ISO 27001:2022 Annex A Controls List

All 93 controls across the four themes, each with a plain-English summary of what it requires. Controls marked **NEW** were introduced in the 2022 edition and have no direct 2013 equivalent.

Prepared by Alan Parker, ISO/IEC 27001:2022 Lead Auditor. These summaries are a practitioner's paraphrase to help you navigate the standard; they are not the text of ISO/IEC 27001 or 27002, which you should obtain from ISO or your national standards body. Each control has a full implementation guide at https://iseoblue.com/iso-27001/annex-a/iso-27001-controls-list/

Organisational controls (5.1 to 5.37)

5.1	**Policies for information security**	The set of approved, documented, and communicated policies that direct how your organisation manages information security.
5.2	**Information security roles and responsibilities**	Clear definitions of who is accountable for what across the ISMS, from top management down to individual contributors.
5.3	**Segregation of duties**	Splitting conflicting tasks between different people so that no single person can both perform and authorise sensitive activities.
5.4	**Management responsibilities**	The expectation that management actively requires staff to follow security policies and procedures, not just assume they will.
5.5	**Contact with authorities**	Established relationships with regulators, law enforcement, and other authorities you may need to engage with, before you need to engage with them.
5.6	**Contact with special interest groups**	Active participation in security forums, industry bodies, and professional networks to stay informed about emerging threats and good practice.
5.7	**Threat intelligence NEW**	The collection and analysis of information about current and emerging threats relevant to your organisation, used to inform security decisions.
5.8	**Information security in project management**	Building security considerations into how projects are planned, run, and delivered, rather than bolting them on at the end.
5.9	**Inventory of information and other associated assets**	A maintained register of the information, systems, and equipment that matter to your business, with named owners.
5.10	**Acceptable use of information and other associated assets**	Documented rules covering how staff and other users are permitted to handle the organisation’s information and equipment.
5.11	**Return of assets**	The process for recovering laptops, access cards, documents, and other assets when staff leave or change roles.
5.12	**Classification of information**	A scheme for categorising information based on its sensitivity, value, and the protection it requires.
5.13	**Labelling of information**	Marking information consistently with its classification so that the people handling it know how to treat it.
5.14	**Information transfer**	Rules and protections for moving information between people, systems, or organisations in a secure way.
5.15	**Access control**	The overall framework that defines who can access what, on what basis, and how that access is governed.
5.16	**Identity management**	The lifecycle of user identities across your systems, from creation through changes to deletion.
5.17	**Authentication information**	The management of passwords, tokens, keys, and other secrets that prove a user is who they say they are.
5.18	**Access rights**	The day-to-day provisioning, review, and removal of user access to systems and information.

5.19	**Information security in supplier relationships**	The approach to identifying, assessing, and managing information security risks from your suppliers and third parties.
5.20	**Addressing information security within supplier agreements**	Ensuring contracts with suppliers include appropriate security clauses, responsibilities, and expectations.
5.21	**Managing information security in the ICT supply chain**	Extending supplier security thinking to the wider chain of providers behind your direct suppliers.
5.22	**Monitoring, review and change management of supplier services**	The ongoing process of checking that suppliers continue to deliver to the agreed security standard.
5.23	**Information security for use of cloud services NEW**	The processes for assessing, adopting, managing, and exiting cloud services securely.
5.24	**Information security incident management planning and preparation**	Having a documented incident response capability in place before you need it.
5.25	**Assessment and decision on information security events**	The process for deciding whether a reported event is actually a security incident that needs a response.
5.26	**Response to information security incidents**	The structured handling of confirmed incidents, including containment, communication, and resolution.
5.27	**Learning from information security incidents**	Capturing lessons from incidents and feeding them back into improvements to the ISMS.
5.28	**Collection of evidence**	Preserving evidence during and after incidents in a way that supports investigation, legal action, or regulatory reporting.
5.29	**Information security during disruption**	Maintaining appropriate information security even when normal operations are disrupted by an incident or crisis.
5.30	**ICT readiness for business continuity NEW**	Ensuring your IT services can be recovered to required levels within required timeframes when disruption occurs.
5.31	**Legal, statutory, regulatory and contractual requirements**	A maintained understanding of the external requirements your organisation must comply with, and how you're meeting them.
5.32	**Intellectual property rights**	Protecting your own IP and ensuring you don't infringe on the IP of others through your operations.
5.33	**Protection of records**	Safeguarding records from loss, destruction, falsification, unauthorised access, and unauthorised release in line with retention requirements.
5.34	**Privacy and protection of PII**	Handling personally identifiable information in line with applicable privacy laws and the expectations of the people whose data you hold.
5.35	**Independent review of information security**	Periodic reviews of the ISMS by someone independent from those who run it day-to-day.
5.36	**Compliance with policies, rules and standards for information security**	Verifying that your own policies and standards are actually being followed in practice.
5.37	**Documented operating procedures**	Written procedures for the operational tasks that support information security, so they happen consistently regardless of who's doing them.

