هيئة تنظيم الاتصالات
TELECOMMUNICATIONS REGULATORY AUTHORITY
Kingdom of Bahrain - مملكة البحرين

Guidelines issued by the Telecommunications Regulatory Authority on Telecommunications Sector Cybersecurity Controls

Date: 5 December 2024
Ref: LAD 1124 068

Purpose: To establish a baseline set of security measures and best practices for the telecommunications industry to protect against cyber and physical threats. These guidelines aim to enhance the overall security posture of the telecommunications sector and ensure the resilience of critical telecommunications infrastructure. By providing a common framework, the guidelines can help organizations in the telecommunications industry implement effective security controls and mitigate cyber and physical risks.

Introduction

The telecommunication sector provides important services which allow everyone to communicate locally and internationally. Internet access is possible because of the telecommunication sector. By developing the telecommunication cybersecurity controls, the TRA[1] aims at protecting the sector which forms part of the Critical National Infrastructure (CNI) from any cybersecurity threats and attacks.

The purpose of these guidelines and the controls within is to provide guidance and recommendations to telecommunication entities to have a robust cybersecurity. The document outlines best practices to be implemented in the following domains:

1. **IT Cybersecurity Governance;**
2. **Cyber Defense;**
3. **Cybersecurity Assessment, Audit and Third Party Cyber Risk Management;**
4. **Cybersecurity Operations and Incident Management;**
5. **Generally Applicable Telecoms Security Controls;**
6. **Peering and Interconnection; and**
7. **National Infrastructure and Services.**

While these Guidelines are currently not binding, they are intended to help telecommunication entities align with industry standards and regulatory expectations. The TRA reserves its right to revisit and amend these Guidelines as necessary to ensure they remain effective and relevant in addressing evolving cybersecurity challenges within the sector.

Abbreviations and Terminology

Throughout this document many abbreviations are used, as it is intended to be digested by a technical audience. Please see appendix A for a glossary of abbreviations and acronyms.

Within this document, we use the term “entities” to refer generally, but not exclusively, to organizations regulated under the Telecommunications Law who fall within the intended scope of this framework. As the framework is intended to help encourage cybersecurity hygiene and resiliency more broadly across the entire telecommunications sector of the Kingdom of Bahrain, these controls may also be beneficial to entities outside the explicit scope of the Telecommunications Law.

[1] These controls were developed in cooperation with the National Cyber Security Center

Domain 1 IT Security Governance

This section of Domains 1 through 4 includes security controls broadly applicable across both a licensee's enterprise and telecommunications infrastructure. These controls are not necessarily technical in nature, and include a variety of governance, management, and communications activities related to managing cybersecurity risk.

This domain aims to ensure that entities define the essential elements for effective governance and oversight of their organizational cyber risk management. These elements include clear definitions of organizational risk thresholds and tolerances, an accountability structure, and clear areas of responsibility.

Subdomain 1.1 Roles and Responsibilities

This subdomain establishes responsibilities for key strategic decision making relating to cybersecurity, sets a requirement to disseminate information to those who need to know it, and ensures that the plan is regularly reviewed. Defining these responsibilities ensures accountability for key tasks.

Control 1.1.1 The Board of Directors is responsible for cybersecurity and must exercise oversight of an entity's cybersecurity program by ensuring that the entity's cybersecurity program is appropriately managed and resourced, as well as by endorsing the cybersecurity strategy and policy.

Control 1.1.2 The Board must establish or designate a board-level committee responsible for cybersecurity, including:

- Monitoring, reviewing, and communicating the entity's cybersecurity risk appetite periodically or when there is a major change in the risk appetite.
- Reviewing the entity's cybersecurity strategy on at least an annual basis to ensure that it is well aligned with its risk management and broader business objectives.
- Approving, supporting, and monitoring cybersecurity strategy, cybersecurity policy, cybersecurity risk management process, the key risk indicators, and key performance indicators for cybersecurity.

Control 1.1.3 The entity must designate a senior accountable role for cybersecurity, such as a Chief Information Security Officer. This role must be of sufficient seniority to regularly brief the Board's cybersecurity committee, and to influence and direct enterprise level investments and change.

Control 1.1.4 The entity must establish governance, risk, and compliance functions to formally define, audit, and report on the entity's cybersecurity and risk management programs.

1.1.4.1 Appropriate confidential escalation paths must be established for the reporting of significant information security risks and issues.

1.1.4.2 Regular internal audits and inspections of organizational compliance with security policies must be conducted, with opportunities for improvements formally

catalogued and implementation initiatives tracked and summarized for senior leadership.

Control 1.1.5 An entity's project management methodology must ensure that IT and telecoms infrastructure projects incorporate Secure by Design, Secure by Default, and Privacy by Design principles, and that a security risk assessment is performed before starting any technology related project.

1.1.5.1 The entity must follow a project design process with defined security risk assessment and acceptance stages.

1.1.5.2 The entity must ensure all projects go through a data protection and privacy assessment, aligned to the Guidelines on the Privacy of Individuals and Data Protection in the Telecommunications Sector issued by TRA, the Personal Data Protection Law and requirements of the Personal Data Protection Authority of the Kingdom of Bahrain.

1.1.5.3 Software projects must adhere to principles of the Secure Software Development Lifecycle (SDLC). An entity's SDLC must include quality control stages, and software testing (static or dynamic) as appropriate.

Control 1.1.6 A risk management plan must be implemented by a team specified by the board of directors, using a framework such as the NIST Risk Management Framework, ISO27001 or ISO31000 Series standard. Senior management must approve the plan before implementation and review the plan annually or after a substantial change.

Control 1.1.7 All members of an entity's workforce, including contractors, must be formally advised of and must acknowledge their cybersecurity responsibilities on an annual basis.

Control 1.1.8 Key officers or senior managers accountable for cybersecurity activities must be clearly identified and the board of directors must receive, on an at least annual basis, a briefing on the cybersecurity program's performance, key activities, and intended strategy.

Subdomain 1.2 Cybersecurity Risk Management

Cybersecurity risk management is the process of identifying, assessing, and reducing risks to an acceptable level. This process is considered the basis for determining the necessary controls to treat cybersecurity risks and establish a contingency plan. Ultimately, to reduce the cybersecurity risks for the information assets, the risks' impact, likelihood, and vulnerability must be accurately identified, assessed, and analyzed. A comprehensive cybersecurity risk management plan must be developed.

Control 1.2.1 The entity must develop a comprehensive plan that clarifies the scope and boundaries of the cybersecurity risk management process determining the business areas, people covered in the plan and allocated recourses with consideration of risk appetite.

Control 1.2.2 Risk management activities must be overseen by a committee, or any team specified by the Board of Directors, based on the NIST Cybersecurity Framework, ISO27001 or ISO31000 Series standard.

Control 1.2.3 The plan must identify the details of the cybersecurity risk management process including risk identification, risk analysis, risk treatment, and risk monitoring along with roles and responsibilities, organizational structure, and charters.

Control 1.2.4 Senior management must approve the plan before implementation and review the plan periodically and after a major change is made to the plan.

Control 1.2.5 Senior management must ensure implementation and effectiveness of the risk management process and risk treatment plan which includes the board of directors' review and approval of the cybersecurity risk assessment results.

Control 1.2.6 The identified risks must be communicated to relevant risk owners for their endorsement. Risk owners must identify or support the identification of risk treatment decisions.

Control 1.2.7 The entity shall maintain the risk register that records risk rating, prioritize risks for treatment and identifies risks that are within the entity's risk tolerance and reviewed periodically.

Control 1.2.8 The entity must monitor and communicate cybersecurity risks as well as review the risk register periodically.

Subdomain 1.3 Strategies, Policies, and Procedures

This subdomain aims to ensure that all cybersecurity strategies, policies, and procedures are well organized, governed, and documented. The strategies include addressing clearly the cybersecurity goals the entity is willing to achieve. The policies and procedures must be defined, approved, and reviewed at least once every year to ensure achieving the entity's objectives.

Control 1.3.1 The cybersecurity strategy must contain: the importance and benefits of cybersecurity to the entity, the cybersecurity objectives to be achieved, the difficulties that may occur, the cybersecurity initiatives, and projects to achieve the cybersecurity objectives.

Control 1.3.2 Entities must have an information security policy, or a suite of policies, governing implementation of the cybersecurity strategy and explicitly defining more granular control objectives and recommended implementation patterns. These policies must be available in written form, formally approved by leaders who have ownership over the cybersecurity strategy and publicized to an entity's workforce. They must also be reviewed and updated periodically.

Control 1.3.3 The Board of Directors, cybersecurity committee, or identified deputies must review the cybersecurity strategy and policy at least once every year.

Control 1.3.4 The entity must ensure that its information security policy sets out handling procedures for its workforce which clarify how information at different classification levels must be handled.

Subdomain 1.4 Asset Management

One of the core subdomains of cybersecurity governance is asset management. Identifying and maintaining the information assets is important to protect the entity's information infrastructure. Information assets include hardware, software, information systems, information services, virtualization, and information stored on-prem or elsewhere.

Control 1.4.1 The entity must define, approve, and implement an asset management process which governs the entire lifecycle of the asset, including its eventual disposal. The process must be monitored and measured on a regular basis.

Control 1.4.2 Automated asset discovery tools are highly recommended to be used to identify assets when they are introduced and periodically validated.

Control 1.4.3 Assets must be identified, classified, prioritized, and maintained in a centralized asset inventory that is periodically reviewed and updated.

Control 1.4.4 All information stored on-premises or elsewhere must be classified based on an entity's information management policies and the classification must be reviewed periodically.

Control 1.4.5 All assets must be labeled with a unique identifier in accordance with their asset classification.

Control 1.4.6 Asset details must be recorded such as, but not limited to, asset identifier, asset name or description, asset function, asset classification, asset owner, asset custodian, asset users, physical asset location, license details, and asset severity.

