Document Ref.: ICTA/DIT/1/2024

Information and Communication Technologies Authority

Guidelines on Security Measures for all licensed telecommunication operators

Guidelines made under Section 17(3) of Information and Communication Technologies Act 2001 (as amended)

28 June 2024

Guidelines on Security Measures for all licensed telecommunication operators

The 29 high-level security objectives are grouped in 8 domains. For each security objective the detailed security measures, which could be implemented by the provider are listed, as well as the type of evidence that could be taken into consideration by an auditor, for example, when assessing if measures are in place.

The 8 domains and the 29 security objectives are as follows: -

1. **D1: GOVERNANCE AND RISK MANAGEMENT**
   - SO1: Information security policy
   - SO2: Governance and risk management
   - SO3: Security roles and responsibilities
   - SO4: Security of third-party dependencies

2. **D2: HUMAN RESOURCES SECURITY**
   - SO5: Background checks
   - SO6: Security knowledge and training
   - SO7: Personnel changes
   - SO8: Handling violations

3. **D3: SECURITY OF SYSTEMS AND FACILITIES**
   - SO9: Physical and environmental security
   - SO10: Security of supplies
   - SO11: Access control to network and information systems
   - SO12: Integrity of network and information systems
   - SO13: Use of encryption
   - SO14: Protection of security critical data

4. **D4: OPERATIONS MANAGEMENT**
   - SO15: Operational procedures
   - SO16: Change management
   - SO17: Asset management

5. **D5: INCIDENT MANAGEMENT**
   - SO18: Incident management procedures
   - SO19: Incident detection capability
   - SO20: Incident reporting and communication

6. **D6: BUSINESS CONTINUITY MANAGEMENT**
   - SO21: Service continuity strategy and contingency plans
   - SO22: Disaster recovery capabilities

7. **D7: MONITORING, AUDITING AND TESTING**

SO23: Monitoring and logging policies

SO24: Exercise contingency plans

SO25: Network and information systems testing

SO26: Security assessments

SO27: Compliance monitoring

8. **D8: THREAT AWARENESS**

SO28: Threat intelligence

SO29: Informing users about threats

1. D1: Governance and risk management

The domain "Governance and risk management" covers the security objectives related to governance and management of network and information security risks.

1.1. SO1: Information security policy

Establish and maintain an appropriate information security policy.

	Security measures	Evidence
1	a) Set a high-level security policy addressing the security of networks and services. b) Make key personnel aware of the security policy.	i. Documented security policy, including networks and services in scope, critical assets supporting them, and the security objectives. ii. Key personnel are aware of the security policy and its objectives (interview).
2	c) Set detailed information security policies for critical assets and business processes. d) Make all personnel aware of the security policy and what it implies for their work. e) Review the security policy following incidents.	iii. Documented information security policies, approved by management, including applicable law and regulations, accessible to personnel. iv. Personnel are aware of the information security policy and what it implies for their work (interview). v. Review comments or change logs for the policy.
3	f) Review the information security policies periodically, and take into account violations, exceptions, past incidents, past tests/exercises, and incidents affecting other (similar) providers in the sector.	vi. Information security policies are up to date and approved by senior management. vii. Logs of policy exceptions, approved by the relevant roles. viii. Documentation of review process, taking into account changes and past incidents.

1.2. SO2: Governance and risk management

Establish and maintain an appropriate governance and risk management framework, to identify and address risks for the communications networks and services.

	Security measures	Evidence
1	a) Make a list of the main risks for security of networks and services, taking into account main threats for the critical assets. b) Make key personnel aware of the main risks and how they are mitigated.	i. List of main risks described at a high level, including the underlying threat(s) and their potential impacton the security of networks and services ii. Key personnel know the main risks (interview).
2	c) Set up a risk management methodology and/or tools based on industry standards. d) Ensure that key personnel use the risk management methodology and tools. e) Review the risk assessments following changes or incidents. f) Ensure residual risks are accepted by management.	iii. Documented risk management methodology and/or tools. iv. Guidance for personnel on assessing risks. v. List of risks and evidence of updates/reviews. vi. Review comments or change logs for risk assessments. vii. Management approval of residual risks.
3	g) Review the risk management methodology and/or tools, periodically, taking into account changes and past incidents.	viii. Documentation of the review process and updates of the risk management methodology and/or tools.