People controls (6.1 to 6.8)

6.1	**Screening**	Background checks on candidates for roles where the level of access or responsibility justifies verifying who they are and what they've done.

6.2	**Terms and conditions of employment**	Building information security responsibilities into employment contracts so that staff obligations around confidentiality and acceptable behaviour are formally established.
6.3	**Information security awareness, education and training**	Ongoing training that ensures staff understand the security risks they face, the policies they need to follow, and what's expected of them in their role.
6.4	**Disciplinary process**	A formal process for handling staff who breach information security policies, with consequences proportionate to the breach.
6.5	**Responsibilities after termination or change of employment**	Making clear which security obligations continue to apply after someone leaves or changes role, particularly around confidentiality.
6.6	**Confidentiality or non-disclosure agreements**	Formal NDAs covering the protection of information shared with staff, contractors, and other parties.
6.7	**Remote working**	Rules and protections for staff who access organisational information from outside the office, including home, client sites, and travel.
6.8	**Information security event reporting**	A clear, accessible process for staff to report suspected security events without fear of blame, so issues surface quickly.

Physical controls (7.1 to 7.14)

7.1	**Physical security perimeters**	Defined and protected boundaries around areas that contain information or information processing facilities, with appropriate access controls at each boundary.
7.2	**Physical entry**	Controls that ensure only authorised people can enter secure areas, typically through a combination of locks, badges, sign-in procedures, and supervision.
7.3	**Securing offices, rooms and facilities**	Practical measures to protect the spaces where work happens, from server rooms to general office areas, against unauthorised access and environmental threats.
7.4	**Physical security monitoring** NEW	Active monitoring of premises through CCTV, alarms, intruder detection, or other systems that identify unauthorised physical access in real time.
7.5	**Protecting against physical and environmental threats**	Protections against natural and man-made threats such as fire, flood, power loss, and theft, proportionate to the value of what's being protected.
7.6	**Working in secure areas**	Rules and protections covering how staff and visitors should behave when working in areas that hold sensitive information or critical systems.
7.7	**Clear desk and clear screen**	Practices that prevent sensitive information being left visible on desks, screens, whiteboards, or printers when unattended.
7.8	**Equipment siting and protection**	Positioning equipment so that it's protected from environmental hazards and from being overlooked, tampered with, or damaged.
7.9	**Security of assets off-premises**	Protections for organisational equipment and information when used outside the office, including laptops in transit, equipment at home, and devices on client sites.
7.10	**Storage media**	Controls covering the lifecycle of removable media (USB drives, backup tapes, disposable hard drives) from acquisition through use to secure disposal.
7.11	**Supporting utilities**	Protections for the utilities that information processing depends on, particularly power, cooling, and telecommunications.
7.12	**Cabling security**	Protecting the network and power cabling that supports information systems against interception, interference, and accidental damage.

7.13	**Equipment maintenance**	Maintaining equipment correctly so that it remains reliable and so that maintenance activities don't introduce security risks.
7.14	**Secure disposal or re-use of equipment**	Ensuring that equipment containing information is wiped or destroyed properly before disposal or reuse, so data isn't recoverable from old kit.