Control 1.4.7 Asset maintenance must be recorded, with the date/time conducted, person completing the maintenance, person completing the record, short summary of actions, and any other details the entity deems sufficient for auditing purposes.

Control 1.4.8 All assets must be sufficiently protected against loss, theft, unauthorized access, and/or unauthorized disclosure in line with their classification level.

Control 1.4.9 Users must only use authorized devices with an endpoint protection solution deployed that comprises anti-virus, anti-malware, Endpoint Detection and Response (EDR), Extended Detect and Response (XDR), device management and control, host firewall, and HIPS or any other solutions recommended or applicable and approved by NCSC.

Control 1.4.10 To minimize the risk of confidential information leakage to unauthorized persons, formal procedures for the secure disposal of information and assets must be established, including the proper steps for asset disposal.

Control 1.4.11 Systems and devices that are known or suspected to have been exploited, compromised, or over which control has otherwise been lost must be isolated and subsequently evaluated before being returned to operational use.

Subdomain 1.5 Change Management

Change management involves planning, implementing, and reviewing information system changes to minimize risks and disruptions. The objective of this subdomain is to ensure entities have a consistent and systematic approach to proposing, approving, and documenting changes to security and IT infrastructure. Effective change management helps enhance the resiliency of critical systems and can be essential to diagnosing and resolving unintended system outages and breaches.

Control 1.5.1 A change management process must be established to ensure that changes to information assets are planned, evaluated, reviewed, and approved before implementation. Organizational compliance with change management process must be monitored and unauthorized changes to critical systems must be investigated.

Control 1.5.2 An entity's change management process and documentation must consider potential requirements related to controlling changes of and impacts on cybersecurity policies and controls.

Control 1.5.3 Where feasible, changes must be tested in a separate environment based on test plans approved by business and IT management.

Control 1.5.4 Test results must be reviewed and accepted by authorized personnel before the changes are approved to ensure there is appropriate oversight and review.

Control 1.5.5 Tests must not use production data which may contain personal or confidential information.

Control 1.5.6 Changes must include a rollback plan to ensure that systems can be restored to full capacity as rapidly as possible in the event of a failed change.

Control 1.5.7 Procedures must be defined for assessing, approving, and implementing urgent or emergency changes that need to be implemented without following the standard change management process. These procedures must designate multiple redundant approval personnel so that critical changes can be made even during periods of reduced organizational availability, such as holidays or vacation periods.

Control 1.5.8 As soon as possible, emergency changes must be documented and reviewed in accordance with the standard change management process. Emergency changes must also be assessed to ensure that any temporary accesses, bypasses, or circumventions of cybersecurity controls have been reverted.

Subdomain 1.6 Business Continuity Management

BCM is an act of proactively anticipating and minimizing impacts on mission-critical operations, services, functions, and processes of the entity and ensuring their availability to enhance overall business resilience. BCM also includes efforts to a wide variety of risks.

Control 1.6.1 Comprehensive BCM plans must be prepared to cover a wide range of risks and in consideration of the organization's risk appetites to various lines of business and assets. These plans must describe essential business continuity measures and critical resources. The

overall BCM program must be approved and periodically reviewed by the Board of Directors or delegated senior management.

Control 1.6.2 The plan must include all steps involved in response to disasters to protect the information assets and restore critical business functions and services.

Control 1.6.3 BCM plans must also specify when and how to perform critical and mandatory notifications to insurance brokers, regulators, and other essential third parties in the event of a major disaster.

Control 1.6.4 A business impact analysis must be performed to prioritize the protection and ensure the availability of services. The results of business impact analysis must be reviewed regularly or when there is an effective change.

Control 1.6.5 Effective crisis communications capabilities must be established to ensure that critical messaging and status updates can be prepared and conveyed to internal team members, customers, citizens, and institutions of the Kingdom of Bahrain.

Control 1.6.6 Out-of-band backup communications capabilities must be established so that BCM tasks can be performed even in the event of a significant outage of the conventional enterprise email, voice, or messaging capabilities.

Control 1.6.7 The entity must ensure that the required resources to deliver essential services and business functions are adequate to maintain availability in a disaster.

Control 1.6.8 A DR plan must be developed and implemented which determines the frequency of data backup including offline backup, the acceptable recovery time, the responsible employees to handle the recovery process steps, RTO and RPO.

Control 1.6.9 The plans for business continuity and disaster recovery must be reviewed at least annually or after major organizational or infrastructure changes to identify any weaknesses or gaps.

Control 1.6.10 A test plan must be developed to test the plans of business continuity and disaster recovery. The plan must include the test scope and objectives, test scenarios and the details related to the test activities performed.

Control 1.6.11 Testing the plans must involve all teams necessary to execute the BCM plan and not be unnecessarily limited to cybersecurity or IT staff.

Control 1.6.12 Offline copies of BCM and DR plans must be available at the main site and at the DR site to be reached if an incident prevents access to their primary copies.

Subdomain 1.7 Cybersecurity Awareness and Training

This subdomain ensures that the workforce of an entity (including contractors and third parties) are provided with the awareness, knowledge, and skills to carry out their organizational responsibilities safely and utilize organizational systems and infrastructure in compliance with the entity's cybersecurity policies.

Control 1.7.1 All users must be informed of and acknowledge their responsibilities for cybersecurity and provided with adequate training on how to use systems and applications in compliance with the organization's security policies on an annual basis.

1.7.1.1 Completion of the relevant information and training programs must be documented, tracked, and managed organizationally. Supervisors, managers, and leaders must be accountable for their subordinates' completion of the awareness and training program.

1.7.1.2 Employee cybersecurity training must be integrated with an entity's onboarding process so that essential training on security policies and responsibilities is delivered on a timely basis as new employees are granted access.

Control 1.7.2 Different awareness and training programs must be tailored to various organizational job levels and roles.

1.7.2.1 Privileged users must understand and acknowledge additional cybersecurity requirements related to the use and safeguarding of their privileged accounts.

1.7.2.2 Senior leaders and executives with key cybersecurity roles and responsibilities must understand and acknowledge these.

1.7.2.3 Contractors, suppliers, and other third parties acting as an extension of an entity's workforce must receive awareness and training on their cybersecurity responsibilities and obligations as part of an entity's contracting and procurement process.

Control 1.7.3 Performance metrics on the organization's cybersecurity training and awareness program must be annually evaluated and reviewed by senior management and the Board of Directors to ensure that the program is achieving its objectives and improving behaviors.

Control 1.7.4 Cybersecurity training and awareness program content must be reviewed at least annually to assess new cybersecurity trends and developments, make necessary updates, and ensure that the material remains engaging and relevant to its audience.

Control 1.7.5 Warning banners must appear prior to system login where possible, which specify requirements for accessing the system and penalties for improper use.

Domain 2 Cyber Defense

The scope of this domain is to address cybersecurity defense processes to ensure they effectively protect an entity's networks, systems, applications, and IT services. This domain defines and describes many processes in six subdomains: Identity and Access Management, Network Security, Email Protection, Cryptography, Physical and Environmental Security and Social Media Cybersecurity.

Subdomain 2.1 Identity and Access Management

This subdomain identifies controls to ensure that access to physical and logical assets and related facilities is limited to authorized users, systems, and processes and that these identities are subjected to appropriate verification in relation to the assets being accessed.

Control 2.1.1 Identity and Access Management (IAM) policies, including user registration and revoking procedures, and processes must be formally defined, documented, approved, reviewed, and audited on a periodic basis.

Control 2.1.2 The approval, provisioning, and use of administrator, superuser, or other privileged accounts must be governed by a policy setting out additional appropriate security controls such as MFA and PIM and designating personnel who will approve, periodically revalidate, and be accountable for requests for such accounts.

2.1.2.1 Where feasible, administrative, or privileged system activities must be conducted only from dedicated management devices which are built from known and trusted operating system images, rather than OEM or ad hoc operating system images.

2.1.2.2 The entity must manage and control privileged access to information systems, using solutions such as a Privileged Identity Management (PIM) or a Privileged Access Management (PAM) system.

2.1.2.3 Local, off-domain administrator or privileged accounts must be present only where strictly necessary and otherwise unavoidable.

2.1.2.4 For high priority systems, where third parties are making changes with high privilege accounts, explicit approval must be provided through the use of process or technologies such as split passwords.

2.1.2.5 Privileged accounts must not be used to perform regular user activities such as reading emails, viewing attachments, or web browsing.

Control 2.1.3 Default operating system and application accounts must be disabled, renamed, and have their credentials changed where possible.

Control 2.1.4 Users must not share their account information and must not share accounts with other users.

Control 2.1.5 Access to networks, systems, and applications by systems and employees must be:

- Requested, reviewed, approved, implemented, and verified in accordance with business needs and cybersecurity requirements.

- Reviewed by the owners or administrators of networks, systems, and applications and access must only be granted after having appropriate approval.

- Maintained to help the entity in identifying and recording all access rights granted to the networks, systems, and applications.

Control 2.1.6 Service, system, or other automated agent accounts must be requested, authorized, and periodically reviewed. Privileges of these accounts must not exceed those of the requestor or accountable account owner.

2.1.6.1 Where possible, API keys and authentication tokens must be stored in a secrets vault, rotated periodically, and scoped to authorized origin IP addresses or networks.

2.1.6.2 The activities and use of API keys and authentication tokens must be logged and audited.

2.1.6.3 Secrets must not be stored in clear text within public or shared code repositories.

Control 2.1.7 The access to networks, systems, and applications must be restricted and granted based on identity and access control principles, including the following:

- Need-to-Know Principle: granting access to users whose job duties, roles, and responsibilities involve the need to access and use data or information in accordance with the Need-to-Know principle. Otherwise, the request must be rejected, and access must not be granted.

- Least Privilege Principle: assigning a user, system, or process with the least privileges needed to do the necessary activities/actions based on the user's role and duties.

- Segregation of Duties Principle: The entity must consider the conflicting roles (for example, Requestor and approver roles or checker and maker roles) and shall segregate them to ensure that no individual has access to control all phases of an operation/process.