1.3. SO3: Security roles and responsibilities

Establish and maintain an appropriate structure of security roles and responsibilities.

	Security measures	Evidence
1	a) Assign security roles and responsibilities to personnel. b) Make sure the security roles are reachable in case of security incidents.	i. List of security roles (CISO, DPO, business continuity manager, etc.),who occupies them and contact information.
2	c) Personnel is formally appointed in security roles. d) Make personnel aware of the security roles in your organisation and when they should be contacted.	ii. List of appointments (CISO, DPO,etc.), and description of responsibilities and tasks for security roles (CISO, DPO, etc.). iii. Awareness/dissemination material for personnel explaining security roles and when/how they should be contacted.
3	e) Structure of security roles and responsibilities is regularly reviewed and revised, based on changes and/or past incidents.	iv. Up-to-date documentation of the structure of security role assignments and responsibilities v. Documentation of review process, taking into account changes and past incidents.

1.4. SO4: Security of third-party dependencies

Establish and maintain a policy, with security requirements for contracts with third parties, to ensure that dependencies on third parties do not negatively affect security of networks and/or services.

	Security measures	Evidence
1	a) Include security requirements in contracts with third-parties, including confidentiality and secure transfer of information.	i. Explicit security requirements in the contracts with third parties supplying IT products, IT services, outsourced business processes, helpdesks, call centres, interconnections, shared facilities, etc.
2	b) Set a security policy for contracts with third-parties. c) Ensure that all procurement of services/products from third-parties follows the policy. d) Review security policy for third parties, following incidents or changes. e) Demand specific security standards in third-party supplier's processes during procurement. f) Mitigate residual risks that are not addressed by the third party.	ii. Documented security policy for contracts with third parties. iii. List of contracts with third-parties. iv. Contracts for third party services contain security requirements, in line with the security policy for procurement. v. Review comments or change logs of the policy. vi. Contracts with equipment suppliers contain requirements for adhering to security best practices and industry standards. vii. Residual risks resulting from dependencies on third parties are listed and mitigated.
3	g) Keep track of security incidents related to or caused by third-parties. h) Periodically review and update security policy for third parties at regular intervals, taking into account past incidents, changes, etc.	viii. List of security incidents related to or caused by engagement with third-parties. ix. Documentation of the policy review process.

2. D2: Human resources security

The domain "Human resources security" covers the security objectives related to personnel.

2.1 SO5: Background checks

Perform appropriate background checks on personnel if required for their duties and responsibilities.

	Security measures	Evidence
1	a) Check professional references of key personnel (system administrators, security officers, guards, etc.).	i. Documentation of checks of professional references for key personnel.
2	b) Perform background checks/screening for key personnel, when needed and legally permitted. c) Set up a policy and procedure for background checks.	ii. Policy and procedure for background checks/screenings. iii. Guidance for personnel about when/how to perform background checks/screenings.
3	d) Review and update policy/procedures for background checks and reference checks at regular intervals, taking into account changes and past incidents.	iv. Review comments or change logs of the policy/procedures.

2.2 SO6: Security knowledge and training

Ensure that personnel have sufficient security knowledge and that they are provided with regular security training.

	Security measures	Evidence
1	a) Provide key personnel with relevant training and material on security issues.	i. Key personnel have followed security trainings and have sufficient security knowledge (interview).
2	b) Implement a program for training, making sure that key personnel have sufficient and up-to-date security knowledge. c) Organise trainings and awareness sessions for personnel on security topics important for your organisation.	ii. Personnel have participated in awareness sessions on security topics. iii. Documented program for training on security skills, including objectives for different roles and how to reach them (by e.g. training, awareness raising, etc.).
3	d) Review and update the training program periodically, taking into account changes and past incidents. e) Test the security knowledge of personnel.	iv. Updated security awareness and training program v. Results of tests of the security knowledge of personnel. vi. Review comments or change logs for the program.

