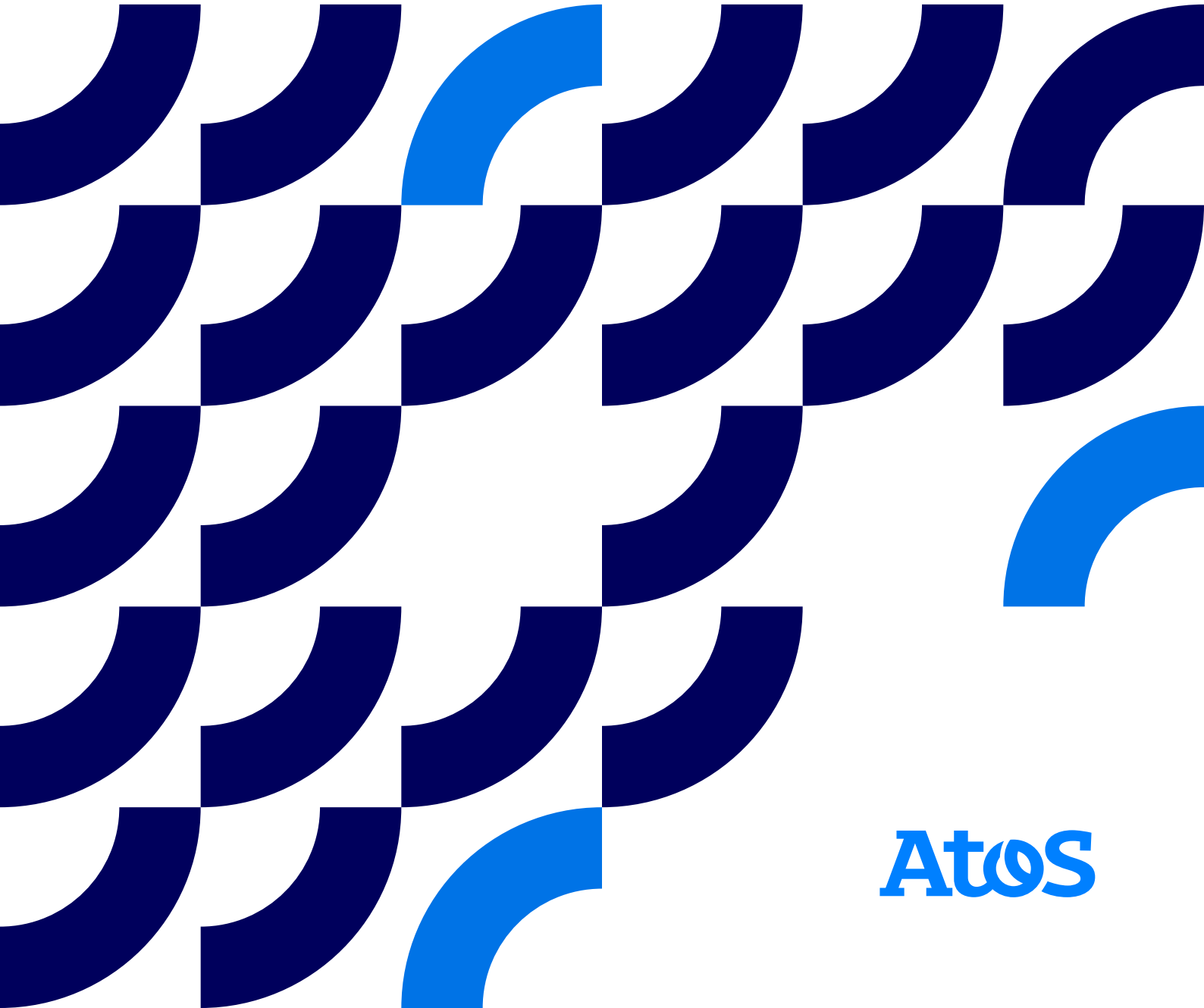
Atos Global Statement of Applicability

Author(s)	Document Reference	Version
Group Security	0000077	4.3
Status	**Source**	**Document Date**
Final	Atos	10 March 2025
Number of Pages	**Owner**	
10	Group Security	



Contents

1 Introduction for Public Version

1.1 Purpose

Atos Group operates an Information Security Management System (ISMS) that is certified against ISO/IEC 27001:2022 and supports service delivery worldwide. This certification demonstrates Atos Group's ongoing commitment to maintaining and continually improving an effective ISMS across the organization.

