ID	Control		Testing Procedure	Interview	Document	Configuration	Observation
8.1	Information stored on, processed by or accessible via user endpoint devices should be protected.	General	**Secure endpoint management policy**	Interview responsible personnel to verify that secure endpoint management policy is known and applied	Analyse the secure endpoint management policy to verify that it includes procedures for: software versioning, restriction of software installation, network rules, access control, storage,anti-malware,backup,web services and apps, remote disabling, partitioning capabilities, removable devices, user analytics		
			List of user endpoint devices	Interview responsible personnel to verify how the list of endpoint devices is managed and how it is updated when devices are added, relocated or removed	Analyse the procedure for managing the list of endpoint devices and verify it requires to include their model, location and unique identifier		Select a sample of devices from the list of endpoint devices and cross check their model, location and unique identifier
		User responsibility	**Policy awareness**	Interview personnel involved in the use of endpoint devices to verify that they are aware of the topic-specific policy about endpoint devices	Analyse the topic-specific policy to verify what responsibilities the user should be aware of		
			Session termination	Interview a sample of users of endpoint devices to verify they terminate session when no longer needed		Review the configuration of a sample of endpoint devices or related systems to verify the presence of session termination timeouts	
			Endpoint devices lock	Interview a sample of users of endpoint devices to verify how they lock them when not in use		Review the configuration of a sample of endpoint devices to verify they include automatic device locking	
			Devices in public areas	Interview a sample of users of endpoint devices to verify how they pay attention to use them in public areas			
		Personal devices	**Separation of personal and business use in personal devices**		Analyse the secure endpoint management policy to identify if and how personal and business use are required be separated on personal devices	Review the configuration of a sample of personal devices to verify the isolation measures between personal and business environment	
			Software licensing agreement used on personal devices	Interview responsible personnel to verify which software license are agreed			Examine relevant license agreements to verify that the organization has software licensing that can be deployed on personal devices
		Wireless connections	**Wireless connections**	Interview responsible personnel to verify they configure wireless connections of endpoint devices according to the policy	Analyse the procedures for the configuration of wireless connections on devices to verify that secure protocols are required to be used	Review the configuration of a sample of endpoint devices to verify the compliance of the wireless configuration with the procedure	
8.2	The allocation and use of privileged access rights should be restricted and managed.		**Privileged user IDs assignation**	Interview responsible personnel to understand privileged user IDs assignation process and to verify that they are assigned only to roles that specifically require such privileged access being restricted to least privileges necessary to perform job responsibilities			Examine the process followed for assigning a sample of user IDs with privileged access to verify that privileges assigned are necessary and restricted for that individual's job function
			Authentication requirements	Interview responsible personnel to verify that authentication requirements for privileged user IDs assignation are higher than normal user IDs		Review the configuration of a sample of systems to verify the authentication requirements for privileged user IDs	
			Privileged user IDs expiry	Interview responsible personnel to understand privileged user IDs expiry process			Examine a sample of active and expired privileged user IDs to respectively verify their expiration date and their effective expiration.
			User awareness	Interview a sample of users with privileged access rights to verify they are aware of using privileged access only when necessary			

ID	Control		Testing Procedure	Interview	Document	Configuration	Observation
			Privileged users review	Interview responsible personnel to verify that privileges access rights are reviewed periodically and after major changes			Examine records of recent privileged users reviews and their outcomes
			Admin usage restriction	Interview responsible personnel to verify that specific rules are in place to avoid or track the use of generic administration user IDs depending on systems' configuration capabilities		Review the configuration of a sample of systems to verify that generic administration user IDs are disabled or tracked	
8.3	Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.		**Anonymous access**	Interview responsible personnel to verify that anonymous and guest users cannot access any non-public information		Review configuration settings for a sample of system to verify that anonymous and guest users are not allowed to have access to non-public information	
			Access control system			Review configuration settings for a sample of systems to verify that access control systems are active	Observe a sample of users logging in different systems to be required authentication
			Dynamic access management	Interview responsible personnel to identify adopted dynamic access management techniques		Review dynamic access management related configurations to protect information access	
8.4	Read and write access to source code, development tools and software libraries should be appropriately managed.		**Access control rules for source code and libraries**	Interview responsible personnel to verify that access to source code and libraries is controlled by rules based on personnel's role and using and development tools	Analyse the procedures for accessing program source code and libraries		Observe a sample of developers accessing source code repositories and libraries through development tools to be controlled by rules based on their role
			Source code management (versioning)		Analyse change controls procedures to verify that a secure procedure for source code modification is defined	Review source code management tools configuration to track all changes	Observe change histories to source code and libraries to verify their consistency
			Source code management (privileges)	Interview responsible personnel to verify how read and write access rights are managed		Review source code management tools configuration allow read and write access rights to personnel needing them only	
			Audit log			Review source code management tools configuration to log all accesses and changes to source code and libraries	Observe recent audit logs of accesses and changes to source code and libraries
			Integrity checks	Interview responsible personnel to verify how and when integrity checks are performed on source code			Observe source code integrity checks results
8.5	Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.		**Authentication policies distribution**	Interview responsible personnel to verify that authentication policies and procedures known to all users			
		User account	**Inactivity timeout**		Analyse the defined timeout policy parameters and related business needs	Inspect system configuration settings on a sample of systems, applications, devices and relevant network sessions to verify that the inactivity period value is consistently configured	
			Inactive account disabling		Analyse the relevant policy to verify the account inactivity period disabling and related business need	Inspect system configuration settings to verify that the number of days that define the inactivity period of accounts is set to 90 days or that no accounts with more than 90 days of inactivity are enabled	