2.3 SO7: Personnel changes

Establish and maintain an appropriate process for managing changes in personnel or changes in their roles and responsibilities.

	Security measures	Evidence
1	a) Following changes in personnel revoke access rights, badges, equipment, etc., if no longer necessary or permitted. b) Brief and educate new personnel on the policies and procedures in place.	i. Evidence that personnel changes have been followed up with revocation of access rights, badges, equipment, etc. ii. Evidence that new personnel has been briefed and educated about policies and procedures in place.
2	c) Implement policy/procedures for personnel changes, taking into account timely revocation of access rights, badges and equipment. d) Implement policy/procedures for education and training for personnel in new roles.	iii. Documentation of process for personnel changes, including responsibilities for managing changes, description of rights of access and possession of assets per role, procedures for briefing and training personnel in new roles. iv. Evidence that personnel changes have been carried out according to the process and that access rights have been updated timely (e.g. checklists).
3	e) Periodically check that the policy/procedures are effective. f) Review and evaluate policy/procedures for personnel changes, taking into account changes or past incidents.	v. Evidence of checks of access rights etc. vi. Up to date policy/procedures for managing personnel changes. vii. Review comments or change logs.

2.4 SO8: Handling violations

Establish and maintain a disciplinary process for personnel who violate security policies and have a broader process that covers security incidents caused by violations by personnel.

	Security measures	Evidence
1	a) Hold personnel accountable for security incidents caused by violations of policies, for example via the employment contract.	i. Rules for personnel, including responsibilities, code of conduct, violations of policies, etc., possibly as part of employment contracts.
2	b) Set up procedures for violations of policies by personnel.	ii. Documentation of procedures, including types of violations which may be subject to disciplinary actions, and which disciplinary actions may be taken.
3	c) Periodically review and update the disciplinary process, based on changes and past incidents.	iii. Review comments or change logs

3. D3: Security of systems and facilities

This domain "Security of systems and facilities" covers the physical and logical security of network and information systems and facilities.

3.1. SO9: Physical and environmental security

Establish and maintain the appropriate physical and environmental security of network and information systems and facilities.

	Security measures	Evidence
1	a) Prevent unauthorised physical access to facilities and infrastructure and set up adequate environmental controls, to protect provider assets against unauthorised access, burglary, fire, flooding, etc.	i. Basic implementation of physical security measures and environmental controls, such as door and cabinet locks, burglar alarm, fire alarms, fire extinguishers, etc.
2	b) Implement a policy for physical security measures and environmental controls. c) Industry standard implementation of physical and environmental controls. d) Apply reinforced controls for physical access to critical assets.	ii. Documented policy for physical security measures and environmental controls, including description of facilities and systems in scope. iii. Physical and environmental controls, like electronic control of entrance and audit trail, segmentation of spaces according to authorization levels, automated fire extinguishers with halocarbon gases, etc. iv. The policy includes lists of critical assets and reinforced physical controls for accessing these assets.
3	e) Evaluate the effectiveness of physical and environmental controls periodically. f) Review and update the policy for physical security measures and environmental controls taking into account changes and past incidents.	v. Up to date policy for physical security measures and environmental controls vi. Documentation about evaluation of environmental control, review comments or change logs.

3.2. SO10: Security of supplies

Establish and maintain appropriate security of critical supplies (for example electric power, fuel, cooling etc.).

	Security measures	Evidence
1	a) Ensure security of critical supplies.	i. Security of critical supplies is protected in a basic way, for example, backup power and/or backup fuel is available.
2	b) Implement a policy for security of critical supplies. c) Implement industry standard security measures to protect critical supplies and supporting facilities (e.g. passive cooling, automatic restart after power interruption, battery backup power, diesel generators, backup fuel, etc.).	ii. Documented policy to protect critical supplies such as electrical power, fuel, etc., describing different types of supplies, and the security measures protecting the supplies. iii. Evidence of industry standard measures to protect the security of critical supplies
3	d) Implement state of the art security measures to protect critical supplies (such as active cooling, UP, hot standby power generators, SLAs with fuel delivery companies, redundant cooling and power backup systems). e) Review and update policy and procedures to secure critical supplies regularly, taking into account changes and past incidents.	iv. Evidence of state of the art measures to protect security of critical supplies. v. Updated policy for securing critical supplies and supporting facilities, review comments and/or change logs.