In accordance with ISO/IEC 27001:2022 requirements, Atos internally produces and maintains the Statement of Applicability (SoA) as part of information security risk treatment (Clause 6.1.3). The internal SoA is a living document that supports the continued effectiveness of the ISMS over time. It records the Annex A controls selected for risk treatment, maps them to the relevant policies, and documents the rationale for inclusion or exclusion.

This document is the public version of the internal SoA, providing a simplified view of the applicability status of the ISO/IEC 27001:2022 Annex A controls for the Atos Group and serves as a reference for our corresponding ISO certificate.

1.2 Scope

The Atos Global SoA applies worldwide to all Atos Group entities. Where required (for example, to meet local legal or regulatory requirements), it may be supplemented by locally applicable additions. Any such additions shall be documented and approved in line with the ISMS Scope Definition for the relevant local scope.

1.3 Document maintenance and distribution

The internal SoA is the authoritative version and is reviewed at least once every two years and whenever relevant changes occur. This public version is updated following each approved change to the internal SoA to ensure it remains aligned and reflects the current applicability status of Annex A controls. The document number, version number and document date are kept identical to the internal SoA to evidence this synchronization.

2 Atos Statement of Applicability

Information Security Control in ISO 27001:2022 Annex A			Applicable
A.5 Organizational Controls			
A.5.1	Policies for information security	Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Yes
A.5.2	Information security roles and responsibilities	Information security roles and responsibilities should be defined and allocated according to the organization needs.	Yes
A.5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility should be segregated.	Yes
A.5.4	Management responsibilities	Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	Yes
A.5.5	Contact with authorities	The organization should establish and maintain contact with relevant authorities.	Yes
A.5.6	Contact with special interest groups	The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Yes
A.5.7	Threat intelligence	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	Yes
A.5.8	Information security in project management	Information security should be integrated into project management.	Yes
A.5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, should be developed and maintained.	Yes
A.5.10	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	Yes
A.5.11	Return of assets	Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	Yes
A.5.12	Classification of information	Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	Yes

Information Security Control in ISO 27001:2022 Annex A			Applicable
A.5.13	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Yes
A.5.14	Information transfer	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.	Yes
A.5.15	Access control	Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.	Yes
A.5.16	Identity management	The full life cycle of identities shall be managed.	Yes
A.5.17	Authentication information	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.	Yes
A.5.18	Access rights	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	Yes
A.5.19	Information security in supplier relationships	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Yes
A.5.20	Addressing information security within supplier agreements	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	Yes
A.5.21	Managing information security in the information and communication technology (ICT) supply-chain	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	Yes
A.5.22	Monitoring, review and change management of supplier services	The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery	Yes
A.5.23	Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.	Yes
A.5.24	Information security incident management planning and preparation	The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	Yes
A.5.25	Assessment and decision on information security events	The organization shall assess information security events and decide if they are to be categorized as information security incidents	Yes
A.5.26	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Yes

Information Security Control in ISO 27001:2022 Annex A			Applicable
A.5.27	Learning from information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	Yes
A.5.28	Collection of evidence	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Yes
A.5.29	Information security during disruption	The organization should plan how to maintain information security at an appropriate level during disruption.	Yes
A.5.30	ICT readiness for business continuity	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Yes
A.5.31	Legal, statutory, regulatory and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	Yes
A.5.32	Intellectual property rights	The organization shall implement appropriate procedures to protect intellectual property rights	Yes
A.5.33	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Yes
A.5.34	Privacy and protection of personal identifiable information (PII)	The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Yes
A.5.21	Managing information security in the information and communication technology (ICT) supply-chain	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	Yes
A.5.35	Independent review of information security	The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	Yes
A.5.36	Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.	Yes
A.5.37	Documented operating procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	Yes

