is up to date, and issued keys can be traced.				
A.7.3 Protecting sensitive rooms	Adequately secure rooms holding sensitive information or equipment (e.g. design office, control room).				
A.7.4 Site and room monitoring	Monitor the site and critical rooms, e.g. with an intruder alarm, video surveillance (involve the works council) or security guards.				
A.7.5 Building hazards and natural events	Fire, water, heat or storms can destroy equipment and documents just as an attack can. Assess which of these hazards are realistic at your sites, also in view of increasingly extreme weather, and protect important rooms accordingly, for example with fire detectors, water sensors or raised installation. The assessment belongs in the risk register.				

Control	What it is about	Applicable	Justification	Status	Evidence
A.7.6 Rules inside protected zones	Set rules for work in secure areas, e.g. mandatory escort for external companies in the server room.				
A.7.7 Nothing left out, screens locked	Introduce clear desk and clear screen rules – including at terminals and HMIs in production.				
A.7.8 Protected locations for equipment	Where a device is located partly determines how well it is protected. Install servers, network components and controllers so that dust, moisture, impacts and curious fingers stay away, for example in lockable cabinets or separate rooms. Spot check: are there open control or network cabinets in freely accessible areas?				
A.7.9 Devices on the move	Protect laptops, mobile devices and service notebooks outside the company (encryption, transport rules).				
A.7.10 Removable media and USB	Regulate the handling of USB sticks and removable media – approval, encryption, sheep-dip PC for production.				
A.7.11 Power, cooling and connectivity	Without power, cooling and connectivity, even well-protected systems come to a halt. Determine which systems depend on an uninterrupted supply and safeguard them, for example with UPS, emergency power or redundant air conditioning. How to check: the backup supply is tested under load regularly, and the results are documented.				
A.7.12 Protecting cables and cable routes	A damaged or tapped cable can paralyse whole areas or expose data. Route cables in protected ways where possible, for example in cable ducts or raised floors, separate power and data lines where necessary, and deactivate unused network sockets in halls and meeting rooms. An up-to-date plan of cables and sockets helps with checking.				
A.7.13 Maintenance of devices and installations	Well-maintained equipment fails less often, and maintenance itself must not open a back door. Schedule maintenance according to manufacturer specifications, escort or log work by external companies, and check devices that were away for repair before they go back on the network. A maintenance plan with completed dates serves as evidence.				
A.7.14 Wiping media before disposal or reuse	Securely erase or destroy storage media before disposal or hand-over – with proof from the service provider.				

A.8 Technological controls

Control	What it is about	Applicable	Justification	Status	Evidence
A.8.1 Managed endpoint devices	Manage laptops, smartphones and tablets centrally (device management), encrypt drives, enforce screen lock and automatic updates, and be able to lock or wipe lost devices remotely. Evidence: device management report with the share of managed, encrypted and up-to-date devices.				
A.8.2 Administrator rights	Grant administrative rights only to named persons, use separate personal admin accounts without email and internet, keep emergency accounts sealed and log every sign-in. Evidence: list of privileged accounts with the date of the last review, every six months being good practice.				
A.8.3 Technical enforcement of permissions	Restrict access technically as the authorization concept provides: rights via roles, shares on file storage by department, confidential areas protected separately. Evidence: role model and a sample showing that the configured rights match the concept.				
A.8.4 Protecting source code and PLC programs	Keep source code, scripts and PLC programs in version control, restrict write access to the project team and attribute changes to a person. Also make sure that system integrators provide you with the current source projects.				
A.8.5 Strong sign-in methods	Use multi-factor authentication (MFA) for all access from the internet, cloud services, email and administration; long rather than complicated passwords, lockout after failed attempts, no default passwords. Evidence: configuration export or report from the identity service showing MFA coverage and justified exceptions.				
A.8.6 Utilization and capacity planning	Monitor the utilization of servers, storage, networks and cloud services, set thresholds with alarms and plan expansions in good time. Full storage is a frequent cause of failed backups and missing logs.				
A.8.7 Defending against malware	Centrally managed protection software with behavior detection on all suitable systems, email filters and blocked macros from the internet. Where the plant manufacturer does not approve protection software: application allow list, sheep-dip PC for USB media and network segregation. Evidence: status report of the protection software and list of exceptions.				
A.8.8 Vulnerability and patch management	Detect vulnerabilities through inventory matching, vendor advisories and scanners, prioritize by severity and exploitation and remediate within fixed deadlines (good practice: 7, 30, 90 and 180 days). For OT systems that cannot be patched, keep time-limited exceptions with compensating controls in the risk register. Evidence: evaluation of open vulnerabilities by age and severity.				
A.8.9 Secure baseline configuration	Define a secure standard configuration for each system type (e.g. according to CIS Benchmarks or BSI IT-Grundschutz), roll it out centrally and check deviations regularly. Back up configurations of network components and controllers and compare them after changes.				