3.3. SO11: Access control to network and information systems

Establish and maintain appropriate (logical) access controls for access to network and information systems.

	Security measures	Evidence
1	a) Users and systems have unique ID's and are authenticated before accessing services or systems. b) Implement logical access control mechanism for network and information systems to allow only authorised use.	i. Access logs show unique identifiers for users and systems when granted or denied access. ii. Overview of authentication and access control methods for systems and users.

2	c) Implement policy for protecting access to network and information systems, addressing for example roles, rights, responsibilities and procedures for assigning and revoking access rights. d) Choose appropriate authentication mechanisms, depending on the type of access. e) Monitor access to network and information systems, have a process for approving exceptions and registering access violations. f) Reinforce controls for remote access to critical assets of network and information systems by third parties.	iii. Access control policy including description of roles, groups, access rights, procedures for granting and revoking access. iv. Different types of authentication mechanisms for different types of access. v. Log of access control policy violations and exceptions, approved by the security officer. vi. Principles of least privilege and segregation of duties are documented and applied where appropriate. vii. Remote access to critical assets by third-parties is minimised and subjected to strict access controls, including state of the art authentication, authorisation and auditing controls, especially for privileged accounts.
3	g) Evaluate the effectiveness of access control policies and procedures and implement cross checks on access control mechanisms. h) Access control policy and access control mechanisms are reviewed and when needed revised.	viii. Reports of (security) tests of access control mechanisms. ix. Tools for detection of anomalous usage of systems or anomalous behaviour of systems (such as intrusion detection and anomaly detection systems). x. Logs of intrusion detection and anomaly detection systems. xi. Updates of access control policy, review comments or change logs. xii. Documented risk analysis for the application of logging and retention xiii. Procedures to ensure that access controls are in effect all the time and that they evolve with the network.

3.4. SO12: Integrity of network and information systems

Establish and maintain integrity of network and information systems and protect from viruses, code injections, and other malware that can alter the functionality of systems.

	Security measures	Evidence
1	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls. b) Check for malware on (internal) network and information systems.	i. Software and data in network and information systems is protected using input controls, firewalls, encryption and signing. ii. Malware detection systems are present, and up to date.
2	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems. d) Apply reinforced software integrity, update and patch management controls for critical assets in virtualised networks.	iii. Documentation about how the protection of software and data in network and information system is implemented. iv. Tools for detection of anomalous usage of systems or anomalous behaviour of systems (such as intrusion detection and anomaly detection systems). v. Logs of intrusion detection and anomaly detection systems. vi. Adequate tools and processes to ensure software integrity when performing software updates and applying security patches to critical assets in virtualised networks.
3	e) Set up state of the art controls to protect integrity of systems. f) Evaluate and review the effectiveness of measures to protect integrity of systems.	vii. State of the art controls to protect integrity of systems, such as code signing, tripwire, etc. viii. Documentation of process for checking logs of anomaly and intrusion detection systems.

3.5. SO13: Use of encryption

Ensure adequate use of encryption to prevent and/or minimise the impact of security incidents on users and on other networks and services.

	Security measures	Evidence
1	a) Where appropriate to prevent and/or minimise the impact of security incidents on users and on other networks and services, encrypt data during its storage in and/or transmission via networks.	i. Description of main data flows, and the encryption protocols and algorithms used for each flow. ii. Description of justified exclusions and limitations in implementing encryption.

2	b) Implement encryption policy. c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys.	iii. Documented encryption policy including details about the cryptographic algorithms and corresponding cryptographic keys, according to international best practices and standards. iv. Documented justified exclusions that provide rationale for when data is not encrypted, including the related impact assessment.
3	d) Review and update the encryption policy. e) Use state of the art encryption algorithms.	v. Updated encryption policy, review comments and/or change logs. vi. Encryption policy includes details about the state of the art cryptographic protocols used.

3.6. SO14: Protection of security critical data

Ensure that cryptographic key material and secret authentication information are adequately protected.