ID	Control		Testing Procedure	Interview	Document	Configuration	Observation
			Lockout policy		Analyse the relevant policy to verify that accounts are locked out after a predefined number of wrong attempts for a defined time	Inspect configuration settings for a sample of systems to verify that the lockout option is configured consistently with the relevant policy	
			Third-party account management	Interview responsible personnel to verify how accounts used for remote access are enabled only when needed and disabled when not in use		Inspect configuration settings for a sample of systems with third-party accounts to verify they are enabled only when needed and disabled when not in use	
			Authentication factors	Interview responsible personnel to verify that a number of authentication factor proportional to the system's criticality and profile role is requested for all accesses		Review configuration settings for a sample of systems to verify that the expected number of different authentication factor is required	Observe personnel connecting to systems being required the expected number of different authentication factor
		Log-on procedure	**Log-on information disclosure**			Review system configurations to verify that system/application information are not sent and displayed until the user is successfully logged in	Observe information provided to personnel connecting to systems before and after log-on
			Log-on error messages			Review system configurations to verify that when inserted authentication information is wrong, no information about what is wrong is provided	Observe information provided to personnel connecting to systems after log-ons failing user ID and all used authentication factors
			Previous log-on attempts information			Review system configurations to verify that previous valid and invalid log-on attempts are recorded and displayed after successful log-on	Observe information provided to personnel connecting to systems including previous valid and invalid log-on attempts
8.6	The use of resources should be monitored and adjusted in line with current and expected capacity requirements.		**Capacity requirements identification**	Interview responsible personnel to verify how capacity is defined for each facility (physical and human resources) according to both functional and business requirements			
			Dynamic capacity evaluation	Interview responsible personnel to verify that ongoing monitoring is used to dynamically estimate the capacity to improve the availability and the efficiency of the systems			
			Stress-test	Interview responsible personnel to verify that verify that stress tests are planned to improve the availability and the efficiency of the systems	Review stress test procedures and related stress test planning		Review stress test records to verify their adherence to the procedure and the outcomes
			Capacity management plan	Interview responsible personnel to verify how capacity management plans are developed for mission critical systems	Analyse the documented capacity management plans for mission critical systems to verify their completeness		
8.7	Protection against malware should be implemented and supported by appropriate user awareness.		**White/blacklisting**	Interview responsible personnel to verify what white/blacklist policy is adopted		Review white/blacklisting configuration settings to be relevant and actual	
			Anti-malware tool deployment	Interview responsible personnel to verify what decisions have been made about systems commonly affected by malware		Review anti-malware configuration to verify that it actively protects all commonly affected systems	Compare the list of systems commonly affected by malware and the ones protected by anti-malware
			Anti-malware tool update	Interview responsible personnel to verify how the software is kept up to date		Review anti-malware configuration to verify that the software is automatically updated with a suitable frequency	Observe the last update of anti-malware definitions on a sample of systems