Control 2.1.8 MFA must be an entity's default authentication standard and enabled wherever possible.

2.1.8.1 The use of SMS as an authentication factor must be avoided if possible.

Control 2.1.9 An entity's security policies must set out requirements for the provisioning, use, and management of passwords.

2.1.9.1 Passwords/passphrases that are set or reset on users' behalf must be randomly generated and must be changed after first access by the user.

2.1.9.2 Server-side passwords and credentials stored in system databases must be hashed and salted where possible, using OWASP best practices as a guideline.

2.1.9.3 Passwords/passphrases must be changed when they are directly compromised or suspected of being compromised, found in databases of an online stored data breach, or found to be stored in the clear on a network or transferred in the clear across a network.

Control 2.1.10 Accounts must be disabled after a specified threshold of failed login attempts.

Control 2.1.11 Authentication via insecure or vulnerable protocols, including outdated or obsolete encryption parameters, must be blocked or disabled.

Control 2.1.12 Employee separations from an entity must be documented, and related user accounts must be disabled or deleted once a separation has taken effect.

Subdomain 2.2 Network Security

The objective of cybersecurity in the communication subdomain is to assure network protection against all threats and risks.

Control 2.2.1 An entity's networks must conform with a formally documented network security architecture that specifies the intended use, operating parameters and security requirements of networks and network segments.

Control 2.2.2 Vulnerable or end-of-life systems that cannot be patched, replaced, or decommissioned must be isolated within a network enclave that has the minimum inbound and outbound access required to maintain the required system functions and whose traffic is monitored.

Control 2.2.3 Sensitive details and documentation about an entity's security controls and network configuration, such as system names, network topology, network device types, or account names must not be publicly accessible.

Control 2.2.4 Ingress and egress traffic from the entity to other networks and vice-versa must pass through appropriate security and inspection capabilities, such as firewall, IPS, IDS, WAF, or proxy.

Control 2.2.5 The entity's network must be scanned regularly to monitor and identify significant network changes such as new IP addresses, new network ports, new reachable subnets.

Control 2.2.6 The configurations of network security devices and information systems used by the entity must be backed-up periodically.

Control 2.2.7 The network security systems and solutions must be upgraded with the necessary modules to assure optimal firewall performance. The firewall administrator must be aware of any hardware and software bugs, as well as firewall software upgrades that are issued by the vendor.

Control 2.2.8 Any remote access to the entity's network must use secure connections such as a VPN.

Control 2.2.9 Entities must move towards zero-trust architectures in existing corporate networks such as IT, Finance, HR, Legal, etc., except the service-provider platform that is used to serve the end user.

Control 2.2.10 Where possible and applicable, the use of SD-WAN and SD-LAN technologies must be used to:

- Enable intent-based networking, and policy-based automation.
- Provide end-to-end secure segmentation of users, device, and applications.
- Cover both wired and wireless enterprise networks.
- Have the capability to deploy access control and ensure continuous compliance by monitoring it actively.

Subdomain 2.3 Enterprise Email Protection

This subdomain ensures that proper controls are in place to minimize the risks associated with email services, servers, and applications.

Control 2.3.1 Secure Email Gateway (SEG) functionality must be used to protect the entity from email attacks. This may be implemented in different ways, such as an on-premises appliance or a cloud-based service.

Control 2.3.2 All emails must be automatically scanned for phishing and spam. The findings and infections must be blocked or quarantined depending on the severity level. The email server administrator has the right to reject any recovery of Infected/Quarantined emails that might compromise the system or network. The source of suspicious emails must be blacklisted.

Control 2.3.3 All files including compressed files sent as attachments in the incoming and outgoing mail (SMTP traffic) must be scanned, any detected malware must be cleaned automatically, and the infected file must be deleted otherwise the email/file must be quarantined.

Control 2.3.4 Email messages must be protected using email filtering solutions and authenticated by enforcing Domain-based Message Authentication, Reporting, and Conformance (DMARC), Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) on inbound and outbound emails.

Subdomain 2.4 Data Security and Encryption

This subdomain sets out controls to prevent unauthorized access, use, modification, or destruction of data. Data security and encryption help to safeguard personal information, sensitive business data, and intellectual property from cyber threats. Effective encryption is also a critical dependency for IAM.

Control 2.4.1 An entity's security policies must specify encryption requirements for different categories of data and information, both while in transit and at rest. These encryption

requirements must consider the confidentiality or sensitivity of the data being transmitted, relevant threat models for the system and data being protected, as well as applicable network or IAM context.

Control 2.4.2 Encryption key management must be consistent with best practices.

Control 2.4.3 Where possible, key material must be managed using a HSM independently certified to standards such as ISO-19790, FIPS, Common Criteria, or PCI-HSM.

Control 2.4.4 Encryption must be based on 3GPP, ISO or NIST-recommended algorithms.

Control 2.4.5 Encryption schemes using Null methods/ciphers must not be used, unless explicitly required (for example, un-authenticated emergency calls in mobility).

Control 2.4.6 In cloud environments, entities must understand where encryption is being provided by a cloud provider and where it is customer-provided. Where feasible, customer-managed keys must be used.

Subdomain 2.5 Physical and Environmental Security

The purpose of this subdomain is to ensure the physical protection of assets, including networks, systems, and applications from unauthorized physical access, loss, theft, and damage, and to reduce the risks of a physical attack being used to disable other security controls or facilitate a logical attack.

Control 2.5.1 Systems and devices must be physically secure from environmental threats. Adequate measures and procedures must be implemented to address and respond to environmental threats including fire, floods, earthquakes, and others.

Control 2.5.2 Network infrastructure and security devices must be physically located in access-controlled and environmentally protected facilities to prevent unauthorized physical access, damage, and interference.

2.5.2.1 Physical access controls to a data center must be consistent with and not more permissive than the logical access controls granted to the infrastructure within that data center.

2.5.2.2 Equipment, such as Wi-Fi access points, which must be located outside of a secure room must be tamper resistant, and physical intrusion must trigger an alert to a monitoring system.

Control 2.5.3 Facilities and equipment installed in physical locations not owned by the entity must be secured in an entity-controlled enclosure or room, monitored, and alarmed in real-time, with a secure management and/or signaling channel.

Control 2.5.4 Environmental controls, including fire, flood, gas and heating, ventilation, and air conditioning (HVAC) systems must be interlinked with monitoring capabilities.

Control 2.5.5 Information assets must be monitored remotely and regularly including using video surveillance to monitor access to critical data centers. This data must be retained for no less than 30 days.

Control 2.5.6 Access to facilities such as data center/server rooms or areas where sensitive information is kept must be restricted using an access control system with multi-factor authentication to prevent any unauthorized physical access. Data center access lists must be logged, reviewed, and maintained daily.

Control 2.5.7 The records of the entrance and exit management systems must be protected. The keys to doors, cabinets, and containers in the data center must be kept safe.

Control 2.5.8 No equipment/media shall be taken off-premises without prior documented authorization, stored in an easily retrievable location such as the asset register.

Subdomain 2.6 Social Media Cybersecurity

Social media applications can create several cybersecurity risks to entities when used in an inappropriate or unsafe manner. Due to their popularity, social media applications are a common way for an adversary to gather information on entities and their employees. When sensitive information is posted to social media, it has the potential to harm the public and the entities' interests. Therefore, entities are required to follow the controls in this subdomain to protect their social media accounts.

Control 2.6.1 The authorized individuals and uses of the entity's social media accounts must be communicated to its workforce.

Control 2.6.2 Only authorized employees must have access to the entity's social media accounts and must be provided with training on their secure use, including management of credentials and authentication factors.

Control 2.6.3 Entities should specify which devices, for example corporate or personal devices, authorized employees may use to access official social media accounts.

Control 2.6.4 An entity's social media accounts must not be configured to automatically sign in.

Control 2.6.5 Employees managing the entity's social media accounts must not share access credentials with anyone except with prior approval of senior management.

Control 2.6.6 MFA must be implemented for access to the entity's social media accounts with a complex password/passphrase where possible.

Control 2.6.7 Employees managing social media accounts must use their official work email address to log in to the social media accounts.

Control 2.6.8 If asked to set up security questions to recover social media accounts, the employee must not provide answers that could be easily obtained from public sources of information. The answers to the security questions must be securely stored with the account credentials and accessible by other authorized personnel such as a manager.

Control 2.6.9 Employees managing social media accounts must not post sensitive information.

Control 2.6.10 Access to an entity's social media accounts must be revoked immediately when there is no longer a requirement for access.

Control 2.6.11 An entity's social media account credentials must be reset upon personal re-positioning, transfer, or termination.

Control 2.6.12 Procedures must be created for managing the social media accounts. The procedure must include managing multi-users for a single account and specifying the roles for writing and approving the posts.

Domain 3 Cybersecurity Assessment, Audit, and Third-Party Cyber Risk Management

Cybersecurity Assessment is a process that enables the discovery of cybersecurity weaknesses in a system. This is essential as the attackers usually exploit a weakness in a system to perform an attack and breach the entity's system. This domain guides entities in performing vulnerability assessment and penetration testing.

Dealing with a third-party brings many threats and risks to the entity especially when third-party is allowed to access the networks, applications, and systems of the entity. To protect the entity from third-party misconduct, this domain includes cybersecurity controls starting from selecting a third party until the termination of the third-party contract.

Subdomain 3.1 Audit

Cybersecurity audits help ensure the performance of cybersecurity controls and an entity's overall cybersecurity strategy by continually reviewing the implementation of these controls, noting improvement opportunities, and ensuring that these opportunities are acted on. Audits help demonstrate compliance with established policies, operational procedures, and relevant standard, legal, and technical requirements.

Control 3.1.1 An entity must have a formalized security audit program which systematically and continually reviews organizational activities for compliance with established policies, contractual requirements, regulations, or legislation.

Control 3.1.2 Audit plans must be established at least annually outlining specific auditing engagements to be carried out over a review period. This plan must be reviewed and approved by the Board of Directors.

