cegid

Statement of Applicability

ISO27001:2022

Certificate No: IS 666376 **Version of 15/01/2025** **Modified by: Security Team**
Classification: Public

ISO27001:2022

		Implemented solution
4	**Context of the organisation**	
4.1	Understanding the organization and its context	Scope of the Security Management System for Cegid Cloud
4.2	Understanding the needs and expectations of interested parties	
4.3	Determining the scope of the information security management system	
4.4	Information security management system	
5	**Leadership**	
5.1	Leadership and commitment	Governance Management, Roles and Responsibilities of ISMS
5.2	Policy	
5.3	Organizational roles, responsibilities and authorities	
6	**Planification**	
6.1	Actions liées aux risques et opportunités	Risk Assessment and Treatment Process
6.2	Information security objectives and planning to achieve them	
6.3	Planning of changes	
7	**Support**	
7.1	Resources	Human Resources Security
7.2	Competence	
7.3	Awareness	
7.4	Communication	ISMS Communication Process
7.5	Documented information	Documentation Management Process
8	**Fonctionnement**	
8.1	Operational planning and control	Control, Monitoring, and Improvement Policy
8.2	Information security risk assessment	Risk Management Process
8.3	Information security risk treatment	
9	**Evaluation des performanaces**	
9.1	Monitoring, measurement, analysis and evaluation	Control, Monitoring, and Improvement Policy
9.2	Internal audit	Compliance and Audit Management
9.3	Management review	Governance Management, Roles and Responsibilities of ISMS
10	**Amélioration**	
10.1	Continual improvement	Control, Monitoring, and Improvement Policy
10.2	Nonconformity and corrective action	Compliance and Audit Management

The implementation of security controls defined in the statement of applicability aims to reduce security risks that may exist within the ISMS

ISO 27001 - Annex A1

ISO27001:2022	Operational Capabilities	Requirements		Applicable (Inclusion) 2 values _ YES _ NO	Justification for Inclusion of the Measure	Implementation of the Measure 2 values _ YES _ NO	Solution Implemented
Organizational controls							
5.1	#Governance	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	Risk Analysis	YES	An information security policy has been drafted. It is reviewed annually and approved by the Cloud Services Management
5.2	#Governance	Information security roles and responsibilities	Information security roles and responsibilities should be defined and allocated according to the organization needs	YES	Risk Analysis	YES	The group security team is organized transversally. It is independent both hierarchically and operationally from ISMS activities
5.3	#Governance	Segregation of duties	Conflicting duties and conflicting areas of responsibility should be segregated	YES	Risk Analysis	YES	DevOps-style organization of missions and teams
5.4	#Governance	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	Risk Analysis	YES	Formal commitment from the Cloud Services Management through various committees, meetings, and communications concerning security and the ISMS
5.5	#Governance	Contact with authorities	The organization should establish and maintain contact with relevant authorities	YES	Risk Analysis	YES	The Cegid Security team maintains regular exchanges with the CNIL and ANSSI
5.6	#Governance	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	Risk Analysis	YES	Members of the Cegid Security team are part of the following associations: CLUSIF, Club ISO27001, Business Continuity Club, Incibe, etc.
5.7	#Threat_and_vulnerability_management	Threat intelligence	Information relating to information security threats should be collected and analysed to produce threat intelligence	YES	Risk Analysis	YES	Subscription to a global monitoring service. Biannual meetings of ISMS Managers for analysis, Threat Intelligence Policy
5.8	#Governance	Information security in project management	Information security should be integrated into project management	YES	Risk Analysis	YES	Organization of teams and processes in agile mode (AzureDevOps) to incorporate security in infrastructure and development in all projects related to ISMS
5.9	#Asset_management	Inventory of information and other associated assets	Management of user registrations/unregistrations in our Cegid Cloud platform orchestration tool	YES	Risk Analysis	YES	The asset inventory is reviewed and updated in the risk analysis tool. Assets are owned by the Cloud Services Management
5.10	#Asset_management #Information_protection	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented	YES	Risk Analysis	YES	A charter for the use of IT tools is communicated to employees
5.11	#Asset_management	Return of assets	Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement	YES	Risk Analysis	YES	Return of assets according to the inventory from the employee departure form under the manager's responsibility
5.12	#Information_protection	Classification of information	Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements	YES	Risk Analysis	YES	Information is classified
5.13	#Information_protection	Labelling of information	An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.	YES	Risk Analysis	YES	All assets (documents, client assets) are subject to the asset management policy. This policy takes into account the classification level of assets associated with their level of dissemination and encryption needed for their distribution
5.14	#Asset_management #Information_protection	Information transfer	Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties	YES	Risk Analysis	YES	A policy outlining encryption and communication security rules is established. It is periodically reviewed. Secure exchange protocols used with third parties ensure the integrity, confidentiality, and non-repudiation of information. Secure protocols are used in email communication
5.15	#Identity_and_access_management	Access control	Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements	YES	Risk Analysis	YES	Access control policy
5.16	#Identity_and_access_management	Identity management	The full life cycle of identities should be managed	YES	Risk Analysis	YES	Management of user registrations/unregistrations in our Cegid Cloud platform orchestration tool
5.17	#Identity_and_access_management	Authentication information	Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information	YES	Risk Analysis	YES	Rules for the use of secret information are clearly defined in the IT tools usage charter
5.18	#Identity_and_access_management	Access rights	Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control	YES	Risk Analysis	YES	Management of user registrations/unregistrations in our Cegid Cloud platform orchestration tool
5.19	#Supplier_relationships_security	Information security in supplier relationships	Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services	YES	Risk Analysis	YES	The security policy in supplier relations takes into account and describes the necessary security needs and measures to meet Cegid's legal, regulatory, and contractual obligations

