ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
7.1	Security perimeters should be defined and used to protect areas that contain information and other associated assets.	**Physical security perimeter definition**	Interview responsible personnel to identify the areas that contain information and their physical security perimeters	Analyse the asset inventory records to verify the areas that contain information. Analyse all in-scope buildings planimetries to identify their physical security perimeters.		Observe the physical security perimeters to verify they correspond to the declared and documented ones
		Physical security perimeter robustness	Interview responsible personnel to understand the robustness of the physical security perimeters	Analyse all in-scope buildings planimetries to verify the absence of gaps in their physical security perimeters		Observe the physical security perimeters to verify their robustness and the absence of gaps
		Public access areas	Interview responsible personnel to identify public access areas and adopted measures to prevent unauthorized access to the bordering premises			Observe public access areas to verify that unauthorized access to the bordering premises is forbidden
7.2	Secure areas should be protected by appropriate entry controls and access points.	**Physical logbook**	Interview responsible personnel to verify that a physical logbook is maintained to document all accesses			Review a sample of physical logbook records to verify they are complete with all required information including date and time of entry, accurate and stored for a limited and defined time period only
		Reception area	Interview the reception personnel to understand their activities and verify their duties			Observe the reception area to verify it can continuously control physical access to the site
		Badge management	Interview the reception personnel to verify what types of badge are adopted to access what secure areas and how they are managed		Review badge configuration system to be configured consistently with access requirements	Observe how badge readers react to badges not authorized for entry for each secure area
		Physical key management	Interview responsible personnel to identify what physical keys or combinations are in use and how they are managed			Review the physical key logbook to be inclusive of all physical keys or combinations and to fully document their assignments
		Additional authentication factors	Interview responsible personnel to identify where additional authentication factors such as biometric means or PINs are deployed			Observe additional authentication factors use to be in line with its expected behavior and how the access control system reacts to their wrong provision
		Personnel identification	Interview reception personnel to verify the procedures to distinguish between onsite personnel and visitors			Observe a sample of personnel within the site to be distinguishable if onsite personnel or visitor

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
		Visitors authorization	Interview reception personnel to verify that visitors are granted access only after being authorized, accompanied and that they surrender any assigned element before leaving the site			Observe a sample of visitor records to verify that they have been properly authorized, accompanied and that have surrendered any assigned element before leaving the site
		Delivery and loading	Interview responsible personnel to identify delivery and loading areas			Observe that delivery and loading areas access doesn't allow unauthorized access to other parts of the building
		Incoming goods	Interview responsible personnel to verify that incoming goods are inspected			Review incoming goods registers to verify they are tracked consistently with all other assets
7.3	Physical security for offices, rooms and facilities should be designed and implemented.	**Critical facilities and public**	Interview responsible personnel to verify what critical facilities are used and which ones are accessible by the public			Observe all critical facilities to verify their direct public accessibility and the visibility of confidential information or activities from the outside
		Buildings indications	Interview responsible personnel to verify how buildings are made unobtrusive and avoid the identification of information processing activities			Observe all buildings to verify the presence of signs, documents and indications confirming that and where information processing facilities are carried over within them
7.4	Premises should be continuously monitored for unauthorized physical access.	**Surveillance system**	Interview responsible personnel to verify what surveillance measures are present, how they are employed for monitoring, how frequently and by who	Analyse all in-scope buildings planimetries to verify the siting of all types of surveillance measures		Observe surveillance measures monitoring reports to verify they are performed as intended
		Contact, sound or motion detectors	Interview responsible personnel to verify what contact, sound or motion detectors are installed and periodically tested			Observe a sample of contact, sound or motion detectors, cross-check them with the planimetries and verify their coverage and that they work as intended
		CCTV	Interview responsible personnel to verify what CCTV cameras are installed and periodically tested			Observe a sample of CCTV, cross-check them with the planimetries and their coverage and that they work as intended
		Alarm system	Interview responsible personnel to verify what alarm system is installed, how it is secured, triggered and who gets alerted			Review the alarm system control panel location and its logs to verify it is secure, it correctly works and appropriate reaction is always initiated
		Access to surveillance system	Interview responsible personnel to verify how CCTV recordings and alarm system panels cannot be accessed by unauthorized people			Review CCTV recordings and alarm system panels siting and access controls to verify they cannot be accessed by unauthorized people
		Laws and regulation compliance	Interview responsible personnel to verify that acquired and recorded personal data, security notices are in accordance with applicable laws and regulation	Examine recording policies to verify that they respect the regulation, including an established retention period of monitoring videos		