Control 3.1.3 Individual audits must have a clear scope, be carried out by auditors who will be able to conduct an impartial and objective review and evaluation and be formally documented in a report with itemized findings, improvement opportunities, and an agreed upon implementation date.

Control 3.1.4 Summarized major findings and the status of improvement opportunities must be briefed to the Board of Directors.

Control 3.1.5 Follow-up audits must be performed to validate that findings have been addressed and committed implementation actions have been carried out.

Control 3.1.6 Entities must perform audits of their partners and third-party suppliers to ensure adherence to contract security clauses.

Subdomain 3.2 Vulnerability Management

A vulnerability is a weakness or flaw in a hardware or software system's design that can be exploited by a threat actor to gain unauthorized access to networks, systems, and applications and conduct malicious activities. These vulnerabilities can be mitigated in various ways, including applying relevant patches, replacing vulnerable products, or isolating vulnerable

systems. This subdomain includes controls to manage this attack surface by effectively identifying and mitigating vulnerabilities.

Control 3.2.1 Vulnerability assessments must be conducted on a regular basis to measure and maintain internal and external baselines of its aggregate exposure to vulnerabilities.

Control 3.2.2 An entity must systematically and on a regular basis measure its exposure to vulnerabilities. This may be accomplished with a variety of automated tools such as vulnerability scanners and attack surface management solutions. These tools may be configured with appropriate credentials to gain access to infrastructure elements to be scanned.

Control 3.2.3 Vulnerability assessments must conform to an entity's change control and change management procedures. They must be planned carefully, with an evaluation of potential adverse impacts on the infrastructure being tested and preparation of any necessary contingency measures.

Control 3.2.4 Where applications or infrastructure are delivered using continuous integration/continuous development (CI/CD) pipelines, vulnerability assessments must be integrated into the pipeline so that the vulnerability exposure level of incremental builds is continuously and systematically evaluated and measured over time.

Control 3.2.5 The vulnerability exposure level of software or firmware components and dependencies must be continuously evaluated. This may be accomplished with a variety of application security testing approaches, including static application software testing (SAST), dynamic application software testing (DAST), and software composition analysis (SCA).

Control 3.2.6 Detected vulnerabilities must be addressed, and corrective action must be performed based on vulnerability classifications and priorities.

Control 3.2.7 An entity's information security policy or policies must set out patch management requirements and guidelines for both scheduled and unscheduled patches or hotfixes. This must include evaluation guidelines and approval personnel for the deployment of emergency patches or hotfixes in the event of a major cyber incident or a zero-day vulnerability.

Control 3.2.8 An entity must have the ability to test and stage patches, hotfixes, and ruleset or signature updates. Ideally, for a given set of users or type of infrastructure, an entity will have identified a subset of elements which can be used to test these elements before deploying them more broadly. Conversely, an entity must also understand where important infrastructure should receive these updates only after they have been tested elsewhere. A variety of mechanisms may be used to effect staged deployments across these subsets, and a soak testing approach may be employed to better evaluate the impacts of hotfixes and patches.

Control 3.2.9 A software register, including versions, integrity signatures, and patch status of devices, applications, drivers, operating systems, and firmware for workstations, servers, mobile devices, and network devices must be maintained and regularly audited.

Subdomain 3.3 Penetration Testing

Penetration tests are exercises where a variety of exploitation techniques are employed against people, systems, and infrastructure to evaluate the effectiveness of an organization's cybersecurity controls, operations, and strategy and identify weaknesses that can be rectified before a real-world attacker discovers them. This subdomain sets out controls to use penetration testing to perform this evaluation and continuous improvement.

Control 3.3.1 Penetration tests must be conducted on a regular basis at appropriate intervals. A proportion of these tests must be by independent third parties to ensure that the tests reflect an objective evaluation.

3.3.1.1 Internally sourced penetration tests must be executed by resources who can reasonably be expected to perform independently. Testing personnel must generally be independent from the teams that built and maintain the infrastructure being tested or which are themselves within the test scope.

3.3.1.2 Externally sourced tests must be provided by a variety of independent third parties. Third parties performing a given test must be rotated at least every two years.

Control 3.3.2 Penetration tests must be authorized and approved by an entity's senior leadership as part of its annual cybersecurity strategy, and summarized findings must be briefed to the Board of Directors.

3.3.2.1 Each test must be formally documented and state the test's scope, identifying elements to be tested and any constraints on the test, such as acceptable techniques, tools, or other elements of the test.

3.3.2.2 This scope must also clarify how any production data exposed or retrieved during the test will be handled and protected in accordance with the entity's data management policies.

3.3.2.3 After a test is complete, its findings must be formally documented in a report and a full recounting of the test execution and results must be provided. This report must also clarify the disposition of any data exposed or retrieved during the test.

Control 3.3.3 An entity must ensure the integrity of its penetration tests and the validity of their findings through the following measures:

- Providing testers with as much discretion as possible to employ any tools, techniques, and procedures that a real-world attacker would likely use.
- Refraining from alerting monitoring or incident response teams ahead of time if their responses are part of the test scope.
- Not adjusting cybersecurity controls or their configurations in advance of the tests.
- If the test is not being conducted in the production environment, ensuring the test environment is as close an approximation of the production environment as possible.
- Ensuring that the penetration testers have the necessary knowledge, experience, qualifications, and certifications to perform the test.

Control 3.3.4 A document authorizing the test and identifying the entity who has approved it on behalf of the entity must be provided to the testers.

Control 3.3.5 The entity must identify, prioritize, and address the findings of the test.

Subdomain 3.4 Third Party Services

Third parties include, but are not limited to, external suppliers of products and services to an entity, both of which can introduce a variety of cyber risks to an organization. The objective of this subdomain is to establish controls to govern the security obligations of third parties, including restricting unauthorized activities and enforcing compliance with an entity's cybersecurity policies.

Control 3.4.1 An entity's cybersecurity policy must set out minimum security requirements for third-party service agreements, particularly those where access to the entity's systems or data may be required. Before a contract or service agreement is finalized, an entity must perform a risk assessment to analyze and identify potential cybersecurity risks associated with the service.

Control 3.4.2 An entity's contracts with third parties must consider the confidentiality, integrity, and availability of its infrastructure and data, and must be consistent in all respects with the entity's cybersecurity policies, procedures, and standards. Contracts must specify appropriate liability and recourse for compliance failures.

> **3.4.2.1** The use of standardized security contract clauses is recommended to reduce ambiguity and provide a central mechanism for revising and updating cybersecurity contractual language as required. Where appropriate, contracts may refer to an externally available code of conduct for suppliers rather than integrating the language itself.
>
> **3.4.2.2** If the products and services provided by the third party require cyber insurance or other coverage, this must be set out in a contract between the entity and the third party. The third party must also undertake in the contract to maintain any cybersecurity controls or other requirements stipulated by these insurance policies.
>
> **3.4.2.3** An entity's contract with a third party must identify clear points of contact on both sides for cyber incident notifications. Where feasible, these points of contact must be group or role addresses rather than individuals to ensure that such notifications can be made even if personnel on either side have changed roles.

Control 3.4.3 Third party access, particularly to privileged accounts or critical systems, must be monitored, logged, and audited to ensure that it is consistent with the business purposes of its service agreement or contract with an entity.

Control 3.4.4 Entities must provide a proxy or jump-point system for third-party remote access to the entity's systems and data.

> **3.4.4.1** Where a third-party must directly access the entity's networks and data without a proxy or jump-point, an entity-provided device that is actively managed to enforce security controls and policies must be used.

Control 3.4.5 The entity must approve all subcontractors to the contract. The roles and responsibilities of both the lead and subcontracted suppliers shall be documented, as applicable, and the security obligations of the prime contractors must also be contractually applied to these subcontractors.

Control 3.4.6 Outsourcing contracts shall include the Service Level Agreement (SLA) to be provided, the level of availability in the event of a disaster and after termination the customer data must be retrieved.

Control 3.4.7 The entity must ensure that the outsourcing service provider encrypts the customers' confidential information and stores it separately from other client data.

Control 3.4.8 Third party contracts must include the following security clauses:

- Mandatory breach reporting where the breach is relevant to the entity or directly impacts entity data/services/products.
- Security requirements that align the third-party with the entity's own security policies, to ensure consistency in security posture and achieve entity objectives (for example, vulnerability remediation times for vulnerability severity, and incident response procedure).
- The entity's right to audit the third-party for adherence to contract security clauses.

Subdomain 3.5 Telecoms Products and Vendor Cybersecurity

This subdomain sets out controls to ensure that a wide range of telecoms and IT products used by an entity directly or resold to customers adhere to core product security principles. In general, these controls aim to ensure that entities perform security due diligence on such products to ensure that they adhere to Secure by Design / Secure by Default design principles, and that the product developer or vendor accepts and upholds security responsibilities over its entire lifecycle.

Control 3.5.1 Entities must ensure, at the start of a new contract, that vendors demonstrate the presence of a secure SDLC (integrity of the process, presence of security embedded in developing product, and so forth) for products that they develop and provide and must periodically review this security at appropriate periods during the life of the contract.

Control 3.5.2 Entities must ensure that vendors provide a Software Bill of Materials (SBOM) for products they provide.

Control 3.5.3 Entities must require vendors to demonstrate that the products they provide have undergone successful security testing (for example, Common Criteria, ISO certification, GSMA NESAS, internal penetration testing, and vulnerability scanning).

Control 3.5.4 Entities must require vendors to provide software integrity checking mechanisms for the software they provide.

Control 3.5.5 Entities must require vendors to explicitly define the supported lifecycle of a product and verify that it has a product security incident response team (PSIRT) to investigate

and mitigate direct or third-party security vulnerabilities that may impact the product over this entire lifecycle.

3.5.5.1 The entity must require that the vendor patch all in-support products on a timeline aligned with the severity of security vulnerabilities as well as the entity's own internal timelines for patch management. If patching is not possible, a workaround must be implemented such that the vulnerability is not exploitable.