5.20	#Supplier_relationships_security	Addressing information security within supplier agreements	Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship	YES	Risk Analysis	YES	Cegid ensures the involvement of its suppliers in the security of the service delivered through certification and contractual commitment
5.21	#Supplier_relationships_security	Managing information security in the ICT supply chain	Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain	YES	Risk Analysis	YES	Cegid ensures the involvement of its suppliers in the security of the service delivered through certification and contractual commitment
5.22	#Supplier_relationships_security #Information_security_assurance	Monitoring, review and change management of supplier services	The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery	YES	Risk Analysis	YES	Security steering committees are planned and organized recurrently with key suppliers. Cegid Cloud monitors the information security certifications of its suppliers
5.23	#Supplier_relationships_security	Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements	YES	Risk Analysis	YES	Cegid ensures that contracts with cloud service providers comply with the organization's information security requirements.
5.24	#Governance #Information_security_event_management	Planification et préparation de la gestion des incidents de sécurité de l'information	The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities	YES	Risk Analysis	YES	Security incident management process (see Security Assurance Plan for more details)
5.25	#Information_security_event_management	Assessment and decision on information security events	The organization should assess information security events and decide if they are to be categorized as information security incidents	YES	Risk Analysis	YES	
5.26	#Information_security_event_management	Response to information security incidents	Information security incidents should be responded to in accordance with the documented procedures	YES	Risk Analysis	YES	
5.27	#Information_security_event_management	Learning from information security incidents	Knowledge gained from information security incidents should be used to strengthen and improve the information security controls	YES	Risk Analysis	YES	
5.28	#Information_security_event_management	Collection of evidence	The organization should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events	YES	Risk Analysis	YES	
5.29	#Continuity	Information security during disruption	The organization should plan how to maintain information security at an appropriate level during disruption.	YES	Risk Analysis	YES	A business continuity policy governs the organization and information security continuity processes
5.30	#Continuity	ICT readiness for business continuity	ICT readiness should be planned, implemented, maintained and tested based on business continuityobjectives and ICT continuity requirements	YES	Risk Analysis	YES	
5.31	#Legal_and_compliance	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 should be identified, documented and kept up to date.	YES	Risk Analysis	YES	The legal process of the Cegid group defines, documents, and updates all legal, regulatory, and contractual requirements applicable to the ISMS. Cegid Cloud complies with applicable agreements, laws, and regulations related to cryptography. Cegid does not import or export cryptographic solutions
5.32	#Legal_and_compliance	Intellectual property rights	The organization should implement appropriate procedures to protect intellectual property rights	YES	Risk Analysis	YES	Cegid Cloud is committed to ensuring compliance with legal, regulatory, and contractual requirements related to intellectual property rights and the use of proprietary software. Software is acquired from known and reputable sources to ensure copyright compliance
5.33	#Legal_and_compliance #Asset_management #Information_protection	Protection of records	Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release	YES	Risk Analysis	YES	Records are protected from loss, destruction, falsification, unauthorized access, and unauthorized distribution
5.34	#Information_protection #Legal_and_compliance	Privacy and protection of PII	The organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements	YES	Risk Analysis	YES	The General Data Protection Regulation has been applicable to the scope since May 25, 2018. As part of this, Cegid has appointed a DPO who is responsible for overseeing the subject transversally at the group level
5.35	#Information_security_assurance	Independent review of information security	The organization's approach to managing information security and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur	YES	Risk Analysis	YES	Cegid Cloud conducts an internal audit of the information system at least once a year. A Management review is planned afterward
5.36	#Legal_and_compliance #Information_security_assurance	Compliance with policies, rules and standards for information security	Compliance with the information security policy, specific thematic policies, organizational rules, and standards should be regularly verified	YES	Risk Analysis	YES	