ID	Control		Testing Procedure	Interview	Document	Configuration	Observation
			Anti-malware disabling	Interview responsible personnel to verify that anti-malware software disabling is not allowed by unprivileged users		Review anti-malware configuration to ensure that its cannot be disabled by unprivileged users	
			Anti-malware scanning	Interview personnel to verify that runtime protections are enabled and periodic scans are performed		Review anti-malware configuration to verify that runtime protections are active and periodic scans are planned	Observe the last periodic scan execution report on a sample of systems
			Anti-malware logging	Interview personnel to verify that logging is performed and protected from unauthorized access		Review anti-malware configuration to verify that log information on malware related events is recorded and complete	Observe the presence, the protection and the completeness log entries generated from anti-malware tools
			Anti-malware messaging coverage	Interview personnel to verify what anti-malware messaging coverage is deployed		Review anti-malware configuration to ensure that scanning of email, attachments and downloads is performed before their use	
			Roles and responsibilities	Interview personnel to verify that security policies for protecting systems against malware are in use	Examine security policies for protecting systems against malware to verify that roles and responsibilities are clearly defined		
8.8	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.	Vulnerability identification	**Roles and responsibilities**	Interview responsible personnel to verify that roles and responsibilities for technical vulnerability management are assigned	Verify that roles and responsibilities are formally documented and assigned to competent personnel for each stage of vulnerability management		
			Information resources vulnerabilities	Interview responsible personnel to verify how the updated asset inventory list is used as input to identify information resources			Cross check asset inventory vendors and models with a sample of identified vulnerabilities to verify the coverage is complete
			Vulnerabilities and information systems suppliers		Verify that supplied information systems contracts require to disclose and report vulnerabilities.		
		Vulnerability disclosure	**Vulnerability disclosure policy**	Interview responsible personnel to verify that vulnerability disclosure policy is defined and distributed to all relevant parties	Analyse vulnerability disclosure policy to verify that it clearly defines procedures that specify to whom, how and when to report vulnerabilities		Review that reporting forms, threat intelligence, information sharing forums are properly used in the vulnerability disclosure process
		Vulnerability evaluation	**Report analysis**	Interview responsible personnel to verify how reports are analysed to identify which measures are necessary depending on the associated risks			Review that report analysis evidence effectively address discovered vulnerabilities
			Vulnerability response procedure		Analyse vulnerability response procedure to verify it includes: -priorities for fixing vulnerabilities -tests to confirm mitigation effectiveness -rescans to validate vulnerability absence		Review vulnerability response actions undertaken to respond to a sample of discovered vulnerabilities
			Change management and information security incident response compliance	Interview responsible personnel to verify that actions performed to fix vulnerabilities are compliant with change management and information security incident response procedures	Examine a sample for each risk level of the discovered vulnerability to verify that actions respect change management and information security incident response procedures		
		Patching	**Patch authenticity**	Interview responsible personnel to verify which are legitimate and trusted sources patches comes from and how are verified to be authentic			Observe how patch authenticity verification is performed
			Patch testing	Interview responsible personnel to verify that testing activities are performed before installing patches in production environments			Review patch testing results records to verify their performance

ID	Control		Testing Procedure	Interview	Document	Configuration	Observation
			Patch deployment	Interview responsible personnel to verify that patch deployment needs to be authorized and is performed on high-risk systems first			Review patch deployment authorization presence and installation on high-risk systems first
			Workarounds	Interview responsible personnel to verify what actions are undertaken when a patch cannot be applied or does not exist yet			Review workaround application cases effectiveness
8.9	Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.	Standard templates	**Configuration templates**	Interview responsible personnel to verify how templates have been defined and the authoritative sources that have been used.	Analyse configurations templates of hardware, software, services and network devices to verify they always include: 1) minimizing the number of identities with privileged or administrator level access rights; 2) disabling unnecessary, unused or insecure identities; 3) disabling or restricting unnecessary functions and services; 4) restricting access to powerful utility programs and host parameter settings; 5) synchronizing clocks; 6) changing vendor default authentication information immediately after installation and reviewing other important default security-related parameters; 7) invoking time-out facilities that automatically log off computing devices after a predetermined period of inactivity; 8) verifying that licence requirements have been met.	Review configurations of a sample of hardware, software, services and network devices to verify defined configuration templates have been implemented.	Cross reference configuration templates with asset inventory to ensure they cover all types of relevant assets.
			Configuration templates periodic review	Interview responsible personnel to verify that review of configuration templates is done periodically to keep them actual with respect to their sources.	Analyse a sample of configuration templates to verify that they have been reviewed to keep them actual with respect to their sources.		
		Configuration management	**Current configurations**	Interview responsible personnel to verify how all configurations currently established are properly recorded			Review a sample of configuration records and compare them to the actual status
			Configurations changes log	Interview responsible personnel to verify that configurations changes over time are properly recorded and retained			Review a sample of configuration records logs, verify they include: 1) up-to-date owner or point of contact information for the asset 2) date of the last change 3) version of the reference template 4) external references to other assets
			Configuration monitoring	Interview responsible personnel to verify how configurations are monitored		Review configuration monitoring tools configurations to verify they are set to be operating periodically covering all configurations	
8.10	Information stored in information systems, devices or in any other storage media should be deleted when no longer required.		**Deletion methods**	Interview responsible personnel to identify deletion methods in use according to classification of information			Observe the application of each deletion method to verify deleted files cannot be recovered
			Evidence	Interview responsible personnel to identify what kind of evidence of the successful deletion are collected (either internally or by a third party)			Review records of deletion activities to verify they are properly recorded and include indication of the employed method and deleted data