Control 3.5.6 Entities must ensure that no products supplied by a vendor have unsupported components (third-party or otherwise).

Control 3.5.7 Entities must not use any equipment that is end-of-life or unsupported for security updates and patches. Where temporary exclusions to this control are required, appropriate compensating controls should be implemented, and the exclusion should be tracked and reviewed periodically.

Subdomain 3.6 Cloud Computing

The main objective of this subdomain is to ensure that an entity's cloud infrastructure is protected by cybersecurity controls that are consistent with its overall cybersecurity strategy and any on-premises controls that may be in place.

Control 3.6.1 An entity must ensure that outsourced cloud services provide an SLA which permits effective execution of the entity's cyber incident response plan and is consistent with its cybersecurity policies. This may include details such as: encryption standards, vulnerability or breach notifications, access to a cloud service provider's cyber incident response team (CIRT), access to digital forensic captures, or access to relevant alert, event, or log data.

Control 3.6.2 Similarly, an entity's business continuity management (BCM) capabilities in cloud infrastructure must be generally consistent with its capabilities for on-premises infrastructure. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for cloud infrastructure must be generally consistent with those for on-premises infrastructure.

Control 3.6.3 An entity must ensure that its outsourced cloud service providers are not unilaterally authorized to release the entity's data or information, including details pertaining to a breach of this information. In situations where that provider is compelled by a legal authority to release the entity's information, the entity must be informed as soon as possible.

Control 3.6.4 Infrastructure and change management practices for cloud infrastructure must be generally consistent with those established for on-premises infrastructure. Assets in cloud computing must be identified, and an inventory of all assets must be created and maintained. The entity must maintain logical, conceptual, and network connection diagrams for the entity's account. Virtual network infrastructure must adhere to a documented network architecture with appropriate zoning, segmentation, and segregation.

Control 3.6.5 The entity must ensure MFA is implemented for all types of access where possible, and specifically mandate MFA for access to privileged cloud accounts.

Control 3.6.6 Backups must be taken for services in cloud computing including taking offline and offsite backup for critical servers and storage where possible. Cloud-based backups need to be appropriately separated from production resources such that a compromise of security

measures in production will not automatically lead to compromise of the backup (for example, different credentials and access methods).

Control 3.6.7 Vulnerability assessment, penetration testing, and risk assessment activities for cloud services must be performed at the same frequency as internally hosted services.

Subdomain 3.7 Virtualized and Containerized Environments

This subdomain addresses security controls relevant to virtualized or containerized environments, especially where part of a Network Functions Virtualization (NFV) environment.

Control 3.7.1 An entity must ensure that only approved, known, and secure container images or code can be deployed.

Control 3.7.2 An entity must deploy appropriate role-based access controls and strong authentication for all container and repository management systems.

Control 3.7.3 Security isolation capabilities must be deployed to ensure sensitive or critical containers or workloads are appropriately protected from less sensitive and publicly exposed infrastructure.

Control 3.7.4 Hypervisors and other virtualization fabric elements must be monitored for malicious or anomalous activity and must be appropriately segregated from the virtualized functions they support.

Control 3.7.5 Virtualized hosts and containerized environments must also be monitored and must be deployed with sufficient redundancy and isolation to minimize the impact of the exploitation of a specific host.

Control 3.7.6 Entities must ensure that containers are not running as root by default.

Control 3.7.7 The root or admin user must not be used within virtual machines or containers, except during initialization.

Control 3.7.8 Entities must make use of read-only containers, file systems, and minimal virtualization images to reduce risk of hypervisor escape.

Control 3.7.9 Remote-management services (for example, SSH, and RDP) must be disabled within VMs and containers unless required. If required, public access to these services should be disabled or managed via dedicated jump-servers (for example, proxies, and SSH relays) with multi-factor authentication.

Control 3.7.10 Different containers and VMs must not run on the same node unless they have the same data classification, sensitivity, and network exposure (for example, internet facing).

Control 3.7.11 VMs and containers must be based on secure, verified 'golden images' that are rebuilt on a regular schedule to ensure that they are kept up to date with security patches.

Control 3.7.12 Periodic and final state relevant snapshots (for example, VM snapshots, or memory dumps) of running VMs and Containers must be captured and kept for a period of time consistent with forensic evidence retention policy, to facilitate incident investigation.

Domain 4 Cybersecurity Operations and Incident Management

Cybersecurity-related incidents may occur even when cybersecurity controls are implemented. However, the cybersecurity controls mentioned in this domain are critical to minimizing the impact of current and future incidents.

Subdomain 4.1 Incident Detection

The purpose of this subdomain is to ensure necessary controls are in place to activate, protect and maintain the cybersecurity event logs within networks, systems, and applications. In addition, this subdomain ensures that monitoring is conducted to required events within the networks, systems, and applications to identify any suspicious behavior which may lead to cybersecurity incidents.

Control 4.1.1 An entity must collect, manage, correlate, and analyze alerts, logs, and events from all systems to enable early warning, detection, and response to cyber incidents. This must include the characterization and detection of suspicious or anomalous activities in addition to confirmed malicious activities.

4.1.1.1 A variety of technologies and systems may be employed in this context, such as SIEM, UEBA, XDR, and SOAR.

4.1.1.2 Alerts, logs, and events from user activities, system and network and physical environments must be monitored. This monitoring must include a measurement of normal operating baselines to enable effective detection of anomalous or suspicious activities.

Control 4.1.2 Alert, log, and event sources and repositories must be protected from and monitored for unauthorized access, modification, and deletion.

Control 4.1.3 System time for all information processing systems must be synchronized regularly. Alerts, logs, and events must clearly indicate the time zone in which they were created.

Control 4.1.4 Alerts, logs, and events must be backed up and a sufficient history maintained to enable cyber incident response, investigations, and threat hunting.

Subdomain 4.2 Incident Management

This subdomain sets out appropriate controls for ensuring that an entity maintains a robust organizational capacity to respond to a cybersecurity incident quickly and effectively. This response capability must not only be able to effectively address the immediate cyber threat under a wide variety of adverse circumstances but must also anticipate a wide variety of post-incident measures that are likely to be necessary.

Control 4.2.1 An entity must maintain a cyber incident response plan which sets out procedures for all aspects of managing and responding to a cyber incident. This plan must be formally endorsed by senior leadership and the Board of Directors.

4.2.1.1 The cyber incident response plan must identify a cyber incident response team (CIRT) that is responsible for assessing and responding to cyber incidents. In large or complex organizations where this function may be fulfilled by multiple teams, the division of responsibilities must be made clear.

4.2.1.2 The cyber incident response plan must designate an appropriate cyber incident reporting mechanism, available internally and externally, that is monitored and broadly available for the reporting and triage of potential cyber incidents.

4.2.1.3 The cyber incident response plan must designate roles and individuals who are authorized to make critical decisions in the event of a cyber incident, such as authorizing negotiations with a threat actor or shutting down potentially impacted systems or services. The plan must also include a list of alternates and procedures for emergency authorizations when primary or alternate designates are unavailable.

4.2.1.4 The cyber incident response plan must set out clear thresholds for notifying an entity's senior leadership, Board of Directors, and/or public authorities. The plan must make clear who is authorized to conduct such a notification and by what means it must be made.

4.2.1.5 The cyber incident response plan must also consider when contractually obligated notifications to third parties, such as customers, insurers, or other entities must be made. Entities must have a mechanism to identify relevant third-party contracts and fulfil any obligations regarding cyber incident notifications.

4.2.1.6 The cyber incident response plan must set out clear procedures for documenting all decisions and actions taken during a potential or actual cyber incident. This documentation must include critical metrics on the entity's performance during the incident response that will allow for measurement and continuous improvement of the response capability.

4.2.1.7 The cyber incident response plan must also require an after-action review after cyber incidents, in order to objectively evaluate how the incident response was executed and to identify improvement opportunities. The plan must identify how this review will be conducted and how lessons learned will be captured and acted on.

Control 4.2.2 An entity must have an out-of-band communications mechanism for the CIRT and other critical participants in a cyber incident response to use for coordination if primary systems are unavailable or are potentially compromised.

4.2.2.1 This out of band communications mechanism must be separate from the primary organizational domain or IAM system, contain a separate copy of critical contact information, and must be tested regularly to ensure that the list of members and their access credentials are kept current.

4.2.2.2 Examples of suitable out-of-band communications mechanisms include a separate Microsoft 365 or Google Workspace instance. A combination of other collaboration capabilities, such as a telephone bridge, may also be suitable.

Control 4.2.3 An entity must provide training to the CIRT to ensure that it maintains essential incident response and recovery capabilities as personnel and technology continually evolves,

is aware of the current cyber threat landscape, and that continually shares and reviews lessons learned and best practices.

4.2.3.1 The CIRT must have the authority, access, and abilities, even if outsourced, to rapidly isolate, contain, and recover from a cyber incident while preserving and capturing necessary digital forensics. This may require direct access to endpoint, network, cloud, or other infrastructure environments or their related operations teams.

Control 4.2.4 An entity must ensure that its entire workforce, including contractors and third parties, is advised of their cybersecurity responsibilities in the event of an incident.

4.2.4.1 In particular, an entity's workforce must be reminded never to directly engage or communicate with a threat actor and that such interactions will be carried out by individuals authorized by the incident response plan.

4.2.4.2 An entity's workforce must also be reminded to follow the directions of the CIRT in the event of a cyber incident, particularly regarding any instructions to disconnect and leave impacted systems running so that forensic evidence can be preserved.

Control 4.2.5 Evidence related to cybersecurity incidents must be collected and protected from any loss or tampering before the containment process. Evidence must be retained and only disposed of after consultations with an entity's legal department.

Control 4.2.6 A centralized cybersecurity incident repository must be maintained by the entity and reviewed periodically.

