ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
5.1	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.	**Information security policies communication**	Interview responsible personnel for the publication and distribution of information security policies and verify the employed means			Verify the distribution means used for the information security policies both to internal personnel and to third parties
		Information security policies approval	Interview top management to verify how it is committed to information security	Analyse information security policies to verify the presence of top management's approval		
		Information security policy maintenance	Interview responsible personnel to verify that the policies are updated periodically and according to significant changes	Analyse the most recent information security policies' update and cross-reference them with occurred significant changes		
		Topic-specific policies		Analyse specific policies to verify the exhaustive coverage of each exemplified topic		
		Information security policies acknowledgement	Interview a sample of personnel to verify how they acknowledged information security policies			Review acknowledgement records to verify the extension and the frequency of acknowledges given to information security policies
		Policy awareness	Interview a sample of personnel to verify they understand the security policies			Examine training records to evaluate the coverage of the reached information security policies awareness
5.2	Information security roles and responsibilities should be defined and allocated according to the organization needs.	**Roles and responsibilities definition**	Interview top management to understand how information security responsibilities are defined and attributed	Verify that information security policies, organization charts and function charts clearly define information security responsibilities for: 1) protection of information and associate assets 2) carrying out information security processes 3) information security risk management activities 4) all personnel		Review relevant information security formal roles attribution letters to verify they are accurate and current
5.3	Conflicting duties and areas of responsibility should be segregated.	**Conflicting duties definition**	Interview relevant personnel to verify that conflicting duties have been detected, with specific regards to: 1) change management 2) access right requests 3) software development and deployment 4) auditing activities	Verify organization charts to identify conflicting duties		
		Activities with required segregation	Interview relevant personnel performing conflicting duties to verify their awareness of segregation measures	Verify function charts and related segregation of duties measures		Observe a sample of conflicting activities or their records to verify that segregation of duties is effectively in place
		Collusion management	Interview relevant personnel to verify how possible collusion is managed	Analyse anti-collusion policies		
5.4	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.	**Information security policies distribution**	Interview management personnel to identify how they ensure personnel is informed about information security policies			

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
		Information security roles and responsibilities	Interview management personnel to identify how they ensure personnel is informed about their information security role and responsibilities			
		Information security in contracts	Interview management personnel to identify how they ensure conformity to information security considerations in contracts			
		Whistleblowing	Interview management personnel to identify how they ensure the presence of a confidential channel for reporting violations on information security topics			Observe records of reported violations on information security topics
		Resources	Interview management personnel to identify how they ensure that adequate resources are destined to information security activities			Observe plans and budgets for information security to evaluate their coherence
5.5	The organization should establish and maintain contact with relevant authorities.	**List of authorities (how)**	Interview relevant personnel to get the list of relevant authorities and identify how security information is provided to them	Analyse the established procedures to contact each authority and verify their compliance to applicable regulations		Observe the list of contacts practically used to get in touch with all authorities and a sample of related communications
5.6	The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations.	**Groups and associations**	Interview relevant personnel to verify what special interest groups the organization has contacts with			Observe the list of contacts practically used to get in touch with all special interest groups and a sample of related communications
5.7	Information relating to information security threats should be collected and analysed to produce threat intelligence.	**Threat intelligence sources**	Interview relevant personnel to identify employed threat intelligence sources			Observe a sample of collected threat intelligence information to verify they are relevant, insightful, contextual, actionable
		Threat intelligence analysis	Interview relevant personnel to verify how threat intelligence information are evaluated and integrated into the organization security process			Observe a sample of actions arising from threat intelligence analysis results
5.8	Information security should be integrated into project management.	**Information security risks**	Interview responsible personnel to verify how information security risks are part of the project risks from the early stages and are object of treatment and review.			Observe project risks assessment to verify that information security risks have been included from their early stages and adequately treated and reviewed.
		Information security requirements definition	Interview responsible personnel to verify how information security requirements have been derived for the project.			Observe that project information security requirements have been derived by: 1) information security or topic-specific policies 2) threat modelling 3) incidents reviews 4) vulnerability thresholds 5) contingency planning
		Information security requirements consideration	Interview responsible personnel to verify what information security requirements have been taking into consideration within the project.			Observe that project information security requirements have been considering: 1) involved information and required protection 2) level of assurance required for authentication 3) access provisioning and authorization processes 4) user information on duties and responsibilities 5) business processes inputs 6) mandates by other controls 7) legal, statutory, regulatory and contractual environment 8) level of assurance required to third parties