Technological controls (8.1 to 8.34)

8.1	**User end point devices**	Protection for laptops, desktops, tablets, and phones used to access organisational information, covering configuration, encryption, and user responsibilities.
8.2	**Privileged access rights**	Strict management of administrator and other elevated accounts, ensuring they are allocated sparingly, used appropriately, and reviewed regularly.
8.3	**Information access restriction**	Limiting access to information and application functions based on the access control policy and individual business needs.
8.4	**Access to source code**	Controls to protect source code, development tools, and software libraries from unauthorised access or modification.
8.5	**Secure authentication**	Authentication mechanisms appropriate to the sensitivity of the information being accessed, including multi-factor authentication where justified by risk.
8.6	**Capacity management**	Monitoring and tuning of resources to ensure systems have the capacity needed to meet current and projected demands.
8.7	**Protection against malware**	A combination of detection tools, prevention measures, and user awareness to defend systems against malicious software.
8.8	**Management of technical vulnerabilities**	A systematic approach to identifying, evaluating, and remediating technical vulnerabilities across the organisation's systems.
8.9	**Configuration management** NEW	Establishing, documenting, and maintaining secure configurations for hardware, software, services, and networks.
8.10	**Information deletion** NEW	Secure deletion of information from systems, devices, and storage media when no longer required, in line with retention obligations.
8.11	**Data masking** NEW	Techniques such as anonymisation and pseudonymisation to protect sensitive data, particularly in non-production environments.
8.12	**Data leakage prevention** NEW	Measures to detect and prevent the unauthorised disclosure or extraction of sensitive information from systems and networks.
8.13	**Information backup**	Regular, tested backups of information, software, and systems, stored and protected so they can be restored when needed.
8.14	**Redundancy of information processing facilities**	Building enough redundancy into critical systems to meet availability requirements, including failover and resilience measures.
8.15	**Logging**	Producing, storing, and protecting logs of activities, exceptions, faults, and security events for review and investigation.
8.16	**Monitoring activities** NEW	Active monitoring of networks, systems, and applications for anomalous behaviour and potential security incidents.
8.17	**Clock synchronisation**	Synchronising the clocks of all relevant systems to a single reference time source to support accurate logging and investigations.
8.18	**Use of privileged utility programs**	Tightly controlled use of utility programs that could override system or application controls, restricted to authorised personnel only.
8.19	**Installation of software on operational systems**	Procedures and controls governing how software is installed and updated on production systems to maintain integrity and security.
8.20	**Networks security**	Securing networks and the information they carry through controls such as segregation, access management, and threat protection.

8.21	**Security of network services**	Identifying and including security mechanisms, service levels, and management requirements for all network services, whether in-house or outsourced.
8.22	**Segregation of networks**	Dividing networks into separate domains based on trust, function, or sensitivity to limit the impact of any single compromise.
8.23	**Web filtering NEW**	Managing access to external websites to reduce exposure to malicious content and inappropriate use of organisational resources.
8.24	**Use of cryptography**	A defined approach to using cryptography effectively, including key management, to protect the confidentiality, integrity, and authenticity of information.
8.25	**Secure development life cycle**	Embedding security into every stage of software and system development, from requirements through to deployment.
8.26	**Application security requirements**	Identifying, specifying, and approving security requirements when developing or acquiring applications.
8.27	**Secure system architecture and engineering principles**	Establishing, documenting, and applying engineering principles to ensure systems are designed and built securely.
8.28	**Secure coding NEW**	Applying secure coding principles and practices to reduce vulnerabilities introduced during software development.
8.29	**Security testing in development and acceptance**	Defining and carrying out security testing throughout the development life cycle and before systems are accepted into production.
8.30	**Outsourced development**	Directing, monitoring, and reviewing the activities of any third parties involved in developing systems on the organisation's behalf.
8.31	**Separation of development, test and production environments**	Keeping development, testing, and live environments separate to reduce the risk of unauthorised changes or accidental impact on production.
8.32	**Change management**	A controlled process for making changes to information processing facilities and systems, including assessment, approval, and review.
8.33	**Test information**	Selecting, protecting, and managing test data appropriately, particularly when it is derived from production information.
8.34	**Protection of information systems during audit testing**	Planning and agreeing audit tests on operational systems carefully so they do not disrupt business processes or compromise data.

Free to use within your own organisation. Please do not resell or republish. For a free Excel version with Statement of Applicability working columns, see the controls list page on iseoblue.com.