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
		Third-party agreements	Interview responsible personnel to identify if third parties include data storage and therefore must address information deletion with specific attention to cloud providers			Review third party agreements to be consistent with the organization defined deletion methods
		Deletion after retention	Interview responsible personnel to verify how information are deleted after their retention time has ended		Review system configurations enabling information deletion after their retention time has ended	Observe that information no longer in their retention period have been effectively deleted
		Secure deletion	Interview responsible personnel to verify which approved tools or certified disposal services are used to implement a secure deletion			
		Deletion of returning equipment	Interview responsible personnel to verify how secure deletion is performed on returning or to-be dismissed equipment			Observe secure deletion records performed on a sample of returned and to-be dismissed equipment
8.11	Data masking should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific, and business requirements, taking applicable legislation into consideration.	**Pseudonymization and anonymization**	Interview responsible personnel to verify if and how pseudonymization and anonymization techniques are adopted	Identify which elements of a sample of sensitive information are anonymized to verify the effectiveness		Observe a sample of pseudonymized or anonymized data to verify there is minimal risk of re-identification
		Data masking techniques	Interview responsible personnel to verify what data masking techniques are applied to what information			Observe a sample of masked data to verify masking is performed correctly and it is not reversible
		Selective data masking	Interview responsible personnel to verify if and how data are masked differently depending on users need-to-know			Observe masked data accesses performed by profiles with different need to know to verify the differences are coherent
8.12	Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.	**Data classification**	Interview responsible personnel to verify how and what data subject to potential leakage has been identified		Review data leakage prevention tool configuration and logs to verify that is set to protect identified information and is actively doing so	
		Channels monitoring	Interview responsible personnel to verify which channels expose identified data to potential leakage		Review data leakage prevention tool configuration to verify that each channel exposing identified data is properly monitored	
		Data leakage prevention actions			Review data leakage prevention tool configuration to verify how it monitors, notifies and blocks cases of data disclosure	Observe records of actions performed by the data leakage prevention tool to ensure it operates coherently with its configuration and that they are taken in consideration as potential incidents
8.13	Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	**Backup policy and plan definition**	Interview responsible personnel to verify that backup policy and plans are established and communicated to interested personnel	Analyse the backup policy and the backup plans to respectively verify they include data retention, business and information security requirements and how they will be implemented.		
		Restoration procedures		Verify that restoration procedures are documented and included in the backup policy for all types of backup		Observe records of restoration procedures performances to verify they are executed correctly and periodically
		Backup location and storage	Interview responsible personnel to verify where backups are stored and how they are protected		Review backup systems' configuration to verify data are effectively encrypted where required	Observe the location where backups are stored and verify it they are sufficiently apart from the primary site and offer similar protection levels
		Backup execution	Interview responsible personnel to verify their periodicity and to identify which operational procedures monitor backups execution		Review backup systems' configuration to verify it is consistent with backup policy and plans	Observe backup execution results to be effective and coherent with their planning
		Backup retention	Interview responsible personnel to verify defined backup retention		Review backup systems' configuration to verify it is consistent with established retention	Observe backup exceeding established retention to be securely deleted

ID	Control		Testing Procedure	Interview	Document	Configuration	Observation
8.14	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.		**Redundancy requirements**	Interview responsible personnel to identify which are the established redundancy requirements	Analyse redundancy procedures and project documents to verify redundancy architectures have been implemented accordingly to the identified requirements		
			Redundant components protection	interview responsible personnel to verify how redundant components protection is addressed	Verify that the security level of redundant components and information processing facilities requires to be equal to level of protection of original data		
			Critical services suppliers redundancy	Interview responsible personnel to verify that agreements with two or more suppliers of critical services are in place	Verify that contracts with several suppliers of critical services are established	Review system settings to verify that more than one critical service from different suppliers are ready to be used	
			Facilities redundancy	Interview responsible personnel to identify which facilities are duplicated and using what approach		Review system and network settings to verify that duplicated facilities can be timely activated as planned	Observe asset inventories and network architectures of the duplicated facilities to very they cover all needed assets
			Redundant systems and networks	Interview responsible personnel to identify which systems and networks are duplicated		Review system and network configurations to verify that more than one instance of system components is in place and correctly configured as a redundancy	
8.15	Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.		**Logging policy definition**	Interview responsible personnel to verify that a policy on logging is established and distributed to all interested parties	Analyse the logging policy to verify that the following aspects are identified: -requirements for handling log data -collected and logged data -purpose of logging		
			Information to be logged		Analyse logging policy to verify they require logging a set of information consistent with applicable requirements, including: 1) user IDs; 2) system activities; 3) dates, times and details of relevant events; 4) device identity, system identifier and location; 5) network addresses and protocols.	Review a sample of systems and applications configurations to verify they are set to log all the information specified within the logging policy.	Observe the production of log events consistently with the system's and application's configuration
			Events to be logged		Analyse logging policy to verify they require logging a set of events consistent with applicable requirements, including: 1) successful and rejected system access attempts; 2) successful and rejected data and other resource access attempts; 3) changes to system configuration; 4) use of privileges; 5) use of utility programs and applications; 6) files accessed and the type of access, including deletion of important data files; 7) alarms raised by the access control system; 8) activation and de-activation of security systems; 9) creation, modification or deletion of identities; 10) transactions executed by users in applications.	Review a sample of systems and applications configurations to verify they are set to log all the events specified within the logging policy.	Observe the production of log events consistently with the system's and application's configuration
		Protection of logs	**Unauthorized log change protection**			Review a sample of log files settings to verify that users aren't allowed to delete or modify logs and, if they are, those activities are recorded elsewhere	