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
5.9	An inventory of information and other associated assets, including owners, should be developed and maintained.	**Inventories coverage**	Interview responsible personnel to verify how inventories cover all information classified and their associated assets			Review all inventories and cross reference them with data flows, network diagrams and other scanning activities to verify that they cover all information and associated assets
		Inventory accuracy	Interview responsible personnel to verify what relevant information are recorded in the inventories along with information and associated assets			Review all inventories to verify they include relevant information for all entries including location, classification and owner individual or group.
		Inventory update	Interview responsible personnel to verify how inventories are kept up-to-date and reviewed.			Review all inventories to verify their latest performed review and that they are aligned with recents changes regarding information associated assets
		Asset management	Interview a sample of assets owners to verify that they understand and carry out their responsibilities for: inventory, classification, protection, periodic revisions, usage, risk management, support.			Observe how sampled asset owners formally take in charge their responsibilities as such
5.10	Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented.	**Acceptable use policy**	Interview responsible personnel to verify that topic-specific policy on the acceptable use of information and other associated assets is established and communicated to anyone who uses or handles information	Analyse the acceptable use policy to verify that rules and procedures for the acceptable use and procedures for handling information and other associated assets are documented, including: 1) expected and unacceptable behaviours of individuals from information security perspective 2) permitted and prohibited use of information and other associated assets 3) monitoring activities		
		Acceptable use procedures	Interview responsible personnel to verify that acceptable use procedures are drawn covering the full information lifecycle and are communicated to anyone who uses or handles information	Analyse documented procedures and verify they include: 1) access restrictions supporting the protection requirements for each level of classification 2) maintenance of a record of the authorized users 3) protection of temporary or permanent copies of information to a level consistent with the protection of the original information and marking them 4) storage of assets in accordance with manufacturer's specifications 5) authorization of disposal of information and supported methods		
		Third-party assets	Interview responsible personnel to verify that agreements with service providers are established and third-party assets are clearly identified	Review agreements with cloud service providers to verify that third-party assets are considered for protection		
		user awareness	Interview users to verify that users are aware of topic-specific policy on the acceptable use of information and other associated assets			
5.11	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.	**Asset return formalization**	Interview responsible personnel to verify how the termination process has been formalized to include the return of all assigned assets	Analyse relevant policies and procedures to verify that the return of all assigned assets upon termination is formalized		

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
		Information deletion	Interview responsible personnel to verify how information deletion is performed on returned assets or personal assets being used by terminated personnel	Analyse relevant procedures to verify how information deletion is required to be performed on returned assets or personal assets being used by terminated personnel		
		Knowledge return	Interview responsible personnel to verify how knowledge of terminated personnel is transferred back to the organization			Review documented information about returned knowledge from terminated personnel
		Prevent unauthorized copies	Interview responsible personnel to verify how unauthorized copies are prevented during the notice period and after termination			Review measures in place to prevent unauthorized copies during the notice period and after termination
		Returned assets	Interview responsible personnel to verify how all assets to be returned are identified including: 1) user endpoint devices 2) personal devices (and portable storage devices) 3) special equipment 4) authentication hardware 5) physical copies of information			Review asset return records to match asset return lists
5.12	Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements	**Information classification policy**	Interview responsible personnel to verify that a topic-specific policy on information classification is established and communicated to all relevant interested parties	Analyse the information classification policy to verify that a scheme for the classification of information including confidentiality, integrity and availability requirements and resulting impacts is defined		
		Access control and business requirements alignment	Interview responsible personnel to verify how information classification is aligned with access control policies and with business requirements	Analyse the access control policy and verify its alignment with the information classification policy and with business requirements		
		Consistency across organization procedures	Interview responsible personnel to verify that the information classification scheme is established and included in organization procedures	Analyse information classification procedures to verify they allow a consistent application of information classification across the organization		
		Interoperability with other organization's schemes	Interview responsible personnel to verify that agreements with other organizations include a way to interpret different classification schemes			Review agreements with other organizations to verify they include procedures to identify the classification of information and to interpret the classification levels from other organizations
		Review of information classification scheme	Interview responsible personnel to verify how information classification is required to be reviewed over time accordingly to change in terms of value, sensitivity or criticality	Analyse the information classification policy to verify that information classification is required to be reviewed over time accordingly to change in terms of value, sensitivity or criticality		
5.13	An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.	**Labelling procedures definition**	Interview responsible personnel to verify that labelling procedures are in place and are distributed to all personnel	Analyse labelling procedures to verify that they cover information and other associated assets in all formats, coherently with the established information classification scheme.		
		Labels application	Interview responsible personnel to verify they know: 1) how to label information, depending on the format 2) how to handle impossible labelling 3) when labelling can be omitted			Review a sample of classification labels to verify that they are: 1) coherent with the classification scheme 2) clear and easily recognizable 3) applied to the appropriate information assets in the appropriate place(s)