ID	Control		Testing Procedure	Interview	Document	Configuration	Observation
7.5	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.		**Risk assessment**	Interview responsible personnel to verify that protection against physical and environmental threats is executed according to results of risk assessment activities prior to beginning critical operations and periodically			Review risk assessment results to verify they identify physical and environmental threats and are performed prior to beginning critical operations and periodically
			Specialist advice	Interview responsible personnel to verify that specialist advices are considered when designing how to manage physical and environmental threats			Review risk treatment plans to verify they included specialist advices are considered when designing how to manage physical and environmental threats
			Physical premises location	Interview responsible personnel to verify that the physical premises locations have taken into account both local topography and urban threats			Observe physical premises locations to verify how they have taken into account both local topography and urban threats
		Safeguards against:	**Fire**	Interview responsible personnel to verify that systems to detect and suppress fires have been designed and installed			Observe deployed alarms, fire detection and suppression system and related activity/testing reports to confirm they work as expected
			Flooding	Interview responsible personnel to verify that systems able to detect and suppress flooding have been designed and installed			Observe deployed alarms, flooding detection systems and water pumps and related activity/testing reports to confirm they work as expected
			Electrical surges	Interview responsible personnel to verify that protection of information systems against electrical surges have been designed and installed			Observe deployed systems protecting servers and clients from electrical surges or similar events and related activity/testing reports to confirm they work as expected
			Explosives and weapons	Interview responsible personnel to verify that inspection of premises is performed against the presence of explosives and weapons			Review records of performed inspections to verify they are done appropriately
7.6	Security measures for working in secure areas should be designed and implemented.		**Personnel awareness**	Interview personnel to verify that secure areas information are distributed according to the need-to-know principle only			Observe all secure areas to verify the presence of signs, documents and indications confirming that and what information processing activities are carried over within them
			Supervision	Interview responsible personnel to verify that working in secure area is always supervised			Observe personnel working in secure areas to verify how they are always supervised
			Secure areas management	Interview responsible personnel to verify that secure areas are locked if vacant, that photo, video and audio recordings are forbidden unless authorized and that endpoint devices use is controlled			Observe all secure areas to verify they are locked if vacant, that photo, video and audio recordings are forbidden unless authorized and that endpoint devices use is controlled

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
7.7	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.	**Clear desk policy definition**	Interview responsible personnel to verify that a topic-specific policy on clear desk and clear screen is established and distributed to all interested parties	Analyze the topic-specific policy to verify it includes protection of critical business information, user endpoint devices, printers, documents and removable storage media		
		Information physical protection	Interview responsible personnel to verify how sensitive or critical information are protected when not in use			Observe means used to protect sensitive or critical business information, documents and removable storage media when not in use to verify their actual protection strength
		Printers	Interview responsible personnel to verify how sensitive or critical information are protected after printing			Observe how printing processes ensure printed information protection
		Vacating facilities	Interview responsible personnel to verify how vacating facilities activities are managed	Analyze procedures used to vacate facilities to verify that they include an extra final sweeping		Review results of procedures for vacating facility
7.8	Equipment should be sited securely and protected.	**Equipment and processing facilities location**	Interview responsible personnel to verify how equipment and processing facilities have been positioned to minimize information security risks			Observe equipment and processing facilities to verify the adequacy of their siting to minimize information security risks
		Physical and environmental threats controls	Interview responsible personnel to verify which controls are in place against physical and environmental threats			Observe deployed controls against physical and environmental threats to confirm they work as expected
		Information processing facilities environmental conditions monitoring	Interview responsible personnel to verify which controls are in place to monitor information processing facilities environmental conditions			Review information processing facilities environmental conditions monitoring results to verify they are under control
		Separation of facilities	Interview responsible personnel to identify which facilities are under the organization control and which ones are not within shared environments			Observe facilities managed by organization in shared environments to verify they are adequately separated from the ones not managed by the organization
7.9	Off-site assets should be protected.	**Off-site assets identification**	Interview responsible personnel to verify that off-site assets and ones used on behalf of the organization are clearly identified during classification and inventory			Review the asset inventory and identify off-site assets. Verify it includes both devices owned by the organization and privately when used on behalf of the organization.