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
		Log integrity protection			Review integrity protection mechanisms settings to ensure they operate properly and can't be circumvented	Observe the production of logs and related integrity protection measures to be operating consistently with their configuration
		Log retention		Analyse the logging policy to verify for how much time logs have to be retained.		Observe log repositories and verify that log retention time is respected and secure deletion is performed thereinafter.
		Log analysis	Interview responsible personnel to verify how log analysis is performed, how frequently, by what competent personnel and which monitoring activities support the analysis	Analyse the procedures adopted to analyse logs and verify they include: -definition of anomalous behaviours and exceptions -threat intelligence -pattern analysis -monitoring activities support		Observe a sample of log analysis records to verify they are coherent with the procedures, they are periodically executed and that produced reports can be used for incident management purposes.
8.16	Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	**Elements to be monitored**			Review monitoring tools configuration to verify they include: 1) outbound and inbound network, system and application traffic; 2) access to systems, servers, networking equipment, monitoring system, critical applications, etc. 3) critical or admin level system and network configuration files; 4) logs from security tools; 5) event logs relating to system and network activity; 6) checking that the code being executed is authorized to run in the system and that it has not been tampered with; 7) use of the resources and their performance	Observe a sample of monitoring records to verify that monitoring tool configurations are performing as expected.
		Baseline behavior			Review the monitoring tools configuration to verify that system monitoring is set to detect anomalous behaviour defined against the normal one including: 1) unplanned termination of processes or applications; 2) activity typically associated with malware or traffic originating from known malicious IP addresses or network domains; 3) known attack characteristics; 4) unusual system behaviour; 5) bottlenecks and overloads; 6) unauthorized access (actual or attempted) to systems or information; 7) unauthorized scanning of business applications, systems and networks; 8) successful and unsuccessful attempts to access protected resources; 9) unusual user and system behaviour in relation to expected behaviour.	Observe a sample of monitoring records to verify that anomalous behaviours are detected and how baselines are defined and actualized.
		Third-party account monitoring			Inspect system configuration settings for a sample of components to verify that third-party account activities are monitored	Observe third-party remote access accounts monitoring results

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
		Alerts generation			Review monitoring tools configurations to verify they are set to generated alerts whenever anomalous behaviours are detected and thresholds are exceeded	Observe received alerts from the monitoring tools to verify they are sent and received consistently with their settings
8.17	The clocks of information processing systems used by the organization should be synchronized to approved time sources.	**Reference clock**	Interview responsible personnel to identify which external time sources are used as reference clock		Verify that the configured reference clocks for time synchronization are the intended atomic clocks	
		Clock synchronization			Verify that all systems are configured to ultimately be synchronized with the reference clock through the use of appropriate time protocols	Observe system timestamps to verify they are correct
8.18	The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.	**Authorized users**			Review system configurations to verify that utility programs are usable by authorized personnel only	Review utility programs authorized users and verify their effective need to use them
		Utility programs limitation			Review utility programs settings to verify they are disabled if their use is not deemed necessary	Observe the list of installed utility programs and verify their effective need
8.19	Procedures and measures should be implemented to securely manage software installation on operational systems.	**Allowed software installation**			Review systems configuration to verify that the installation of software is restricted to authorized and competent users only	Observe changes recently implemented on a sample of systems and verify that the personnel which implemented them was duly authorized
		Supported software				Observe that employed versions of vendor supplied software are still under support
		Configuration control			Review configuration control system configuration to verify it controls all operational software and system documentation	Observe configuration control system records to verify it is used for tracking all modifications
8.20	Networks and network devices should be secured, managed and controlled to protect information in systems and applications.	**Network diagrams**		Analyse network diagrams to verify they are current and complete	Review network device configuration files to verify network diagrams are correct	
		Authentication systems			Review network device configurations to verify authentication is required	Observe authentication attempts performed on network devices to verify it is required
		Hardening		Analyse network device hardening documentation to verify it is actual, covers all network devices models and mandates disabling of vulnerable network protocols	Review network device configurations to verify security hardening measures are consistently applied	
		Network filtering and restriction		Analyse network diagrams to verify network filtering devices are deployed on the boundaries of the network	Review network device configurations to verify network filtering devices are configured to restrict and filter inbound and outbound traffic	
		Separate network for the administrator			Review network devices configurations to verify dedicated networks or channels are defined for administration purposes and are segregated from the others	Observe networks used by the administrators to verify they have a separate address range from other networks and they use a dedicated channel
8.21	Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.	**Allowed networks and services**	Interview responsible personnel to identify which network and network services are allowed and under which authentication requirements		Review firewall rules to verify that only allowed network and services have allowed network traffic	Observe accesses to a sample of network and network services and verify their authentication requirements implementation
		Security features			Review a sample of network devices configurations to verify that strong encryption is configured to be used and other along with other network access control methods.	Observe accesses to a sample of network and network services and verify the invocation of strong encryption and other network access control methods