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
		Metadata	Interview responsible personnel to verify that labelling procedures include: 1) how to attach metadata to information 2) what labels to use 3) how data are handled	Analyse labelling procedures to verify that they include descriptions on how to attach metadata to information and what metadata to attach.		
		Metadata application	Interview responsible personnel to verify they know how to apply metadata and what metadata to apply to information			Review a sample of metadata to verify that they: 1) are coherent with the classification scheme 2) are applied to the appropriate information assets in the appropriate way 3) include metadata used by systems to process information depending on their information security properties
5.14	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.	**Information transfer policy definition**	Interview responsible personnel to verify that a topic-specific policy on information transfer is established and communicated to all interested parties	Analyse the information transfer policy to verify that information transfer is documented and established through rules, procedures and agreements		
		General information transfer agreements		Analyse information transfer documented rules and procedures to verify they include: 1) controls designed to protect transferred information and to ensure traceability and non-repudiation 2) identification of appropriate contacts related to the transfer 3) responsibilities and liabilities in the event of information security incidents 4) use of an agreed labelling system for sensitive or critical information 5) retention and disposal guidelines for all business records		Review a sample of information transfer agreements to verify they include: 1) controls designed to protect transferred information and to ensure traceability and non-repudiation 2) identification of appropriate contacts related to the transfer 3) responsibilities and liabilities in the event of information security incidents 4) use of an agreed labelling system for sensitive or critical information 5) retention and disposal guidelines for all business records
		Electronic information transfer agreements		Analyse electronic information transfer documented rules and procedures to verify they additionally include: 1) detection of and protection against malware that can be transmitted 2) protection of attachments 3) prevention against sending information to wrong recipients 4) obtaining approval prior to using external public services 5) stronger levels of authentication when using publicly accessible networks 6) restrictions associated with electronic communication facilities 7) advising personnel and other interested parties not to send SMS or instant messages with critical information 8) advising personnel and other interested parties about the problems of using fax machines or services		Review a sample of electronic information transfer agreements to verify they include: 1) detection of and protection against malware that can be transmitted 2) protection of attachments 3) prevention against sending information to wrong recipients 4) obtaining approval prior to using external public services 5) stronger levels of authentication when using publicly accessible networks 6) restrictions associated with electronic communication facilities 7) advising personnel and other interested parties not to send SMS or instant messages with critical information 8) advising personnel and other interested parties about the problems of using fax machines or services

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
		Physical information transfer agreements		Analyse physical information transfer documented rules and procedures to verify they additionally include: 1) responsibilities for controlling and notifying transmission, dispatch and receipt 2) ensuring correct addressing and transportation of the message 3) packaging protecting the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications 4) a list of authorized reliable couriers agreed by management and courier identification standards 5) tamper evident or tamper-resistant controls 6) procedures to verify the identification of couriers 7) approved list of third parties providing transportation 8) keeping logs for identifying the content of the storage media, the protection applied as well as recording the list of authorized recipients, the times of transfer to the transit custodians and receipt at the destination		Review a sample of physical information transfer agreements to verify they include: 1) responsibilities for controlling and notifying transmission, dispatch and receipt 2) ensuring correct addressing and transportation of the message 3) packaging protecting the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications 4) a list of authorized reliable couriers agreed by management and courier identification standards 5) tamper evident or tamper-resistant controls 6) procedures to verify the identification of couriers 7) approved list of third parties providing transportation 8) keeping logs for identifying the content of the storage media, the protection applied as well as recording the list of authorized recipients, the times of transfer to the transit custodians and receipt at the destination
		Verbal transfer awareness	Interview sample personnel to verify that they are aware they should: 1) not have confidential verbal conversations in public places or over insecure communication channels 2) not leave messages containing confidential information 3) begin any sensitive conversations with a disclaimer			Review verbal transfer security awareness initiatives records to verify they include indications: 1) not have confidential verbal conversations in public places or over insecure communication channels 2) not leave messages containing confidential information 3) to begin any sensitive conversations with a disclaimer