	Security measures	Evidence
1	a) Make sure that cryptographic key material and secret authentication information (including cryptographic key material used for authentication) are not disclosed or tampered with. b) Access to private keys is strictly controlled and monitored.	i. Cryptographic key material and secret authentication information are protected using security best practices and standards for protection mechanisms (like split knowledge and dual control, encryption, hashing, secure hardware etc.). ii. Description of mechanisms for controlling and monitoring access to private keys.
2	c) Implement policy for management of cryptographic keys. d) Implement policy for management of user passwords.	iii. Key management policy including roles, responsibilities and controls for the use, protection and lifetime of cryptographic keys throughout their life cycle including controls for access to and backup and recovery of private keys. iv. User password management policy including processes, methods and techniques for secure storing of user passwords using industry best practices.
3	e) Review and update of key management policy. f) Review and update of user password management policy.	v. Updated key management policy, review comments and/or change logs. vi. Updated user password management policy, review comments and/or change logs.

4. D4: Operations management

The domain "Operations management" covers operational procedures, change management and asset management.

4.1. SO15: Operational procedures

Establish and maintain operational procedures for the operation of critical network and information systems by personnel.

	Security measures	Evidence
1	a) Set up operational procedures and assign responsibilities for operation of critical systems.	i. Documentation of operational procedures and responsibilities for key network and information systems.
2	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures.	ii. Documented policy for operation of critical systems, including an overview of network and information systems in scope.
3	c) Review and update the policy/procedures for operation of critical systems, taking into account incidents and/or changes.	iii. Updated policy/procedures for critical systems, review comments and/or change logs.

4.2. SO16: Change management

Establish change management procedures for critical network and information systems in order to minimise the likelihood of incidents resulting from changes.

	Security measures	Evidence
1	a) Follow predefined methods or procedures when making changes to critical systems	i. Documentation describing predefined methods or procedures followed when making changes to critical systems.
2	b) Implement policy/procedures for change management, to make sure that changes of critical systems are always done following a predefined way. c) Document change management procedures, and record for each change the steps of the followed procedure.	ii. Documentation of change management policy/procedures, including systems subject to the policy, objectives, roll back procedures, etc. iii. For each change, a report is available describing the steps and the result of the change.
3	d) Review and update change management procedures regularly, taking into account changes and past incidents.	iv. Up to date change management procedures, review comments and/or change logs.

4.3. SO17: Asset management

Establish and maintain asset management procedures and configuration controls in order to manage availability of critical assets and configurations of critical network and information systems.

	Security measures	Evidence
1	a) Identify critical assets and configurations of critical systems.	i. List of critical assets and critical systems. The list should include all critical assets and critical systems for network or service, operational and security, including relevant third party assets.
2	b) Implement policy/procedures for asset management and configuration control.	ii. Documented policy/procedures for asset management, including roles and responsibilities, the assets and configurations that are subject to the policy, the objectives of asset management. iii. An asset inventory or inventories, containing critical assets and the dependency between assets. iv. A configuration control inventory or inventories, containing configurations of critical systems.
3	c) Review and update the asset management policy regularly, based on changes and past incidents.	v. Up to date asset management policy/procedures, review comments and/or change logs.

5. D5: Incident management

The domain "Incident management" covers detection of, response to, incident reporting, and communication about incidents.

5.1. SO18: Incident management procedures

Establish and maintain procedures for managing incidents, and forwarding them to the appropriate personnel (triage).

	Security measures	Evidence
1	a) Make sure personnel is available and prepared to manage and handle incidents. b) Keep a record of all major incidents.	i. Personnel is aware of how to deal with incidents and when to escalate. ii. Inventory of major incidents per incident, impact, cause, actions taken and lessons learnt.
2	c) Implement policy/procedures for managing incidents.	iii. Policy/procedures for incident management, including, types of incidents that could occur, objectives, roles and responsibilities, detailed description, per incident type, how to manage the incident, when to escalate to senior management (e.g. CISO) etc.
3	d) Investigate major incidents and draft final incident reports, including actions taken and recommendations to mitigate future occurrence of this type of incident. e) Evaluate incident management policy/procedures based on past incidents.	iv. Individual reports of the handling of major incidents. v. Up to date incident management policy/procedures, review comments and/or change logs.