ID	Control		Testing Procedure	Interview	Document	Configuration	Observation
8.22	Groups of information services, users and information systems should be segregated in the organization's networks.		**Network separation criteria**	Interview responsible personnel to verify that criteria used to define and divide the organization network into separate sub-domains include: 1) business needs and security requirements 2) levels of trust 3) criticality and sensitivity	Review the network schemes to verify the criteria used to define and divide the organization network into separate sub-domains have been correctly applied	Review a sample on network devices configuration to verify the documented segregation is effective	
			Wireless networks		Review the network schemes to verify the presence of wireless networks and their segregation from other networks	Review a sample on network devices configuration to verify the documented segregation for wireless networks is effective	
8.23	Access to external websites should be managed to reduce exposure to malicious content.		**Malicious website access**			Review website blocking technology settings to verify that, for a specified set of profiles, they are configured to block connections to: 1) websites that have an information upload function 2) known or suspected malicious websites 3) command and control servers 4) malicious website acquired from threat intelligence 5) websites sharing illegal content are included	Observe that attempted connections to websites classified as malicious are denied for a sample of profiles
			Use of online resources	Interview responsible personnel to identify rules for appropriate use of online resources and verify they are distributed throughout the organization	Analyse distributed rules for appropriate use of online resources and verify they are complete, up-to-date and include indications not to overrule any blocking		
8.24	Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.		**Cryptography policy definition**	Interview responsible personnel to verify that topic-specific policy on cryptography is established, communicated to interested parties and that related roles and responsibilities are allocated	Analyse the policy on cryptography to verify that it includes general principles for protection of information, use of cryptography roles and responsibilities and details of all approved algorithms, protocols and keys and key strength	Review a sample of cryptography-using systems configurations to verify they are aligned with approved algorithms, protocols and keys and key strength	
			Standards and usage practices compliance with regulations		Analyse the policy on cryptography to verify that approved standards, cryptographic algorithms, solutions and usage practices respect regulations and national restrictions such as: 1) restrictions on import or export of computer hardware and software for performing cryptographic functions or designed to have cryptographic functions added to it 2) restrictions on the usage of cryptography 3) mandatory or discretionary methods of access by the countries' authorities to encrypted information 4) validity of digital signatures, seals and certificates		
		Key management	**Key management procedures**		Analyse procedures for key management to verify they include secure methods for: 1) key generation 2) key distribution 3) key storage 4) key replacement or retirement 5) key destruction		Review key management logs to verify the documented procedures are followed for: 1) key generation 2) key distribution 3) key storage 4) key replacement or retirement 5) key destruction

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
		Key management logging	Interview key management responsible personnel to verify how key management logs are produced and stored.			Review key management logs to verify they are produced for every key management related activity, are complete and are retained for a consistent amount of time.
		Compromised key	Interview responsible personnel to verify that keys are replaced as soon as they are suspected to be compromised			Review key management logs to verify suspected compromised keys have been changed
		Cryptoperiods	Interview responsible personnel to verify that cryptoperiods are defined for all keys based on risk considerations			Review key inventories to verify consistent cryptoperiods are defined for all keys
8.25	Rules for the secure development of software and systems should be established and applied.	**Secure development coverage**	Interview responsible personnel to verify that rules for secure development of software are established and communicated to interested parties	Analyse rules for secure development of software to verify they cover: 1) separation of development, test and production environments 2) guidance on the security in the software development life cycle 3) security requirements in the specification and design phase 4) security checkpoints in projects 5) system and security testing, such as regression testing, code scan and penetration tests 6) secure repositories for source code and configuration 7) security in the version control 8) required application security knowledge and training 9) developers' capability for preventing, finding and fixing vulnerabilities 10) licensing requirements and alternatives to ensure cost-effective solutions 11) assurance that the used suppliers conform with the organization's rules for secure development		Observe developers' environments to verify how secure software development is implemented following the established rules.