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
5.15	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.	**Access control policy definition**	Interview responsible personnel to verify that a topic-specific policy on access control is established and communicated to all relevant interested parties	Analyse the access control policy to verify that established requirements consider business, risk and information security and include: 1) determining which entities require which type of access to the information and other associated assets 2) security of applications 3) physical access, which needs to be supported by appropriate physical entry controls 4) information dissemination and authorization and information security levels and classification of information 5) restrictions to privileged access 6) segregation of duties 7) relevant legislation, regulations and any contractual obligations regarding limitation of access to data or services 8) segregation of access control functions 9) formal authorization of access requests 10) the management of access rights 11) logging		
		Access control rules		Analyse documented access control rules to verify that they have taken into account: 1) consistency between the access rights and information classification 2) consistency between the access rights and the physical perimeter security needs and requirements 3) considering all types of available connections in distributed environments so entities are only provided with access to information and other associated assets, including networks and network services, that they are authorized to use; 4) considering how elements or factors relevant to dynamic access control can be reflected.	Review configured access control rules to verify they are consistent with the access control policy, the access control principles of need to know and need to use and that they are aligned with the documented access control rules.	
		Access control models	Interview responsible personnel to identify what access control model (MAC, DAC, RBAC, ABAC) is adopted and for what systems.		Review configured access control rules to verify they are consistent with the access control model they belong to.	
5.16	The full life cycle of identities should be managed.	**Unique ID**	Interview responsible personnel to verify how an identity is assigned to a single person		Review user ID repositories to verify they are unique and not reused	
		Shared identity	Interview responsible personnel to verify if and how shared identities are managed			Review the approval documentation for a sample of shared identities and observe how they are used.
		Non-human entities	Interview responsible personnel to verify how identities associated to non-human entities are managed and overseen			Review the approval documentation for a sample of non-human identities and observe how they are used and independently overseen.

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
		Identity disabling	Interview responsible personnel to verify how identities are removed as soon as no longer needed			Review a sample of identities belonging to persons that have left the organization to verify that they have been timely removed
		Identities information change management	Interview responsible personnel to verify how changes to identities are handled			Review a sample of identities recently changed to verify that changes have been correctly managed
5.17	Allocation and management of authentication information should be controlled by a management process, including advising personnel of appropriate handling of authentication information.	**Identity verification**	Interview responsible personnel to verify how the identity of the user to be assigned the authentication information is verified	Analyse the procedure used to verify the identity of user to be assigned the authentication information to ensure that they are not provided without its successful conclusion		
		Receipt	Interview responsible personnel to verify how users acknowledge the reception of authentication information			Observe a sample of user reception of authentication information acknowledge
		Change of default password	interview responsible personnel to verify that authentication information provided by vendors is changed immediately			Observe a sample of installation to verify that right after installation users are enforced to change authentication information
		Confidential password input			Examine the system configuration to verify that functionality that hides the passwords when are being entered is enabled	Observe how confidentiality of passwords inputed by personnel connecting to systems is provided on the screen
		Random password	Interview password assignment responsible personnel to understand how initial and to-be-reset passwords are generated differently to each other			Observe two or more password assignment or reset processes and how those passwords differ
		First password change			Review system configurations to enforce that a password change is required when a new account is created or its password is reset	Observe the presence of a change password request after personnel connects to a newly created or password-reset account
		Password length		Analyse password policies to verify that require a minimum password length	Review system configurations to enforce a minimum password length consistent with the policy for all users	
		Password complexity		Analyse password policies to verify that passwords are required to include characters belonging to different types (i.e. lower case, upper case, numbers, special character) and common dictionary words	Review system configurations to enforce a password complexity consistent with the policy for all users	
		Password change time		Analyse password policies to verify that require a minimum and a maximum time for password change	Review system configurations to enforce minimum and a maximum times for password change	