Information Security Control in ISO 27001:2022 Annex A			Applicable
A.6 People Controls			
A.6.1	Screening	Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Yes
A.6.2	Terms and conditions of employment	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	Yes
A.6.3	Information security awareness, education and training	Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	Yes
A.6.4	Disciplinary process	A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	Yes
A.6.5	Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	Yes
A.6.6	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	Yes
A.6.7	Remote working	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Yes
A.6.8	Information security event reporting	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Yes
A.7 Physical Controls			
A.7.1	Physical security perimeters	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	Yes
A.7.2	Physical entry	Secure areas shall be protected by appropriate entry controls and access points.	Yes
A.7.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and implemented.	Yes
A.7.4	Physical security monitoring	Premises shall be continuously monitored for unauthorized physical access.	Yes
A.7.5	Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	Yes
A.7.6	Working in secure areas	Security measures for working in secure areas shall be designed and implemented	Yes

Information Security Control in ISO 27001:2022 Annex A			Applicable
A.7.7	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	Yes
A.7.8	Equipment siting and protection	Equipment shall be sited securely and protected.	Yes
A.7.9	Security of assets off-premises	Off-site assets shall be protected.	Yes
A.7.10	Storage media	Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Yes
A.7.11	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes
A.7.12	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	Yes
A.7.13	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	Yes
A.7.14	Secure disposal or re-use of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Yes
A.8 Technological Controls			
A.8.1	User end point devices	Information stored on, processed by or accessible via user end point devices shall be protected.	Yes
A.8.2	Privileged access rights	The allocation and use of privileged access rights shall be restricted and managed.	Yes
A.8.3	Information access restriction	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	Yes
A.8.4	Access to source code	Read and write access to source code, development tools and software libraries shall be appropriately managed.	Yes
A.8.5	Secure authentication	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	Yes
A.8.6	Capacity management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	Yes
A.8.7	Protection against malware	Protection against malware shall be implemented and supported by appropriate user awareness.	Yes
A.8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	Yes
A.8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	Yes

Information Security Control in ISO 27001:2022 Annex A			Applicable
A.8.10	Information deletion	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	Yes
A.8.11	Data masking	Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	Yes
A.8.12	Data leakage prevention	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Yes
A.8.13	Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	Yes
A.8.14	Redundancy of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Yes
A.8.15	Logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed. Logging facilities and log information shall be protected against tampering and unauthorized access. System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	Yes
A.8.16	Monitoring activities	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Yes
A.8.17	Clock synchronization	The clocks of all relevant information processing.	Yes
A.8.18	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	Yes
A.8.19	Installation of software on operational systems	Procedures and measures shall be implemented to securely manage software installation on operational systems.	Yes
A.8.20	Networks security	Networks shall be managed and controlled to protect information in systems and applications.	Yes
A.8.21	Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	Yes
A.8.22	Segregation of networks	Groups of information services, users and information systems shall be segregated on networks.	Yes
A.8.23	Web filtering	Access to external websites shall be managed to reduce exposure to malicious content	Yes
A.8.24	Use of cryptography	A policy on the use of cryptographic controls for protection of information shall be developed and implemented. A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	Yes
A.8.25	Secure development life cycle	Rules for the development of software and systems shall be established and applied to developments within the organization.	Yes

Information Security Control in ISO 27001:2022 Annex A			Applicable
A.8.26	Application security requirements	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification. Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay	Yes
A.8.27	Secure system architecture and engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	Yes
A.8.28	Secure coding	Secure coding principles shall be applied to software development.	Yes
A.8.29	Security testing in development and acceptance	Testing of security functionality shall be carried out during development. Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	Yes
A.8.30	Outsourced development	The organization shall supervise and monitor the activity of outsourced system development.	Yes
A.8.31	Separation of development, test and production environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment. Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	Yes
A.8.32	Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled. Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security. Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	Yes
A.8.33	Test information	Test data shall be selected carefully, protected and controlled.	Yes
A.8.34	Protection of information systems during audit testing	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes	Yes

About Atos Group

Atos Group is a global leader in digital transformation with c. 63,000 employees and annual revenue of c. €8 billion, operating in 61 countries under two brands — Atos for services and Eviden for products. European number one in cybersecurity, cloud and high performance computing, Atos Group is committed to a secure and decarbonized future and provides tailored AI-powered, end-to-end solutions for all industries. Atos Group is the brand under which Atos SE (Societas Europaea) operates. Atos SE is listed on Euronext Paris.

The purpose of Atos Group is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us
atos.net
atos.net/career

Let's start a discussion together

107643-JS+GR-Brochure-Statement of Application