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
8.26	Information security requirements should be identified, specified and approved when developing or acquiring applications.	**Application security requirements identification**	Interview responsible personnel to verify that application security requirements are identified and how information security specialists are involved in their identification			Review documented application security requirements to verify they include as applicable: 1) level of trust in identity of entities 2) identifying the type of information and classification level to be processed by the application 3) need for segregation of access and level of access to data and functions in the application 4) resilience against malicious attacks or unintentional disruptions 5) legislation, regulations and statutory requirements in the jurisdiction where the transaction is generated, processed, completed or stored 6) need for privacy associated with all parties involved 7) the protection requirements of any confidential information 8) protection of data while being processed, in transit and at rest 9) need to securely encrypt communications between all involved parties 10) input controls, including integrity checks and input validation 11) automated controls 12) output controls, also considering who can access outputs and its authorization 13) restrictions around content of "free-text" fields, as these can lead to uncontrolled storage of confidential data 14) requirements derived from the business process, such as transaction logging and monitoring, nonrepudiation requirements 15) requirements mandated by other security controls 16) error message handling
		Application security requirements for transactional services				Review documented application security requirements for transactional services to verify they include as applicable: 1) the level of trust each party requires in each other's claimed identity 2) the level of trust required in the integrity of information exchanged or processed and the mechanisms for identification of lack of integrity 3) authorization processes associated with who can approve contents of, issue or sign key transactional documents 4) confidentiality, integrity, proof of dispatch and receipt of key documents and the non-repudiation 5) the confidentiality and integrity of any transactions 6) requirements on how long to maintain the transaction confidential 7) insurance and other contractual requirements

ID	Control		Testing Procedure	Interview	Document	Configuration	Observation
			Application security requirements for applications involving electronic ordering and payment				Review documented application security requirements for applications involving electronic ordering and payment to verify they include as applicable: 1) requirements for maintaining the confidentiality and integrity of order information 2) the degree of verification appropriate to verify payment information supplied by a customer 3) avoidance of loss or duplication of transaction information 4) storing transaction details outside of any publicly accessible environment 5) where a trusted authority is used, security is integrated and embedded throughout the entire end-to-end certificate or signature management process
8.27	Principles for engineering secure systems to be established, documented, maintained and applied to any information system development activities.		**Security engineering principles definition**	Interview responsible personnel to verify how secure system engineering principles are established and applied to information system engineering activities	Analyse established security engineering principles to verify they include the analysis of: 1) the full range of security controls required to protect information and systems against identified threats 2) the capabilities of security controls to prevent, detect or respond to security events 3) specific security controls required by particular business processes 4) where and how security controls are to be applied 5) how individual security controls (manual and automated) work together to produce an integrated set of controls		Observe information system engineering activities to verify that established secure system engineering principles are consistently applied
			Integration of architectural, infrastructural and technological requirements		Analyse established security engineering principles to verify they address considerations coming from: 1) the integration with security architecture 2) technical security infrastructure 3) chosen technology 4) cost, time and complexity of meeting security requirements 5) good practices		
			Security-oriented design review	Interview responsible personnel to verify that security-oriented design reviews are regularly performed			Review security-oriented design reviews results to verify they are performed periodically and they help identifying information security vulnerabilities and ensuring security controls are specified meeting security requirements
8.28	Secure coding principles should be applied to software development.		**Secure coding governance**	Interview responsible personnel to verify how organization-wide processes are established and regularly reviewed to provide up-to-date governance for secure coding			Observe the practical application of the established secure coding baseline on a sample of actual development projects
		Planning and before coding	**Training on secure coding**	Interview developers to verify they are competent in secure coding techniques and have undergone periodical trainings			Review records of training to verify that software developers receive up-to-date training on secure coding techniques periodically, including how to avoid common coding vulnerabilities