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
		Password history		Analyse password policies to verify that already used passwords are prohibited to be reused	Review system configurations to enforce passwords difference from already used ones	
		Password storage			Review system configuration settings to render all authentication credentials stored in an unreadable, unreversible fashion	Observe password storage locations to ensure they are unreadable and unreversible
		Password transmission			Review system configuration settings to render all authentication credentials unreadable during transmission	Observe eavesdropped network traffic to ensure password transmission is unreadable
5.18	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.	**Owner and management authorization**	Interview responsible personnel to verify how owner of information and associated assets grants access rights			Review a sample of access right grants to verify they have been duly authorized by the owner of information and associated assets
		segregation of duties	Interview responsible personnel to verify how segregation of duties between approver and implementers of access rights is addressed	Analyse function and organizational charts to verify segregation of roles of approval and implementation of access rights		
		Removing rights	Interview responsible personnel to verify how access rights that need to be removed are effectively removed			Review records of removal of access rights and verify they have been performed correctly and timely
		Modifying rights	Interview responsible personnel to verify how access rights that need to be modified for job/role change are managed			Review records of access rights modification after job/role change and verify they have been performed correctly and timely
		Temporary rights	Interview responsible personnel to verify how temporary access rights are managed			Review records of temporary access rights attribution to verify their correctness and effective expiration
		Regular reviews	Interview responsible personnel to verify how regular review are performed and with what frequency			Review the most recent access rights review report to verify it is regularly performed and it includes: -users' access rights changes -authorization for privileged access rights
5.19	Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	**Supplier relationship policy definition**	Interview responsible personnel to verify that topic-specific policy on supplier relationships is established and communicated to all relevant interested parties	Analyse the policy on supplier relationships to verify it describes processes and procedures to address security risks associated with the use of products and services provided by suppliers		
		Supplier choice and evaluation	Interview responsible personnel to verify how relevant suppliers with impact on CIA are selected and evaluated			Review evidence of supplier selection and evaluation processes to verify they are coherent and performed on all relevant suppliers
		Supplier controls review	Interview responsible personnel to verify what information security controls are reviewed and how for each supplied product or services			Review evidence of supplier information security control review to verify they are in line with information security requirements and performed on all relevant supplies of products and services

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
		Supplier risk assessment	Interview responsible personnel to verify how risks associated with the suppliers' use of the organization's information and other associated assets and malfunctioning or vulnerabilities of supplied products or services are addressed			Review evidence about the supplier risk management to verify it included risks associated with the suppliers' use of the organization's information and other associated assets and malfunctioning or vulnerabilities of supplied products or services are addressed
		Supplier non-conformance mitigation	Interview responsible personnel to verify how non-conformance of a supplier is mitigated			Review evidences regarding supplier non-conformance to verify they have been effectively handled
		Secure termination of supplier relationship	Interview responsible personnel to verify how the termination of a supplier is handled			Review past secure terminations to verify they included: 1) de-provisioning of access rights 2) information handling and return of assets 3) identifying ownership of intellectual property developed during the engagement 4) records management 5) secure disposal of information and other associated assets 6) ongoing confidentiality requirements
5.20	Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.	**Register of supplier agreements**	Interview responsible personnel to verify that agreements with suppliers are periodically reviewed and maintained in a register			Review the register to verify it is kept, the agreements are up-to-date and are cover all relevant products and services supplies

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
		Supplier agreements contents	Interview responsible personnel to verify how agreements with suppliers are defined and negotiated	Analyse supplier agreements templates to verify they contain as applicable: 1) classification and description of the information to be provided or accessed and methods of providing or accessing the information 2) legal, statutory, regulatory, contractual, information security (such as incident management, training and awareness, screening, backup, physical security, information transfer), business continuity requirements 3) obligation of each contractual party to implement an agreed set of controls, to periodically deliver a report on the effectiveness of controls, right to audit the supplier processes and controls related to the agreement and agreement on timely correction of relevant issues raised 4) rules of acceptable use of information and other associated assets 5) procedures or conditions for authorization and removal of the authorization for the use of the organization's information and other associated assets by supplier personnel 6) indemnities and remediation for failure of contractor to meet requirements, defect resolution and conflict resolution processes 7) incident management procedures 8) change management process ensuring advance notification to the organization and the possibility for the organization of not accepting changes 8) relevant provisions for sub-contracting, including the		Review supplier agreements to verify they contain as applicable: 1) classification and description of the information to be provided or accessed and methods of providing or accessing the information 2) legal, statutory, regulatory, contractual, information security (such as incident management, training and awareness, screening, backup, physical security, information transfer), business continuity requirements 3) obligation of each contractual party to implement an agreed set of controls, to periodically deliver a report on the effectiveness of controls, right to audit the supplier processes and controls related to the agreement and agreement on timely correction of relevant issues raised 4) rules of acceptable use of information and other associated assets 5) procedures or conditions for authorization and removal of the authorization for the use of the organization's information and other associated assets by supplier personnel 6) indemnities and remediation for failure of contractor to meet requirements, defect resolution and conflict resolution processes 7) incident management procedures 8) change management process ensuring advance notification to the organization and
5.21	Processes and procedures should be defined and implemented to manage information security risks associated with the ICT products and services supply chain.	**Propagation of security requirements and practices**	Interview responsible personnel to verify what supplied ICT services and products provided to the organization include sub-contracted elements			Review ICT services and products supplier agreements involving sub-contracted elements to verify they propagate the organization's security requirements and security practices to their supply chain.
		Critical components management	Interview responsible personnel to verify how critical components for maintaining functionality are identified and managed			Review the list of identified critical components for maintaining functionality to verify they are correctly identified and subject to increased scrutiny where built outside the organization, also allowing their tracing along the supply chain
		Genuine and unaltered components	Interview responsible personnel to verify how supplied components are verified to be genuine and unaltered			Review a sample of verifications for genuine and unaltered components to verify they are performed periodically and on a relevant sample.
		ICT supply chain risk management	Interview responsible personnel to verify how ICT supply chain risk management is implemented			Review ICT supply chain risk management results to verify they are periodically used to improve supply chain security
5.22	The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	**Conformant performance**	Interview responsible personnel to verify that supplier service performance is monitored			Review supplier service performance monitoring results with respect to agreed service levels and related actions to verify the process is active