Subdomain 4.3 Threat intelligence and information sharing

Cyber threat intelligence is information about current and emerging cyber threats, in the form of both indicators of compromise (IOCs) and information on the tools, techniques, and procedures (TTPs) of a given cyber threat adversary. This subdomain sets out controls to help entities take proactive measures to prepare for and respond to the relevant cyber threats which may be targeting a geographic region or market vertical.

Control 4.3.1 Entities must participate in industry-wide information sharing forums to ensure rapid communication, problem resolution, mutual aid, education, and best practices development. Existing international forums include NANOG and the GSMA Fraud and Security Group. National forums may also exist for more focused sharing. Within these forums and subject to appropriate information sharing rules, entities must share high-level lessons learned from major cyber incidents with other entities.

Control 4.3.2 Entities must make use of threat intelligence sources to make sure that cyber detection and analysis systems have up-to-date knowledge on current indicators of compromise (IOCs) and other relevant information on the latest tools, techniques, and procedures (TTPs) employed by threat actors.

4.3.2.1 Entities must make use of an automated threat intelligence information sharing platform and subscribe to relevant threat intelligence feeds such as the T-ISAC feed.

Control 4.3.3 Entities must maintain an 'abuse' function, which responds to external security complaints about their subscribers and notifies them of the complaint, with the goal of remediating the security vulnerability. (IETF RFC 2142).

Subdomain 4.4 Testing and Exercises

Cyber exercises are simulated scenarios that test the preparedness and resilience of an organization against cyber threats. They help to identify gaps, improve skills, and enhance coordination among different stakeholders. This subdomain identifies controls to continually measure and reinforce this organizational preparation and resilience.

Control 4.4.1 Entities must periodically conduct cyber exercises using different threat scenarios to test and validate different aspects of their cybersecurity controls and capabilities.

Control 4.4.2 Exercises must be formally planned, executed, and documented, with a summary of the exercise briefed to senior leaders and the board of directors. This summary must include lessons learned, root cause analysis, and an action plan to address these findings.

Control 4.4.3 Exercises must involve a complete cross section of organizational resources and teams who may be required to fully respond to the threat scenario being exercised. This may include representatives from an entity's communications, customer service, legal, privacy, or finance departments.

Domain 5 Generally Applicable Telecoms Security Controls

The recommendations in domains 1 through 4 broadly apply to all areas of the organization including telecommunications systems. The following three domains set out controls which are specific to the technology of telecommunications systems.

This domain focuses on telecom security controls that are broadly applicable and relevant across all environments and technologies, as well as on managing and operating networks based on the GSMA mobile cyber security knowledge base. Where possible, controls are scoped to Signaling, Management, and User planes based on the ITU X.805 security architecture definition of these planes Subdomain 5.1 Architecture and Design Controls

The following represents design patterns and practices that can be broadly applied to all areas of the telecommunications provider to serve as a foundation for strong security.

Control 5.1.1 Physical or logical separation must be maintained between Signaling, Management and User planes and prevent communication between planes (for example, user to signaling, and management to user).

Control 5.1.2 Systems that support more than one plane (such as DNS) must ensure logical or physical separation to avoid cross-contamination and abuse.

Control 5.1.3 Network Security Monitoring must be designed and enabled by the operator through specific and dedicated devices to allow for anomaly and attack detection through the use of techniques that may include network flow analysis and in-band tapping.

Control 5.1.4 Network products must have the ability to filter incoming IP packets at the network and transport layer (for example, RFC 3871, and 3GPP TS 33.117).

Control 5.1.5 Communications integrity protection must be enabled where supported and recommended by industry standards (for example, 5G air interface, and user-plane).

Control 5.1.6 Centralized logging must be used for all systems via the management plane.

Control 5.1.7 Centralized AAA with MFA and command-logging must be used for all systems, where supported and possible.

Control 5.1.8 Centralized timing must be used for all systems (for example, NTP), generated from an authoritative and secure internal source (for example, atomic clock), and propagated outward to external and user plane systems as required. Where supported, at least two different time sources are used to ensure that the timestamps in logs are consistent.

Control 5.1.9 All systems must be hardened via the application of security controls following the vendor recommendation and/or security best practices. This includes the configuration of security features on the systems, the integration with security systems (centralized authentication), and the application of new security software and agents where possible.

Control 5.1.10 Entities must validate the integrity of software prior to use.

Control 5.1.11 Where possible, hardware must support secure boot process (such as, defined memory device for boot image, UEFI, Hardware-Based Root of Trust, and so forth).

Control 5.1.12 Security agents must be used on systems that support it for the detection of anomalous or malicious events and intrusions.

Control 5.1.13 All API connections, including those used in mobility such as CAPIF, network slicing, SDN and NFV MANO deployments, must use TLS protection.

Subdomain 5.2 Control Plane Controls

The control plane supports the integrity of the telecommunications infrastructure. The following controls aim to ensure that signaling, which controls the topology and traffic flow of the network, are secure.

Control 5.2.1 Signaling endpoints and path must be controlled and validated (such as an allow list) through the use of techniques that include logically or physically separate network resources, firewalls or packet filters, and IPSec VPNs.

Control 5.2.2 Cryptographic protection of signaling must be used where supported and recommended by industry standards (such as S1-MME).

Control 5.2.3 Signaling origin must be cryptographically authenticated with unique credentials per signaling source and administrative domain.

Control 5.2.4 Signaling content must be filtered to ensure receipt and/or transmission of desired signals only (whitelist).

Control 5.2.5 Signaling speaker resources (such as CPU and so forth) must be protected with interface and control-plane filters to prevent denial of service attacks.

Control 5.2.6 Signaling anomalies and abuse must be monitored and alerted.

Subdomain 5.3 Management Plane Controls

Ultimately, the primary concern of a telecommunications provider is to maintain control over its infrastructure, and this is done primarily through the management plane. The management plane is among the highest priority and sensitivity networks in critical infrastructure.

Control 5.3.1 The management plane must be separate (from any other network) with perimeter access controls (such as firewalls), strong user authentication (multi-factor), and granular user-access control designed to provide the least privilege required per connection.

Control 5.3.2 The management plane must not have an Internet connection.

Control 5.3.3 Least privilege network access must be enforced via network segmentation in a hub-and-spoke architecture, with central systems in the hub and managed elements on isolated spokes, and routing controls.

Control 5.3.4 Managed elements, by default, must not be able to inter-communicate on the management plane.

Control 5.3.5 All communicating endpoints on the management interface must be mutually authenticated (for example. pre-shared client-based IPSec or TLS certificates).

Control 5.3.6 Management systems must only be able to view elements that they are intended to manage, using separate logical and physical segmentation and routing controls.

Control 5.3.7 Access to the management plane must be via dedicated jump-servers (for example, proxies, and SSH relays) with multi-factor authentication.

Control 5.3.8 Root or administrator accounts must be limited to console access only.

Control 5.3.9 Entities must not provision or enable multi-user, shared accounts.

Control 5.3.10 Remote access must be restricted to provide only the minimum privileges necessary to accomplish designated tasks or functions. Remote access systems must be accessed with origin validation (whitelist) and multi-factor authentication, must be encrypted, and fully logged.

Control 5.3.11 Vendor and third-party remote access must be escorted by entity team members (physically, or logically through the use of techniques which include sharing split MFA token credentials) and monitored at all times, with logs stored for later review if required.

Control 5.3.12 Where static or shared passwords are required, or user-level access controls are not available, systems must be protected by authentication and authorization proxies and network segmentation.

Control 5.3.13 Comprehensive audit logs of all management and administrative functions, including per-command logs, must be maintained, and monitored for abuse.

Subdomain 5.4 User (Data) Plane Controls

The primary role of the telecommunications provider is to maintain the availability of the user plane for its customers and the country. To that end, the following simple controls ensure that the telecommunications provider's network minimizes the amount of disruptive traffic on its network.

Control 5.4.1 All connections to the entity's network, both customer and peers, must be validated to prevent false traffic sources (spoofing).

Control 5.4.2 An entity must prevent malicious or inappropriate traffic from being received and transmitted through the use of packet and route filtering and/or payload inspection.

Control 5.4.3 Entity must prevent volumetric attacks (DoS) via packet and protocol filters, rate-limiting, or mitigation systems.

Subdomain 5.5 Security Practices

The following high-level best practices ensure that the telecommunications environment can support and maintain the security controls referenced in this document.

Control 5.5.1 Network and design documentation and diagrams must be created and maintained for all telecom systems, including hardware and software inventory, and a description of data flows.

Control 5.5.2 Logging must be reviewed regularly for evidence of abuse and real-time alerting must be enabled for pre-defined security use-cases.

Control 5.5.3 Vulnerability scans must be performed in both lab and production systems to reduce the attack surface and eliminate flaws from systems.

Control 5.5.4 Lab security must be maintained at the same level as that of production systems.

Control 5.5.5 Formal change control with dual oversight must be used throughout to maintain resiliency and ensure stability of the technology and to prevent abuse.

Control 5.5.6 A SIRT function must exist and have scope for telecom systems and services to respond to security incidents in any of the entity environments and technologies.

Domain 6 Peering and Interconnection

This domain focuses on security controls which are relevant in the context of international peering and interconnection. Implementing these controls will help the Kingdom of Bahrain enhance the security of its regional and global interconnections and maintain its position as one of the region's leading countries for IT infrastructure and connectivity.

Subdomain 6.1 Internet

Internet peering is the primary data connection for the national critical infrastructure and the connection to the rest of the world. This subdomain sets out the basic security controls for a secure global interconnect. While these controls are primarily aimed at network service providers, these controls may also apply to enterprises that do not provide network services to customers but own their own ASN and publicly registered network resources for corporate use.

Control 6.1.1 Entities must define a clear routing policy and implement a system that ensures correctness of their own announcements and announcements from their customers to adjacent networks with prefix and AS-path granularity.

Control 6.1.2 Publicly documented routing policy, ASNs and prefixes must be registered with the IRRs to ensure appropriate transit filters and contact information.