ID	Control		Testing Procedure	Interview	Document	Configuration	Observation
			Secure design and architecture	Interview responsible personnel to verify how secure design and architecture, including threat modelling, is properly performed			Review secure design and architecture related records, including threat modelling, to verify they are properly considered before coding
			Secure coding guidelines	Interview responsible personnel to verify what secure coding practices and techniques are used and documented	Analyse adopted secure coding practices to verify they are adequate to the programming languages and techniques being used		Review records generated by the application of secure coding practices and techniques to verify they are consistent
		Review and maintenance	**Code maintenance**	Interview responsible personnel to verify that after code has been made operational: 1) updates are securely packaged and deployed 2) reported vulnerabilities are handled 3) errors and suspected attacks are logged 4) external libraries are managed and updated			Review a sample of projects to verify they include where applicable: 1) updates of securely packaged and deployed 2) handled reported vulnerabilities 3) logged errors and suspected attacks 4) managed and updated external libraries
8.29	Security testing processes should be defined and implemented in the development life cycle.		**Test coverage**	Interview responsible personnel to verify that software security testing processes include: 1) security functions 2) secure coding 3)secure configurations			Review a sample of software security testing activities results to verify that they always include: 1) security functions 2) secure coding 3)secure configurations
			Test plans	Interview responsible personnel to identify how software security testing is planned and verify that the effort is proportional to the importance of the system			Review a sample of development projects to verify they are always include a software security test plan with: 1) detailed schedule of activities and security test 2) inputs and expected outputs under a range of conditions 3) criteria to evaluate the results 4) decision for further actions as necessary
			Test independence	Interview responsible personnel to identify what tools are used for software security testing and who is going to use them			Review a sample of development projects to verify the appropriateness of the employed tools and the independence of the software security testers from the development team.
			Test types	Interview responsible personnel to identify whether all of the following type of tests are performed: 1) code reviews 2) vulnerability assessment 3) penetration tests			Review a sample of development projects to verify that they always include: 1) code reviews 2) vulnerability assessment 3) penetration tests
			Test environments	Interview responsible personnel to verify that testing is performed within multiple test environments that always reflect the target deployment/operating environments			Observe test environments where tests are performed to verify they always reflect the target deployment/operating environments

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
8.30	The organization should direct, monitor and review the activities related to outsourced system development.	**requirements and expectations definition**	Interview responsible personnel to verify what outsourced system development activities are performed			Review agreements with outsourced system developers to verify they include: 1) secure design, coding, testing 2) acceptance testing 3) development environment specifications 4) compliance with applicable legislation 5) right to audit development processes and controls 6) requirements to provide to the organization evidence of minimum acceptable levels of security and privacy in place 7) requirements to provide to the organization evidence of sufficient testing against the presence of malicious content and known vulnerabilities
8.31	Development, testing and production environments should be separated and secured.	**Development and production domains separation**	Interview responsible personnel to verify how development, test and production environments are separate		Review development, test and production environments configuration settings enforcing their separation	Observe that separated environments are used for development, test and production
		Authorized software deployment		Analyse rules and authorization procedures for the deployment of software from development to production environment and verify they include testing in a separate testing environment		Review deployment evidences to verify that rules and authorization for the deployment of software into production environment are followed
		Environments security controls			Review developing and testing environments configuration settings to verify they are subject to: 1) patching and updating 2) secure configuration 3) access control 4) change control 5) security monitoring 6) backup	Observe evidence of the following activities on developing and testing environments: 1) patching and updating 2) secure configuration 3) access control 4) change control 5) security monitoring 6) backup
8.32	Changes to information processing facilities and information systems should be subject to change management procedures.	**Change control procedures**	Interview responsible personnel to verify that change control procedures are communicated to all interested parties and they are modified as needed	Analyse ICT and software change control procedures to verify they include: 1) evaluation of the impact of changes before authorizing them 2) communicating changes to relevant interested parties 3) tests and acceptance of tests for the changes 4) deployment plans of implemented changes 5) fall-back procedures 6) recording of changes 7) continuity, response and recovery plans 8) operating documentation		Review a sample of ICT and software change records to verify they always include coherent information about: 1) evaluation of the impact of changes before authorizing them 2) communicating changes to relevant interested parties 3) tests and acceptance of tests for the changes 4) deployment plans of implemented changes 5) fall-back procedures 6) continuity, response and recovery plans 7) operating documentation
8.33	Test information should be appropriately selected, protected and managed.	**Test information selection**	Interview responsible personnel to verify how test information is selected to ensure: 1) reliability of tests results 2) not leaking confidential or sensitive data			Observe a sample of test information to verify that: 1) the volume of data used for testing is substantial 2) sensitive data is properly masked when used for testing

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
		Test information protection	Interview responsible personnel to verify how test information is protected		Review the configuration of the environment where test information is used to verify that: 1) the same production access control procedures are applied 2) authorization for production data copy is provided 3) test information copy and use audit trail are enabled 4) secure deletion procedures are in place	
8.34	Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management.	**Audit requests management**	Interview responsible personnel to verify how audit requests and their scope are agreed			Review a sample of audit requests approved requests and scope to verify they have been properly agreed
		Audit rights	Interview responsible personnel to verify that audit activities are performed in read-only access by the auditor or by an administrator who has the necessary access rights on behalf of the auditor, keeping adequate audit trails		Review auditor profile's privileges to verify that the auditor has read-only access rights to software and data and is configured to generate audit trails	
		Audit scheduling	Interview responsible personnel to verify how audit tests that can affect system availability are scheduled			Review a sample of audit tests records to verify audit tests that can affect system availability have been scheduled outside business or peak hours