5.37	#Asset_management #Physical_security #System_and_network_security #Application_security #Secure_configuration #Identity_and_access_management #Threat_and_vulnerability_management #Continuity #Information_security_event_management	Documented operating procedures	Operating procedures for information processing facilities should be documented and made available to personnel who need them	YES	Risk Analysis	YES	All operational procedures are documented and accessible to all Cegid Cloud employees in the GED (Electronic Document Management system)
People controls							
6.1	#Human_resource_security	Screening	Background verification checks on all candidates to become personnel should 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	Risk Analysis	YES	Background checks (information on CV, diplomas, criminal record, etc.) are conducted during the recruitment and onboarding of candidates
6.2	#Human_resource_security	Terms and conditions of employment	The employment contractual agreements should state the personnel's and the organization's responsibilities for information security	YES	Risk Analysis	YES	The employment contract signed by new employees includes a confidentiality clause and a non-compete clause
6.3	#Human_resource_security	Information security awareness, education and training	Personnel of the organization and relevant interested parties should 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	Risk Analysis	YES	Security training for new employees is systematically provided, and an annual awareness plan is developed and monitored
6.4	#Human_resource_security	Disciplinary process	A disciplinary process should be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation	YES	Risk Analysis	YES	A disciplinary process may be initiated in case of violation of the IT tools and equipment usage charter
6.5	#Human_resource_security #Asset_management	Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties	YES	Risk Analysis	YES	The employee is informed of their responsibilities in case of modification, breach, or termination of the contract by their HR contact
6.6	#Human_resource_security #Information_protection	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties	YES	Risk Analysis	YES	All Cegid personnel handling confidential data sign a confidentiality agreement with no time limit, involving disciplinary measures or legal action in case of non-compliance
6.7	#Asset_management #Information_protection #Physical_security #System_and_network_security	Remote working	Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises	YES	Risk Analysis	YES	Encryption of employee laptop disks, privacy filters, MFA, and VPN in mobile situations
6.8	#Information_security_event_management	Information security event reporting	The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner	YES	Risk Analysis	YES	Security incident management process (see Security Assurance Plan for more details)
Physical controls							
7.1	#Physical_security	Physical security perimeters	Security perimeters should be defined and used to protect areas that contain information and other associated assets	YES	Risk Analysis	YES	The operations and production teams are located in physically isolated premises
7.2	#Physical_security #Identity_and_access_management	Physical entry	Secure areas should be protected by appropriate entry controls and access points	YES	Risk Analysis	YES	Secure access with badges to the Production premises is restricted to authorized employees only
7.3	#Physical_security #Asset_management	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities should be designed and implemented	YES	Risk Analysis	YES	Doors are locked with an alarm in case of prolonged opening
7.4	#Physical_security	Physical security monitoring	Premises should be continuously monitored for unauthorized physical access	YES	Risk Analysis	YES	Cegid Cloud sites are continuously monitored
7.5	#Physical_security	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 should be designed and implemented	YES	Risk Analysis	YES	Protection of the building housing the production teams: power supply, air conditioning, network cabling, etc
7.6	#Physical_security	Working in secure areas	Security measures for working in secure areas should be designed and implemented	YES	Risk Analysis	YES	Protection of the building housing the production teams: power supply, air conditioning, network cabling, etc
7.7	#Physical_security	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced	YES	Risk Analysis	YES	Clean desk policy - Shredder available for documents, automatic session lock in case of prolonged inactivity
7.8	#Physical_security #Asset_management	Equipment siting and protection	Equipment should be sited securely and protected	YES	Risk Analysis	YES	Sensitive equipment is stored in secure premises
7.9	#Physical_security #Asset_management	Security of assets off-premises	Off-site assets should be protected	YES	Risk Analysis	YES	Disk encryption, Antivirus, secure remote connection via access gateway and/or VPN