Control 6.1.3 Entities must maintain globally accessible and current contact information in official public registries (such as RIPE, RADB, and PeeringDB) in addition to on their public web site.

Control 6.1.4 Entities must communicate to their adjacent networks which announcements are correct, via IRR information and/or PKI ROAs.

Control 6.1.5 Entities must be able to validate received route announcements via IRR information and/or PKI ROAs and must be able to drop prefixes with invalid ROAs.

Control 6.1.6 Entities must prevent source spoofing by blocking received route advertisements for their own network or networks of their customers.

Control 6.1.7 Entities must implement a mechanism to secure Border Gateway Protocol (BGP) routing, such as Resource Public Key Infrastructure (RPKI), to prevent route prefix hijacking and ensure the integrity and reliability of telecommunications services.

Control 6.1.8 Entities must filter BGP for invalid ASNs via AS path filtering.

Control 6.1.9 Entities must filter BGP communities from all received and transmitted routes across the ASN boundary, unless explicitly required.

Control 6.1.10 Entities must monitor route advertisements and registrations for abuse and hijacking.

Control 6.1.11 Entities must implement anti-spoofing filtering to prevent packets with incorrect source IP address from entering and leaving the network.

Subdomain 6.2 Voice and Mobility

Voice and mobility peering involves a number of legacy technologies from legacy PSTN to current 5G mobile networks. As a result, it has a wide attack surface, and many legacy vulnerabilities may be exposed.

Control 6.2.1 Entities must implement Home Routing.

Control 6.2.2 Entities must monitor edge network nodes, such as STP/DEA/DRAs, for SS7 and Diameter signaling attacks.

Control 6.2.3 Entities must prevent SS7 and Diameter signaling attacks by implementing a signaling firewall at edge network nodes, either on-premises or via an upstream IPX service.

Control 6.2.4 Entities must also prevent SS7 and Diameter signaling attacks by filtering core network elements, such as the VLR and MME.

Control 6.2.5 Entities must harden signaling termination points per GSMA guidelines (such as HLR, and MSC).

Control 6.2.6 Entities must protect roaming and interconnections from attacks (such as eavesdropping, and denial of service) through the use of techniques listed in GSMA FS.31, which includes filters for malformed and/or inappropriate requests, signaling proxies, and rate-limits.

Subdomain 6.3 Satellite Ground Stations

Satellite has previously been a relatively isolated network but is increasingly being used for Internet and mobility backhaul. As a result, it is important to secure the ground station to ensure the integrity of the ground-to-space connection. In addition, as the satellite is a difficult device to remediate, ensuring that it is protected from attack through the ground-station is equally important.

Control 6.3.1 Satellite ground station consists of two centers which must be kept separate: Mission Operations Center (which controls the satellite itself), and Payload Control Centers (which controls the various payloads on the satellite). The satellite itself is out of scope of these guidelines.

Control 6.3.2 Mission Operations Centers and Payload Control Centers must be kept separate at both a systems and network level, and protected by firewalls and other security measures to prevent unauthorized access. These represent different administrative zones and policies.

Control 6.3.3 Mission Operations Center must be kept securely isolated from all other networks (such as the internet) with appropriate separation (for example, an air gap or DMZ). This is the highest priority zone for protection as it controls the satellite itself.

Control 6.3.4 Spot beams (concentrated signals to geographic areas) and frequency hopping must be employed to avoid eavesdropping.

Control 6.3.5 Satellite transmissions must be encrypted and authenticated.

Control 6.3.6 To protect against replay attacks or spoofing, entity must employ measures such as a command count or nonce on encrypted satellite transmissions.

Control 6.3.7 Entity must employ hardware or software integrated into the ground station to detect and mitigate radio frequency jamming and spoofing events in addition to radio frequency interference and degradation.

Control 6.3.8 Network activity at satellite ground stations must be monitored to detect malicious or anomalous events.

Control 6.3.9 As satellites have limited abilities for self-protection, the satellite transmissions must be monitored for malware or attacks at the ground station, in both the Mission Operations Centers and Payload Operations Centers for their respective transmissions. Where possible, network monitoring on this segment must be correlated with that in the ground station to identify active attacks against the satellite.

Control 6.3.10 Payloads providing user-plane connectivity (such as internet) must meet the same requirements as wireline providers for user-plane security (such as filtering, and so forth).

Control 6.3.11 Entities must be able to contain security events in the ground station, which may include transitioning Mission and Payload Operations to an alternate site. Playbooks governing this decision must be created in advance and tested.

Control 6.3.12 Software, firmware and code must be protected to maintain integrity and prevent tampering.

Domain 7 National Infrastructure and Services

This domain focuses on telecoms security controls that are principally applicable within the Kingdom of Bahrain's domestic networks and infrastructure.

Subdomain 7.1 Internet

In addition to global Internet peering security, some basic security practices are required to ensure the integrity of the national Internet network.

Control 7.1.1 Entity must apply due diligence when checking the correctness of its customer's announcements, specifically that the customer legitimately owns the ASN and the address space it announces.

Control 7.1.2 Entity must maintain an abuse-reporting function to receive complaints about inappropriate or illegal use of network resources originating from the entity, an ability to notify entity's customers of abuse, and a remediation function to prevent abuse from repeat offenders. This is applicable to entities offering customer network services, as well as entities that do not, as the abuse complaints can reflect a corporation's incidents as well as its customers.

Control 7.1.3 Entity must deploy RPKI and validate national peer prefix advertisements, dropping advertisements that do not have valid ROAs.

Subdomain 7.2 Voice and Mobility

This subdomain outlines the requirements for secure voice and mobility services with the goal of reducing spoofed content, ensuring the security of user equipment, preventing eavesdropping and interception of customer traffic, and protecting the privacy of customers.

Control 7.2.1 Entity must prevent the connection and use of stolen, defective, or counterfeit devices. This may be done by using community-sourced information on such devices (such as the GSMA FASG IMEI registry).

Control 7.2.2 Entity must have a program to securely manage (e)UICC/SIMs, including secure provisioning and purchase from reputable vendors.

Control 7.2.3 The administrative function of moving (porting) SIM/eSIM between entities must be protected from abuse through security mechanisms which include the use of robust customer authentication, MFA, out-of-band confirmation, and wait periods.

Control 7.2.4 SIP server connections must be protected by Session Border Controllers (SBCs).

Control 7.2.5 Entities must implement means to cryptographically sign the calls they originate and validate the origin of received calls (such as the STIR/SHAKEN protocols).

Control 7.2.6 ENUM service (E164 Number to URL Mapping) must use a trusted and protected (internal only) DNS service.

Control 7.2.7 Entity must use temporary mobile identifiers (for example SUPI, and TMSI) to prevent user tracking.

Control 7.2.8 The strongest encryption must be enabled on mobility networks (such as 2G, and 3G) with the use of Null encryption, if required, as the last resort.

Control 7.2.9 For over-the-air mobility traffic, including for GSM, GPRS, UMTS, LTE, and NR networks, an entity must comply with telecoms encryption best practices to protect against unauthorized interception or interference.

7.2.9.1 For GSM, A5/3 must be enabled. A5/4 and A5/1 must be enabled if possible.

7.2.9.2 For GPRS, GEA3 must be enabled. GEA4 must be enabled if possible.

Control 7.2.10 5G functions in the SBA are authenticated cryptographically, and accessed via properly configured OAUTH, per industry specifications (3GPP). This includes inter-SEPP communication in all cases.

Control 7.2.11 The 5G UPF must validate receipt of GTP-U traffic from whitelisted senders only and drop unvalidated connections, either on the UPF or an associated security device.

Control 7.2.12 Entities must ensure that internal 5G core information such as SUPI, DNN, S-NSSAI is not disclosed by NEF to application functions residing outside the MNO domain.

Control 7.2.13 VMs and containers in MEC must be encrypted in storage.

Control 7.2.14 Both the physical security of base-stations and small-cells must be protected with methods that include secure buildings or tamper-resistant casings.

Subdomain 7.3 Domain Name System (DNS)

The DNS system is, in essence, a control plane for data networks, as it translates between addresses and names. As a result, it can be a target for an attacker who is trying to subvert any of the telecommunications' services and must be secured. These controls apply to both those entities that provide DNS services to customers, as well as those that simply use and maintain DNS services for corporate use.

Control 7.3.1 DNS servers must be separated into public-facing server which responds to queries (recursive), and the private authoritative server which maintains the entity DNS database, separated by a firewall or other protective device.

Control 7.3.2 Authoritative servers must be protected by refusing all connections except those from valid resolvers.

Control 7.3.3 Authoritative servers must be geographically separate to maximize resiliency against DNS attacks.

Control 7.3.4 Client DNS queries must be resolved by authorized recursive resolvers which are allowed to query authoritative servers.

Control 7.3.5 Recursive resolvers must be protected by rate limiting and packet filters.

Control 7.3.6 Properly configured and managed DNSSEC must be used to protect queries and responses between servers.

Control 7.3.7 DNS servers must use cryptographic methods to secure stub, recursive and authoritative communications (for example, DNSSec, DTLS per RFC 7858 and RFC8310).

Control 7.3.8 Entity must protect DNS transactions (such as updates of resolution data, or data replication between nodes) with cryptographic techniques per IETF TSIG (transaction signature) specification.

Control 7.3.9 Entity must maintain an ability to monitor DNS service for abuse.

Control 7.3.10 Entity must maintain an ability to filter DNS service for abuse and malicious content using techniques which include RPZ (Response Policy Zones) on recursive servers.

Subdomain 7.4 Messaging

Messaging abuse is one of the more pervasive abuses on the Internet. Simple content and volume controls at the provider edge can reduce this impact and ensure that telecommunications providers are acting as Internet 'good neighbors'. These controls apply both to entities that are providing messaging services for customers, as well as those that simply use messaging in a corporate setting. In all cases, messaging abuse must be managed.

Control 7.4.1 Entity must filter outbound SMTP from itself and subscribers, where possible, to remove abuse (such as SPAM, and volumetric attacks).