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
		Supplier's changes monitoring	Interview responsible personnel to verify how all changes made by suppliers to their services are monitored.			Review that suppliers monitored changes include: 1) enhancements of current services 2) development of new systems 3) updates of supplier's policies and procedures 4) changed controls 5) changes to network 6) use of new technologies, new products or releases, new development tools 7) changes to physical location of service facilities 8) change of sub-suppliers and new sub-contracting with other suppliers
		Communication of relevant service security information	Interview responsible personnel to verify how: 1) security incident information 2) audit trails and records of information security events 3) operational problems, failures and disruption 4) follow-up on audit findings 5) vulnerabilities and other security aspects related to services delivered are communicated by suppliers to the organization			Review service reports, audit reports and service communications on the supplied services to verify they include: 1) security incident information 2) audit trails and records of information security events 3) operational problems, failures and disruption 4) follow-up on audit findings 5) vulnerabilities and other security aspects related to services delivered
5.23	Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements.	**Policy on the use of cloud services**	Interview responsible personnel to verify that topic-specific policy on the use of cloud services is established and communicated to all relevant interested parties	Analyse the policy on the use of cloud services to verify it includes how it intends to manage information security risks associated with the use of cloud services and defines information security requirements associated with cloud services usage		
		Cloud provider selection	Interview responsible personnel to verify which cloud services are deployed and how cloud provider are selected			Observe cloud provider selection processes and results to verify cloud provider selection is properly implemented, including: 1) respective roles and responsibilities definition 2) information security controls to be implemented by each part 3) contact establishment for mutual exchange of information
		Agreements with cloud service providers		Analyse agreements templates with cloud service providers to verify they provide protection of the organization's data and availability of services. Verify they include: 1) solution based on accepted standards 2) access control managing 3) malware monitoring and protection 4) approved storage location of organization's information and adequate backup 5) dedicated support for information security incident and digital evidence gathering 6) information security requirements compliance also when sub-contracting, if accepted by the organization 7) organization's information provide or return when requested or at termination of service		Review a sample of agreements with cloud service providers to verify they provide protection of the organization's data and availability of services. Verify they include: 1) solution based on accepted standards 2) access control managing 3) malware monitoring and protection 4) approved storage location of organization's information and adequate backup 5) dedicated support for information security incident and digital evidence gathering 6) information security requirements compliance also when sub-contracting, if accepted by the organization 7) organization's information provide or return when requested or at termination of service