7.10	#Physical_security #Asset_management	Storage media	Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements	YES	Risk Analysis	YES	Restriction on the use of removable media (USB) for employees. Datacenter (DC) supplier procedure for removable media storing client data. Physical destruction of storage media containing client data by hosting providers. Encryption of removable storage media in case of client data transfer. Tracking of receptions and shipments
7.11	#Physical_security	Supporting utilities	Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities	YES	Risk Analysis	YES	An independent power supply system is operational in case of general system failure
7.12	#Physical_security	Cabling security	Cables carrying power, data or supporting information services should be protected from interception, interference or damage	YES	Risk Analysis	YES	The local network of SaaS production is a switched network, physically independent from the rest of the company
7.13	#Physical_security #Asset_management	Equipment maintenance	Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information	YES	Risk Analysis	YES	Maintenance of internal equipment and employee devices is outsourced and contracted by the IT department
7.14	#Physical_security #Asset_management	Secure disposal or re-use of equipment	Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use	YES	Risk Analysis	YES	Destruction of media containing client data or related to this data (employee workstations)
Technological controls							
8.1	#Asset_management #Information_protection	User endpoint devices	Information stored on, processed by or accessible via user endpoint devices should be protected.	YES	Risk Analysis	YES	Encryption of employee laptop disks, privacy filters, MFA, and VPN in mobile situations
8.2	#Identity_and_access_management	Privileged access rights	The allocation and use of privileged access rights should be restricted and managed	YES	Risk Analysis	YES	Rights assignment by user group for applications to be used
8.3	#Identity_and_access_management	Information access restriction	Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control	YES	Risk Analysis	YES	The rights and access matrix defines access by business group and application
8.4	#Identity_and_access_management #Application_security #Secure_configuration	Access to source code	Read and write access to source code, development tools and software libraries should be appropriately managed	YES	Risk Analysis	YES	Scripts are stored in secure spaces accessible only to production teams
8.5	#Identity_and_access_management	Secure authentication	Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control	YES	Risk Analysis	YES	Cegid Cloud employees connect to production environments via a PAM and a secure remote access system (RDM)
8.6	#Continuity	Capacity management	The use of resources should be monitored and adjusted in line with current and expected capacity requirements	YES	Risk Analysis	YES	Continuous monitoring of resource allocation. Monthly committee on infrastructure and resource sizing
8.7	#System_and_network_security #Information_protection	Protection against malware	Protection against malware should be implemented and supported by appropriate user awareness	YES	Risk Analysis	YES	Centralized and administered antivirus/antimalware for all resources
8.8	#Threat_and_vulnerability_management	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken	YES	Risk Analysis	YES	Vulnerability management is conducted via a scanning tool and alerts raised by CERTs. Vulnerability treatment policy by perimeter in escalation mode. A policy of pentests and technical audits helps identify gaps
8.9	#Secure_configuration	Configuration management	Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed	YES	Risk Analysis	YES	Hardening of workstations and servers
8.10	#Information_protection #Legal_and_compliance	Information deletion	Information stored in information systems, devices or in any other storage media should be deleted when no longer required	YES	Risk Analysis	YES	Sensitive data (client data, logs) is deleted when no longer needed
8.11	#Information_protection	Data masking	Data masking should 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	Risk Analysis	YES	Cegid Cloud complies with applicable agreements, laws, and regulations concerning personal data.
8.12	#Information_protection	Data leakage prevention	Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information	YES	Risk Analysis	YES	Multiple actions and procedures prevent data leakage, such as internet access management, data classification, workstation hardening, and encryption
8.13	#Continuity	Information backup	Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup	YES	Risk Analysis	YES	The backup policy considers the specificity of each client offer. It takes into account availability, integrity, and retention
8.14	#Continuity #Asset_management	Redundancy of information processing facilities	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements	YES	Risk Analysis	YES	Redundancy and resilience mechanisms for architectures and teams are active end-to-end. There is constant supervision of these mechanisms
8.15	#Information_security_event_management	Logging	Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed	YES	Risk Analysis	YES	Information security events are centralized in a log concatenation tool governed by a well-defined policy. The log management tool is hosted in a secure architecture (redundancy, encryption of flows and disks, access management, backup). An automatic report of administrator and operator logs is produced monthly
8.16	#Information_security_event_management	Monitoring activities	Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents	YES	Risk Analysis	YES	Monitoring of servers, workstations, email inboxes, networks