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
		Personnel behaviour	Interview responsible personnel to verify that personnel authorized to use off-site assets is aware of: 1) not leaving devices unattended in public 2) following manufacturers' instructions for asset protection 3) paying attention on viewing information in public			Review personnel agreement on guidance about the use of off-site devices including: 1) not leaving devices unattended in public 2) following manufacturers' instructions for asset protection 3) paying attention on viewing information in public
		Chain of custody of transferred off-site equipment	Interview responsible personnel to verify how a log identifying the chain of custody for transferred off-site equipment is maintained			Review a sample of logs to verify that chain of custody records include names and organizations of those who have been responsible for the off-site equipment in transfer
		Permanently off-site equipment	Interview responsible personnel to verify how permanently off-site equipment is protected from information security threats.			Review a sample of permanently off-site equipment to verify adopted information security measures work as intended.
7.10	Storage media should be managed through its life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	**Storage media management policy definition**	Interview responsible personnel to verify that a topic-specific policy on the management of removable storage media is established and communicated to all interested parties	Analyze the storage media management policy to verify it includes all relevant aspects of the lifecycle of storage media		
		Removable storage media identification	Interview responsible personnel to verify how removable storage media are identified during classification and inventory			Review asset inventories and verify the removable storage media are adequately identified and included
		Safe storage environment	Interview responsible personnel to verify how removable storage media are stored in a secure environment that reflects classification of information and manufacturer's specifications			Observe a sample of media to be stored accordingly to their classification and to their manufacturer's specifications
		Cryptographic protection	Interview responsible personnel to identify which media require cryptographic protection according to classification of stored information			Observe a sample of media requiring cryptographic protection to verify they effectively use it
		Degradation handling	Interview responsible personnel to verify how storage media degradation is addressed			Observe how media degradation prevention is applied to older storage media to verify it is effectively performed

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
		Secure reuse and disposal	Interview responsible personnel to verify how storage media are reused and disposed of			Observe a sample of reused storage or disposed media to verify that previous information have been effectively deleted
7.11	Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.	**Deployment of equipment supporting the utilities**	Interview responsible personnel to identify which equipment supporting the utilities is deployed		Review supporting utilities equipment network configurations to verify they are deployed on separated networks.	Review supporting utilities equipment inspection and testing records to verify that they follow relevant manufacturer's specifications and are regularly performed.
		Utilities appraisal and control	Interview responsible personnel to verify that utilities that support facilities are regularly appraised to meet business growth or interaction with other utilities			Observe how utilities that support facilities are monitored against malfunctions and verify that their usage capacity is adequate for the foreseen business growth
		Emergency management	Interview responsible personnel to verify that emergency contact details for utilities are made available to personnel			Observe that emergency lighting and communications are deployed and verify that switches for utilities are located near emergency exits or equipment rooms
7.12	Cables carrying power, data or supporting information services should be protected from interception, interference or damage.	**Power and telecommunications lines protection**	interview responsible personnel to identify where power and telecommunications lines are underground and where alternative protection is necessary			Observe that adequate alternative protection for power and telecommunication lines is addressed
		Interference prevention	Interview responsible personnel to verify how interference between cables is addressed in each information processing facility			Review cabling plans of each information processing facility to verify the effective segregation of the cables
		Critical or sensitive systems protection	Interview responsible personnel to verify what critical or sensitive system cabling requires additional protection			Observe critical or sensitive systems cabling to verify that they are effectively protected
		Cable labelling	Interview responsible personnel to verify how cables are distinguished between each other			Review a sample of information processing facilities cabling plans and match them with physical observation to verify the effective distinguishability of the cables
7.13	Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.	**Supplier's maintenance recommendations**	Interview responsible personnel to verify that equipment maintenance considers supplier's and insurance recommended frequency			Review a sample of equipment maintenance records to verify they are aligned with supplier's and insurance recommended frequency

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
		Authorized maintenance personnel	Interview responsible personnel to verify that only authorized personnel carry out maintenance on equipment and they act under a suitable confidentiality agreement and under supervision			Review a sample of equipment maintenance records to verify they have been performed by authorized personnel, covered by suitable confidentiality agreements and supervised
7.14	Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	**Equipment analysis**	Interview responsible personnel to verify how equipment analysis is performed before disposal or re-use			Review a sample of performed equipment analysis to verify they are duly performed before allowing disposal or re-use
		Damaged equipment analysis	Interview responsible personnel to verify how damaged equipment is analyzed before deciding whether to destroy or repair it			Review a sample of performed damaged equipment analysis to verify they are duly performed before allowing destruction or repair