5.2. SO19: Incident detection capability

Establish and maintain an incident detection capability that detects incidents.

	Security measures	Evidence
1	a) Set up processes or systems for incident detection.	i. Documented examples of past incidents that were detected and timely forwarded to the appropriate people.
2	b) Implement industry standard systems and procedures for incident detection. c) Implement systems and procedures for registering and forwarding incidents timely to the appropriate people.	ii. Incident detection systems and procedures, such as Security Incident and Event Management (SIEM) tools, security helpdesk for personnel, reports and advisories from Computer Emergency Response Teams (CERTs), tools to spot anomalies, etc. iii. Network Operation Centres (NOC) and/or Security Operation Centres (SOC) for ensuring visibility and effective network monitoring and to detect anomalies and to identify and avoid threats.
3	d) Review systems and processes for incident detection regularly and update them taking into account changes and past incidents. e) Implement state of the art systems and procedures for incident detection.	iv. Up to date documentation of incident detection systems and processes. v. Documentation of review of the incident detection process, review comments, and/or change logs. vi. NOC/SOC solutions with state of the art capabilities are used - e.g. SOAR (Security Orchestration, Automation and Response), ensuring integration with threat and vulnerability management and incident response function, security operations automation etc.

5.3. SO20: Incident reporting and communication

Establish and maintain appropriate incident reporting and communication procedures, taking into account national legislation on incident reporting to government authorities.

	Security measures	Evidence
1	a) Communicate and report about on-going or past incidents to third parties, customers, and/or government authorities, when necessary.	i. Evidence of past communications and incident reporting.
2	b) Implement policy and procedures for communicating and reporting about incidents.	ii. Documented policy and procedures for communicating and reporting about incidents, describing reasons/motivations for communicating or reporting (business reasons, legal reasons etc.), the type of incidents in scope, the required content of communications, notifications or reports, the channels to be used, and the roles responsible for communicating, notifying and reporting. iii. Templates for incident reporting and communication.
3	c) Evaluate past communications and reporting about incidents. d) Review and update the reporting and communication plans, based on changes or past incidents.	iv. List of incident reports and past communications about incidents. v. Up to date incident response and communication policy, review comments, and/or change logs.

6. D6: Business continuity management

The domain "Business continuity management" covers continuity strategies and contingency plans to mitigate major failures and natural or man-made disasters.

6.1. SO21: Service continuity strategy and contingency plans

Establish and maintain contingency plans and a strategy for ensuring continuity of networks and communication services provided.

	Security measures	Evidence
1	a) Implement a service continuity strategy for the communications networks and/or services provided.	i. Documented service continuity strategy, including recovery time objectives for key services and processes
2	b) Implement contingency plans for critical systems. c) Monitor activation and execution of contingency plans, registering successful and failed recovery times. d) Implement contingency plans for dependent and inter-dependent critical sectors and services.	ii. Contingency plans for critical systems, including clear steps and procedures for common threats, triggers for activation, steps and recovery time objectives. iii. Decision process for activating contingency plans. iv. Logs of activation and execution of contingency plans, including decisions taken, steps followed, final recovery time. v. Map of critical sectors and services essential for and/or dependent on the continuity of the network and service operation and contingency plans for mitigating the impact related to dependent and interdependent sectors and services.
3	e) Review and revise service continuity strategy periodically. f) Review and revise contingency plans, based on past incidents and changes.	vi. Up to date continuity strategy and contingency plans, review comments, and/or change logs.

6.2. SO22: Disaster recovery capabilities

Establish and maintain an appropriate disaster recovery capability for restoring network and communication services in case of natural and/or major disasters.