8.17	#Information_security_event_management	Clock synchronization	The clocks of information processing systems used by the organization should be synchronized to approved time sources	YES	Risk Analysis	YES	An NTP synchronization is configured on all assets
8.18	#System_and_network_security #Secure_configuration #Application_security	Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled	YES	Risk Analysis	YES	A tool to manage and limit shadow IT is used to control the use of unauthorized programs and applications
8.19	#Secure_configuration #Application_security	Installation of software on operational systems	Procedures and measures should be implemented to securely manage software installation on operational systems	YES	Risk Analysis	YES	A tool and centralized console allow inventory management of operating software. Installation templates are used for virtual server configuration. IT charter
8.20	#System_and_network_security	Networks security	Networks and network devices should be secured, managed and controlled to protect information in systems and applications	YES	Risk Analysis	YES	Networks and links are monitored by surveillance tools. Accesses are traced and controlled
8.21	#System_and_network_security	Security of network services	Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored	YES	Risk Analysis	YES	An internal service agreement is contracted annually with the IT department, taking network security into account
8.22	#System_and_network_security	Segregation of networks	Groups of information services, users and information systems should be segregated in the organization's networks	YES	Risk Analysis	YES	Network segmentation through the implementation of DMZ and VLAN
8.23	#System_and_network_security	Web filtering	Access to external websites should be managed to reduce exposure to malicious content	YES	Risk Analysis	YES	Use of internet browsing filtering systems
8.24	#Secure_configuration	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented	YES	Risk Analysis	YES	Policy established on encryption of flows and data. This policy is regularly revised to offer the best security level in accordance with standardized best practices. Administration of certificates for HTTPS access in agreement with best practices, recognized certificate authority, key storage in a key vault. Management of encryption keys for data stored in data centers
8.25	#Application_security #System_and_network_security	Secure development life cycle	Rules for the secure development of software and systems should be established and applied	YES	Risk Analysis	YES	A policy describes and frames the security of development processes
8.26	#Application_security #System_and_network_security	Application security requirements	Information security requirements should be identified, specified and approved when developing or acquiring applications	YES	Risk Analysis	YES	Perimeter protection of access to public networks (Firewall, IDS/IPS probe). Encryption of flows by certificates from a recognized certification authority, keys are stored in a digital safe. Use of secure protocols ensuring complete transmission without possible modification of information and prohibiting unauthorized modification, disclosure, duplication
8.27	#Application_security #System_and_network_security	Secure system architecture and engineering principles	Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities	YES	Risk Analysis	YES	Scripts and automation are standardized and tested before being deployed to production
8.28	#Application_security #System_and_network_security	Secure coding	Secure coding principles should be applied to software development	YES	Risk Analysis	YES	Scripts and automation are standardized and tested before being deployed to production Secure coding best practices
8.29	#Application_security #Information_security_assurance #System_and_network_security	Security testing in development and acceptance	Security testing processes should be defined and implemented in the development life cycle	YES	Risk Analysis	YES	Testing phases and compliance tests are ensured in the AzureDevOps workflow
8.30	#System_and_network_security #Application_security #Supplier_relationships_security	Outsourced development	The organization should direct, monitor and review the activities related to outsourced system development	YES	Risk Analysis	YES	An internal service agreement with development BUs supervises and controls activities and applications external to the ISMS
8.31	#Application_security #System_and_network_security	Separation of development, test and production environments	Development, testing and production environments should be separated and secured	YES	Risk Analysis	YES	Segregation ensured by automated workflow in a DevOps organization
8.32	#Application_security #System_and_network_security	Change management	Changes to information processing facilities and information systems should be subject to change management procedures	YES	Risk Analysis	YES	Standard changes are operated via the platform orchestrator workflow. Non-standard changes are handled by the change process. Hardware and/or system updates are tested on pilot groups before application in production environments. All changes related to scripts and automation are recorded in a GIT repository.
8.33	#Information_protection	Test information	Test information should be appropriately selected, protected and managed	YES	Risk Analysis	YES	Managed by the AzureDevOps workflow and development servers
8.34	#System_and_network_security #Information_protection	Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management	YES	Risk Analysis	YES	Various policies (Scan) and agreements (Pentest) take into account business activity periods to minimize impacts