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
5.24	The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	**Incident management plan**	Interview responsible personnel to verify that an incident management plan is established and communicated to all relevant interested parties	Analyse the incident management plan to verify it includes: 1) evaluation of information security events 2) information security events and incidents handling 3) coordination with internal and external interested parties 4) logging incident management activities 5) handling of digital evidence 6) root cause analysis or post-mortem procedures 7) identification of lessons learned and improvements		
		Incident management procedures	Interview responsible personnel to verify that appropriate information security incident management procedures are established and communicated to all relevant parties	Analyse incident management procedures to verify they include: 1) monitoring, detecting, analysing and reporting 2) incident response and escalation, possible activation of crisis management and continuity plans 3) coordination with internal and external interested parties 4) logging incident management activities 5) handling digital evidence 6) root cause analysis or post-mortem procedures 7) identification of inputs to improvements to incident managements or to controls		Review a sample of performed incident management activities to verify the procedures have been correctly followed and were effective
		Incident reporting procedures	Interview responsible personnel to verify that appropriate information security incident reporting procedures are established and communicated to all relevant parties	Analyse incident reporting procedures to verify they include: 1) reactive actions to information security events 2) incident forms to support personnel 3) feedback processes to notify who reported events 4) creation of incident reports		Review a sample of incident reports to verify he procedures have been correctly followed
5.25	The organization should assess information security events and decide if they are to be categorized as information security incidents.	**Categorization and prioritization scheme**	Interview point of contact personnel to verify what agreed categorization and prioritization scheme is used by the point of contact to classify security events and how it is based on their potential consequences			Review a sample of results of the assessment decisions to verify the correct use of the adopted information security categorization scheme
5.26	Information security incidents should be responded to in accordance with the documented procedures.	**Incident response procedures**	Interview responsible personnel to verify that incident response procedures are established and are distributed to all relevant interested parties	Analyse incident response procedures to verify they include: 1) affected systems identification 2) collection of evidence 3) requiring crisis management activities and business continuity plans 4) logging of response activities 5) requiring forensic analysis 6) informing interested parties 7) formally closing and recording solved incidents 8) coordination with authorities, external interest groups and forums, suppliers and clients 9) post-incident analysis including root cause 10) vulnerabilities and weaknesses management		
5.27	Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.	**Procedures to gain incident information**	Interview responsible personnel to verify that procedures to quantify and monitor types, volumes and costs of information security incidents are established			Review a sample of information gathered from security incidents to verify how types, volumes and costs have been quantified and monitored
		Incident management improvements	interview responsible personnel to verify how incident management has benefited from information gained from the evaluation of security incidents			Review performed actions to improve incident management considerations derived from information security incidents experience

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
5.28	The organization should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	**Evidence management procedures**	Interview responsible personnel to verify that procedures to manage evidence are established and applied to information security events that require legal actions in compliance with national legislation	Analyse procedures for evidence management to verify they provide instructions for the identification, collection, acquisition and preservation of evidence in compliance with national legislation		
		Collected evidence quality	Interview responsible personnel to verify that collection of evidence is performed by qualified personnel			Review collected evidence to verify that there are elements proving that: 1) records have not been tampered with in any way 2) copies of electronic devices are identical to the originals 3) any source information system was operating correctly when the gathered evidence was recorded
5.29	The organization should plan how to maintain information security at an appropriate level during disruption.	**Adapting controls during disruption**	Interview responsible personnel to verify which processes are implemented to adapt information security controls during disruption	Analyse business continuity plans to verify they include adapting controls to maintain information security levels during disruption		
		Adopting compensating controls during disruption	Interview responsible personnel to identify which compensating controls are planned to be used during disruption	Analyse business continuity plans to verify they include appropriate compensating controls		
5.30	ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	**ICT continuity requirements**	Interview responsible personnel to verify how ICT continuity requirements involving ICT services are defined, including RTOs and RPOs	Analyse the BIA from which ICT continuity requirements are formalized from to verify it is accurate, complete of RTOs and RPOs for each service or resource and actual		
		Continuity plans	Interview responsible personnel to verify how continuity plans are defined, developed, implemented and tested following continuity strategies	Analyse continuity plans to verify they include: 1) response and recovery procedures 2) performance and capacity specifications 3) recovery time objective of each prioritized ICT service and the procedures for restoring those components 4) recovery point objectives of the prioritized ICT resources defined as information and the procedures for restoring the information		Review continuity plans review and testing reports to verify they are done periodically and exhaustively, being approved by the management
		Organizational plan to face disruption	Interview responsible personnel to verify that organizational plan to face disruption involves personnel with authority and adequate competences	Analyse the foreseen organizational structure for facing disruptions to verify it is actual, complete and functional		
5.31	Legislation, regulations and statutory 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.	**External requirements management**	Interview responsible personnel to verify that legal, statutory, regulatory and contractual requirements relevant for the organization's type of business are identified and regularly reviewed	analyse information security policies and procedures to verify that legal, statutory, regulatory and contractual requirements have been taken in consideration and kept up-to-date		Observe implemented information security controls and activities to verify that legal, statutory, regulatory and contractual requirements have been taken in consideration and kept up-to-date
		Foreign countries compliance	Interview responsible personnel to identify countries included in the business of the organization and the related products and services			Observe provisioned products and services to verify how foreign countries legal requirements are taken into account
5.32	The organization should implement appropriate procedures to protect intellectual property rights.	**Policy on intellectual property rights protection**	Interview responsible personnel to verify that a topic-specific policy on protection of intellectual property rights is established and communicated to all relevant interested parties	Analyse the policy to verify that the intellectual property rights include assets like software or document copyright, design rights, trademarks, patents and source code licences		