	Security measures	Evidence
1	a) Prepare for recovery and restoration of services following disasters.	i. Measures are in place for dealing with disasters, such as failover sites in other regions, backups of critical data to remote locations, etc.
2	b) Implement policy/procedures for deploying disaster recovery capabilities. c) Implement industry standard disaster recovery capabilities, or be assured they are available from third parties (such as national emergency networks).	ii. Documented policy/procedures for deploying disaster recovery capabilities, including list of natural and/or major disasters that could affect the services, and a list of disaster recovery capabilities (either those available internally or provided by third parties). iii. Industry standard implementation of disaster capabilities, such as mobile equipment, mobile sites, failover sites, etc.
3	d) Set up state of the art disaster recovery capabilities to mitigate natural and/major disasters. e) Review and update disaster recovery capabilities regularly, taking into account changes, past incidents, and results of tests and exercises.	iv. State of the art disaster recovery capabilities, such as full redundancy and failover mechanisms to handle natural and/or major disasters. v. Updated documentation of disaster recovery capabilities in place, review comments and/or change logs

7. D7: Monitoring, auditing and testing

The domain "Monitoring, auditing and testing" covers monitoring, testing and auditing of network and information systems and facilities.

7.1. SO23: Monitoring and logging policies

Establish and maintain systems and functions for monitoring and logging of relevant security events in critical network and communication systems.

	Security measures	Evidence
1	a) Implement monitoring and logging of critical systems.	i. Logs and monitoring reports of critical network and information systems.
2	b) Implement policy for logging and monitoring of critical systems. c) Set up tools for monitoring critical systems d) Set up tools to collect and store logs of critical systems.	ii. Documented policy for monitoring and logging, including minimum monitoring and logging requirements, retention period, and the overall objectives of storing monitoring data and logs. iii. Tools for monitoring systems and collecting logs. iv. List of monitoring data and log files, in line with the policy.
3	e) Set up tools for automated collection and analysis of monitoring data and logs. f) Review and update logging and monitoring policy/procedures, taking into account changes and past incidents.	v. Tools to facilitate structural recording and analysis of monitoring and logs. vi. Updated documentation of monitoring and logging policy/procedures, review comments, and/or change logs.

7.2. SO24: Exercise contingency plans

Establish and maintain policies for testing and exercising backup and contingency plans, where needed in collaboration with third parties.

	Security measures	Evidence
1	a) Exercise and test backup and contingency plans to make sure systems and processes work and personnel is prepared for large failures and contingencies.	i. Reports of past exercises of backup and contingency plans.
2	b) Implement a program for exercising backup and contingency plans regularly, using realistic scenarios covering a range of different scenarios over time. c) Make sure that the issues and lessons learnt from exercises are addressed by the responsible people and that the relevant processes and systems are updated accordingly.	ii. Exercise program for backup and contingency plans, including types of contingencies, frequency, roles and responsibilities, templates and procedures for conducting exercises, templates for exercise reports. iii. Reports about exercises and drills showing the execution of contingency plans, including lessons learnt from the exercises. iv. Issues and lessons learnt from past exercises have been addressed by the responsible people
3	d) Review and update the exercise plans, taking into account changes, past incidents and contingencies which were not covered by the exercise program. e) Involve suppliers and other third parties in exercises, for example business partners and customers.	v. Updated exercise plans, review comments, and/or change logs. vi. Input from suppliers and other third parties involved about how to improve exercise scenarios.

7.3. SO25: Network and information systems testing

Establish and maintain policies for testing network and information systems, particularly when connecting to new networks or systems.

	Security measures	Evidence
1	a) Test networks and information systems before using them or connecting them to existing systems.	i. Test reports of the network and information systems, including tests after big changes or the introduction of new systems.
2	b) Implement policy/procedures for testing network and information systems. c) Implement tools for automated testing.	ii. Policy/procedures for testing networks and information systems, including when tests must be carried out, test plans, test cases, test report templates.
3	d) Review and update the policy/procedures for testing, taking into account changes and past incidents.	iii. List of test reports. iv. Updated policy/procedures for testing networks and information systems, review comments, and/or change log.

7.4. SO26: Security assessments

Establish and maintain an appropriate policy for performing security assessments of network and information systems.