Control	What it is about	Applicable	Justification	Status	Evidence
A.8.10 Deletion periods and methods	Define a retention period and deletion route for each data type, also in backups, archives and at cloud providers. Securely erase media and devices before disposal, repair or return, or have them destroyed in accordance with DIN 66399. Evidence: deletion logs and certificates of destruction.				
A.8.11 Masking real data	Do not use real personnel or customer data in test, training and analysis environments; where real data is necessary, mask or pseudonymize names and identifiers and document the approval.				
A.8.12 Securing data outflow channels	Determine which information is worth protecting, such as design data, and secure the leakage routes: restrict USB media, block private cloud storage, send confidential attachments only to approved recipients, exchange data via a logged platform. Coordinate technical monitoring with data protection and the works council.				
A.8.13 Backup and restore testing	Derive the backup concept from the recovery time objective and the maximum tolerable data loss of the processes, apply the 3-2-1-1-0 rule with at least one immutable or offline copy, and give the backup system its own credentials. Also back up PLC programs and plant configurations after every change. Evidence: log of the last full restore test with time measurement.				
A.8.14 Redundant design of critical systems	Design systems whose failure is not tolerable redundantly (second line, cluster, second power supply, second site) and test the failover regularly. Redundancy does not replace a backup, because deleted or encrypted data is mirrored as well.				
A.8.15 Collecting and protecting logs	Log sign-ins and sign-outs including failed attempts, permission changes, admin actions, configuration changes, findings of the protection software, connections between zones and remote maintenance sessions, collect them centrally and protect them against alteration. Retention, good practice: 90 days searchable, 6 to 12 months archived, agreed with data protection.				
A.8.16 Alerting on anomalies	Define a few well-tuned alarm rules with clear responsibility (e.g. many failed sign-ins, admin sign-in at night, new connection into the production network, deleted backups) and document regular evaluations. In production, passively reading network traffic on a mirror port has proven effective.				
A.8.17 Uniform system time	Synchronize all systems, including network components and controllers, with a common, reliable time source, store logs in a uniform time zone and report deviations. Without a uniform time, incidents can hardly be reconstructed.				
A.8.18 Powerful admin tools	Install tools that can bypass security mechanisms or change systems fundamentally (admin tools, debuggers, scanners, engineering software for controllers) only on designated systems, restrict them to named persons and make their use traceable.				
A.8.19 Approved software	Give users no installation rights, distribute software only from an approved catalog and approve new programs after checking origin, license and security. On servers and operator stations, install only through change management.				

Control	What it is about	Applicable	Justification	Status	Evidence
A.8.20 Network components and network map	Configure and manage network components securely (management only from an admin network, no default passwords, current firmware), keep a current network map and control transitions between IT and OT through firewalls with documented rules. Evidence: network map and rule set with the date of the last review.				
A.8.21 Requirements for network providers	Define security requirements for internet, VPN and site connections and agree them with the providers (availability, encryption, reporting of faults and incidents). Evaluate performance and fault reports regularly.				
A.8.22 Network zones and segmentation	Divide networks into zones by protection requirement, at a minimum office IT, production network, DMZ for transitions, guest network and a management network for administrators. Connections between zones only where expressly permitted; the zone and conduit logic of IEC 62443 is a good basis for this.				
A.8.23 Web and DNS filtering	Block access to malicious and unwanted websites through a web filter or DNS filter and prevent uploads to private cloud storage. Production systems should have no direct internet access.				
A.8.24 Encryption and key management	Define where encryption or signing is used (drives, transmission, backups, stored passwords, remote maintenance), set minimum standards according to the state of the art (e.g. BSI TR-02102), switch off insecure methods and manage keys and certificates over their whole lifecycle, including recovery and revocation.				
A.8.25 Security in every development phase	Build security into every phase of in-house development: requirements and threat analysis before the start, secure coding, tests before release, maintenance of the software components. This also applies to control software; manufacturers of products with digital elements must additionally demonstrate this under the Cyber Resilience Act.				
A.8.26 Security in the requirements specification	Define security requirements before applications or plants are developed or procured, e.g. as an annex to the requirements specification: personal accounts, MFA for remote access, logging, updates over the service life, component list, documented ports.				
A.8.27 Architecture principles	Define architecture principles such as defense in depth, least privilege, secure defaults and the zone model in writing and demonstrably apply them in the design of systems, networks and plants, e.g. in a short architecture review.				
A.8.28 Coding rules and code review	Define coding rules (e.g. according to OWASP), have changes reviewed by a second person, automate static code analysis and checking of third-party components for known vulnerabilities. For PLC programs, a separate programming guideline with commenting and approval.				
A.8.29 Security testing before commissioning	Test security before commissioning: automated tests for software, penetration tests for exposed systems, and for plants a security check in the factory and site acceptance test (FAT/SAT) covering default passwords, open services and remote accesses.				

Control	What it is about	Applicable	Justification	Status	Evidence
A.8.30 External developers and integrators	Control external development and system integrators through security requirements in the contract, evidence (test reports, component list), controlled access to your systems and an acceptance with handover of all program versions and accounts.				
A.8.31 Keeping development, test and production apart	Separate development, test and production; developers have no write rights in production. Test changes to controllers first on a simulation or spare controller where possible.				
A.8.32 Controlled changes	Request changes to IT and OT systems, assess them by risk and impact, test, approve, implement with a fallback plan and document them. Approve standard changes in advance, document emergency changes retrospectively. Evidence: change log with sample.				
A.8.33 Handling test data	Select and protect test data deliberately; real data in test systems only exceptionally, with approval, masked or pseudonymized and for a limited time. Protect test environments with real data like production.				
A.8.34 Testing without disrupting operations	Plan technical checks such as penetration tests, vulnerability scans or audits on running systems, agree scope and time window with those responsible and limit the auditors' access in time. In production, active scans only by arrangement and during planned downtimes.				

About this template

Template version 1.0-80a8b81c
Content as of 26 September 2026
Published by Made with Complass, https://complass.eu

Legal basis (as of): ISO/IEC 27001:2022 und ISO/IEC 27001:2022/Amd 1:2024 (Originaltext)

This template is not legal advice. It does not replace checking which requirements apply to your company and does not guarantee any audit or certification result.

License: Creative Commons Attribution 4.0 International (CC BY 4.0). You may use, change and pass on the template, also commercially, as long as you name the source. Attribution: "Template: Complass (complass.eu), CC BY 4.0". https://creativecommons.org/licenses/by/4.0/deed.en