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
		Software and products conformance with intellectual property rights protection	Interview responsible personnel to verify which procedures are defined to guarantee conformance in using software and products covered by intellectual property rights	Analyse procedures that involve software and products covered by intellectual property rights to verify they include: 1) acquiring authorized software and licensed products by reputable sources 2) maintaining appropriate licence conditions 3) how to dispose of or transfer software to others 4) copying and duplicating prohibition unless permitted by copyright law or the applicable licences		Review proof and evidence of ownership of a sample of software licences for the correct user / employed resources
5.33	Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	**Guidance on records management**	Interview responsible personnel to verify that topic-specific guidance on records management is established according to business context and requirements for their management change over time	Analyse the guidance on records management to verify it includes record and related retention schedules		Review a sample of records to verify that retention periods are implemented according to the applicable categorization of records
		Storage and handling records	Interview responsible personnel to verify that procedures to manage records' storage and handling including disposal and prevention of manipulation are established	Analyse the procedures to manage records' storage to verify they include safeguards against loss due to future technology change and are in accordance with recommendations provided by manufacturers of storage media		
5.34	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.	**Policy on privacy and protection of PII**	Interview responsible personnel to verify that topic-specific policy on privacy and protection of PII is established and communicated to all relevant interested parties	Analyse the policy on privacy and protection of PII to verify they include responsibility for handling PII		
		PII preservation and protection procedures	Interview responsible personnel to verify that procedures to preserve privacy and protect PII are established and communicated to all parties involved in PII processing	Analyse PII preservation and protection procedures to verify they include the implementation of controls mandate by applicable legislation		
5.35	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.	**Independent reviews**	Interview responsible personnel to verify how independent reviews are periodically performed by competent individuals independent of the area under review			Review that independent review reports are periodically produced and distributed to the management
		Additional reviews	Interview responsible personnel to verify that independent reviews are also performed when: 1) laws and regulations affecting the organization change 2) significant incidents occur 3) new business or changes a current business are introduced 4) new product or service, or changes the use of a current product or service are introduced 5) the organization changes the information security controls and procedures significantly			Review that independent review reports are produced and distributed to the management when: 1) laws and regulations affecting the organization change 2) significant incidents occur 3) new business or changes a current business are introduced 4) new product or service, or changes the use of a current product or service are introduced 5) the organization changes the information security controls and procedures significantly
		Corrective actions	Interview responsible personnel to verify how corrective actions introduced after independent reviews are managed			Review a sample of corrective actions introduced after independent reviews of information security to verify they are recorded and implemented

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
5.36	Conformance with the organization's information security policy, topic-specific policies, rules and standards should be regularly reviewed.	**Review of the conformance of information security**	Interview responsible personnel to verify how reviews of information security conformance with policies and standards are regularly performed			Review outputs of automatic measurement and reporting tools for information security conformance reviews to verify they are producing valid inputs and they are timely taken into account
		Non-conformance management	Interview responsible personnel to verify how any detected non-conformance is addressed			Review evidence of non-conformance management to verify that they include: 1) identification of the causes of the non-conformance 2) evaluation of the need for corrective actions to achieve conformance 3) implementation of appropriate corrective actions 4) review of corrective actions taken to verify its effectiveness and identify any deficiencies or weaknesses
5.37	Operating procedures for information processing facilities should be documented and made available to personnel who need them.	**Operating procedures**	Interview responsible personnel to verify how documented operational activities are prepared for activities: 1) performed in the same way by many people 2) rarely performed or new 3) presenting a risk if not performed correctly 4) to be handed over to new personnel	Analyse procedures for organization's operational activities to verify they specify: 1) responsible individuals 2) secure installation and configuration of systems 3) processing and handling of information 4) scheduling requirements, including interdependencies with other systems 5) maintenance instructions		
		Review and update of procedures	Interview responsible personnel to verify how documented procedures are regularly reviewed and updated when needed	Review a sample of procedures to verify they have been properly updated		