	Security measures	Evidence
1	a) Ensure critical systems undergo security scans and security testing regularly, particularly when new systems are introduced and following changes.	i. Reports from past security scans and security tests.
2	b) Implement policy/procedures for security assessments and security testing.	ii. Documented policy/procedures for security assessments and security testing, including, which assets, in what circumstances, the type of security assessments and tests, frequency, approved parties (internal or external), confidentiality levels for assessment, test results and the objectives of security assessments and tests.
3	c) Evaluate the effectiveness of policy/procedures for security assessments and security testing. d) Review and update policy/procedures for security assessments and security testing, taking into account changes and past incidents.	iii. List of reports about security assessments and security tests. iv. Reports of follow up actions on assessments and test results. v. Up to date policy/procedures for security assessments and security testing, review comments, and/or change log.

7.5. SO27: Compliance monitoring

Establish and maintain a policy for monitoring compliance to standards and legal requirements.

	Security measures	Evidence
1	a) Monitor compliance to standards and legal requirements.	i. Reports describing the result of compliance monitoring.
2	b) Implement policy/procedures for compliance monitoring and auditing.	ii. Documented policy/procedures for monitoring compliance and auditing, including what (assets, processes, infrastructure), frequency, guidelines who should carry out audits (in- or external), relevant security policies that are subject to compliance monitoring and auditing, the objectives and high level approach of compliance monitoring and auditing, templates for audit reports. iii. Detailed monitoring and audit plans, including long term high level objectives and planning
3	c) Evaluate the policy/procedures for compliance and auditing. d) Review and update the policy/procedures for compliance and auditing, taking into account changes and past incidents.	iv. List of all compliance and audit reports v. Updated policy/procedures for compliance and auditing, review comments, and/or change logs.

8. D8: Threat awareness

The domain "Threat awareness" covers security objectives related to threat intelligence and to outreach to end-users for the purpose of sharing the information about major threats to the security of networks and services.

8.1. SO28: Threat intelligence

Establish and maintain appropriate mechanisms for monitoring and collecting information about relevant threats to the security of networks and services.

	Security measures	Evidence
1	a) Perform regular threat monitoring.	i. Regular monitoring of external threat intelligence feeds (OSINT, commercial feeds, security researches etc.) with a recorded log of relevant significant threat events. ii. Informal and ad-hoc sharing of relevant threat intelligence with relevant organisations on bilateral basis.
2	b) Implement threat intelligence program.	iii. Documented and implemented threat intelligence program that includes roles, responsibilities, procedures and mechanisms for collecting information related to significant threats and corresponding mitigation measures. iv. The program also includes mechanisms for systematic sharing of threat intelligence with relevant organisations on bilateral and multilateral basis using a dedicated threat intelligence sharing platform (e.g. MISP). v. Appropriate information marking scheme in place for facilitation of sharing of sensitive threat information (e.g. TLP).
3	c) Review and update the threat intelligence program. d) Threat intelligence program makes use of state of the art threat intelligence systems.	vi. Updated threat intelligence program, review comments and/or change logs. vii. Threat intelligence platform (TIP) with state of the art functionality is used (e.g. consolidation of threat intelligence feeds from various sources, automation, security analytics and integration with other security tools etc.)

8.2. SO29: Informing users about threats

Inform users of particular and significant security threats to network or service that may affect the end-user and of the measures they can take to protect the security of their communications.

	Security measures	Evidence
1	a) Inform end-users of communication networks and services about particular and significant security threats to network or service that may affect them.	i. Security bulletin, a dedicated threat information web page or another documented and tested mechanism for reaching out to end-users in case of significant threats. ii. Documented lists of best practices and security recommendations for end-users to mitigate typical risks (e.g. encryption, strong authentication, updates, backups, user awareness etc.).
2	b) Implement policy/procedures for regular update of end-users about security threats to network or service that may affect them.	iii. Documented and implemented end-user outreach policy with defined roles and responsibilities, mechanisms and criteria for identifying significant threats and procedures, tools and methods for timely and appropriate informing of end-users. iv. The policy includes mechanisms for identifying and sharing recommendations and best practices for end-users to mitigate specific threats.
3	c) Review and update the policy/procedures for regular update of end-users about security threats to network or service that may affect them.	v. Updated outreach policy, review comments and/or change logs.