Control 7.4.2 Messaging (SMS, MMS, and so forth) must be filtered to prevent subscribers from receiving attacker traffic (such as OTA solicitation attempts).

Control 7.4.3 SMS gateways, such as email-to-SMS, must implement rate-limiting to minimize abuse

Control 7.4.4 Entities must be responsive to direction and regulations from the TRA regarding the management of unsolicited messaging.

Control 7.4.5 Entities sending bulk messages must ensure that:

- Recipient permission is obtained.
- Recipient opt-out is provided and honored.
- Message originator is properly identified.
- Recipient information is protected when stored.

Subdomain 7.5 Private Wireless

For private mobile networks (especially private 5G networks) offered as a managed service by the entities, the following controls must apply to ensure security of the private network and protection between it and other entity networks:

Control 7.5.1 Entities must provide a separate data gateway for private network user-plane (for example, GGSN, PGW, UPF, and APN).

Control 7.5.2 Entities must provide separate data network external addressing for private networks, to isolate the attack surface.

Control 7.5.3 Entities must ensure logical and/or physical separation of user-planes in the RAN (such as separate GTP tunnels from other networks).

Control 7.5.4 Entities must employ dedicated SIM/eSIMs for the private network, not usable on other networks.

Control 7.5.5 Entities must not offer the air interface Null encryption scheme on IoT or private networks where the UE is well defined and supports encryption.

Control 7.5.6 Where telecommunications equipment is deployed at a customer site for private mobile, it must be physically secured with operator access only.

Control 7.5.7 Where the private network is deployed partially on non-telecommunications facilities, encryption must be used on all links containing signaling or management plane traffic.

Control 7.5.8 Where a customer-facing system is provided for management (such as an IoT console), the entities must ensure logical or physical separation between customers.

Control 7.5.9 All private network elements and systems must be secured, including remote management, as per the standards for the entities own network.

Appendix A

Glossary of Abbreviations and Acronyms

3rd Generation Partnership Project (3GPP) – An umbrella term for several standards organizations which develop protocols for mobile telecommunications.

Access Point Name (APN) – A gateway between a GSM, GPRS, 3G or 4G mobile network and another computer network, frequently the public Internet. A mobile device making a data connection must be configured with an APN to present to the carrier.

Application Programming Interface (API) – A set of definitions and protocols for building and integrating application software.

Authentication, Authorization, and Accounting (AAA) – Authentication is the process of confirming the correctness of the claimed identity, Authorization is the approval, permission, or empowerment for someone or something to do something, and Accounting is the recording of actions to form an audit trail.

Autonomous System (AS) – A very large network or group of networks with a single routing policy. Each AS is assigned a unique ASN.

Autonomous System Number (ASN) – Each AS is assigned an official number, or autonomous system number, similar to how every business has a business license with a unique, official number. They are unique 16-bit numbers between 1 and 65534 or 32-bit numbers between 131072 and 4294967294. ASNs are only required for external communications with inter-network routers.

Border Gateway Protocol (BGP) – BGP is the protocol that makes the Internet work by enabling data routing. When a user in Singapore loads a website with origin servers in Argentina, BGP is the protocol that enables that communication to happen quickly and efficiently.

Bring Your Own Device (BYOD) – Allows employees to use their personal devices such as laptops, tablets, mobile phones and other devices, to connect to the internal network.

Business Continuity Management (BCM) – Holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities.

Business Continuity Plan (BCP) – A Business Continuity Plan is the plan for emergency response, backup operations, and post-disaster recovery steps that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

Business Impact Analysis (BIA) – A Business Impact Analysis determines the tolerable levels of impact to a system.

Central Processing Unit (CPU) – The central processing unit or processor is the unit which performs most of the processing inside a computer. It processes all instructions received by software running on the PC and by other hardware components and acts as a powerful calculator.

Chief Information Security Officer (CISO) – A CISO focuses on developing and leading the information security program. This involves protecting the organization's assets, applications, systems, and technology while enabling and advancing business outcomes.

Common API Framework (CAPIF) – A standardized API framework for use in 5G networks.

Continuous Delivery (CD) – A software engineering approach in which teams produce software in short cycles, ensuring that the software can be reliably released at any time and, following a pipeline through a "production-like environment", without doing so manually.

Continuous Integration (CI) – The practice of merging all developers' working copies to a shared mainline several times a day. Nowadays it is typically implemented in such a way that it triggers an automated build with testing.

Continuous Integration and Continuous Delivery (CDI/CD) – the combined practices of continuous integration (CI) and continuous delivery (CD) or, less often, continuous deployment.

Cyber Incident Response Team (CIRT) – Group of individuals usually consisting of Security Analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents. Also called a Computer Security Incident Response Team (CSIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability, or Cyber Incident Response Team).

Data Network Name (DNN) – A network representation in 5G networks, typically in the form of an Access Point Name.

Demilitarized Zone (DMZ) – A perimeter network that protects and adds an extra layer of security to an organization’s internal local-area network from untrusted traffic.

Denial of Service (DoS) – The prevention of authorized access to a system resource or the delaying of system operations and functions.

Diameter Edge Agent (DEA) – A network component in a telecommunications network that performs routing functions and acts as an interface between the core Diameter network and external networks.

Diameter Routing Agent (DRA) – A functional element in a 3G or 4G (such as LTE) network that provides real-time routing capabilities to ensure that messages are routed among the correct elements in a network.

Disaster Recovery (DR) – Disaster Recovery is the process of recovery of IT systems in the event of a disruption or disaster and is normally codified in a DR plan.

Domain Name System (DNS) – The domain name system is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

Domain Name System Security Extensions (DNSSEC) – A feature of the Domain Name System that authenticates responses to domain name lookups. It does not provide privacy protections for those lookups but prevents attackers from manipulating or poisoning the responses to DNS requests.

Domain-based Message Authentication, Reporting, and Conformance (DMARC) – DMARC is a technical specification that allows Message Senders and Message Receivers to cooperate and thereby better detect when messages don't originate from the Internet domain they claim to have been sent from. It does this by allowing the Domain Owner to indicate they are using email authentication on the messages they send, optionally requesting that messages that fail to authenticate be blocked. Message Receivers honor these requests (unless there is a local policy overriding this action) and send reports on all the messages - whether or not they pass email authentication - to the Domain Owner.

DomainKeys Identified Mail (DKIM) – Domain Keys Identified Mail is a signature-based Email Authentication technique. It is the result of merging the DomainKeys and Identified Internet Mail specifications.

Dynamic Application Software Testing (DAST) – A non-functional testing process where one can assess an application using certain techniques and the end result of such testing process covers security weaknesses and vulnerabilities present in an application.

Embedded Subscriber Identity Module (eSIM) – A SIM where the subscriber profile can be changed over the air without changing the actual SIM.

Extended Detection and Response (XDR) – A software as a service (SaaS) tool that offers holistic, optimized security by integrating security products and data into simplified solutions.

Firewall – A logical or physical discontinuity in a network to prevent unauthorized access to data or resources.

Fraud and Security Group (FASG) – GSMA’s FASG provides an open, receptive, and trusted environment within which fraud and security intelligence and incident details can be shared in a timely and responsible way.

Gateway GPRS Support Node (GGSN) – Converts the incoming data traffic coming from the mobile users through the Service gateway GPRS support node (SGSN) and forwards it to the relevant network, and vice versa. The GGSN and the SGSN together form the GPRS support nodes (GSN).

General Packet Radio Service (GPRS) – Also called 2.5G, is a packet oriented mobile data standard on the 2G cellular communication network's global system for mobile communications.

Global System for Mobile Communications (GSM) – A standard developed by the European Telecommunications Standards Institute to describe the protocols for second-generation digital cellular networks used by mobile devices such as mobile phones and tablets.

Global System for Mobile Communications Association (GSMA) – A global organization unifying the mobile ecosystem to discover, develop and deliver innovation that helps business and society thrive.

Governance, Risk, and Compliance (GRC) – A set of processes and procedures to help organizations achieve business objectives, address uncertainty, and act with integrity.

GPRS Tunnelling Protocol - Userplane (GTP-U) – GTP-U is used to carry the user traffic within the mobility RAN network.

Hardware Security Module (HSM) - a physical computing device that safeguards and manages secrets (most importantly digital keys), performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions.

High-Level Diagram (HLD) – Overall Network Design describing the relationship between various system modules and functions.

Hypertext Transfer Protocol (HTTP) – An application layer protocol designed to transfer information between networked devices and runs on top of other layers of the network protocol stack. It is the foundation of the World Wide Web, and is used to load webpages using hypertext links.

Hypertext Transfer Protocol Secure (HTTPS) – When used in the first part of a URL (the part that precedes the colon and specifies an access scheme or protocol), this term specifies the use of HTTP enhanced by a security mechanism, which is usually SSL.

Identity and Access Management (IAM) – The process of employing emerging technologies to manage information about the identity of users and control access to company resources.

Indicators of Compromise (IOCs) – IOCs are pieces of digital forensics that suggest that an endpoint or network may have been breached.

Information Sharing and Analysis Centers (ISACs) – Organizations that provide a central resource for gathering information on cyber threats (in many cases to critical infrastructure) as well as allow two-way sharing of information between the private and the public sector about root causes, incidents, and threats, as well as sharing experience, knowledge, and analysis.

International Mobile Equipment Identity (IMEI) – A numeric identifier, usually unique, for 3GPP and iDEN mobile phones, as well as some satellite phones. GSM networks use the IMEI number to identify valid devices and can stop a stolen phone from accessing the network.

Internet Engineering Task Force (IETF) – The IETF creates voluntary standards that are often adopted by Internet users, network operators, and equipment vendors, and it thus helps shape the trajectory of the development of the Internet.

Internet Protocol (IP) – The method or protocol by which data is sent from one computer to another on the Internet.

Internet Protocol Security (IPsec) – A developing standard for security at the network or packet processing layer of network communication.

Internet Routing Registry (IRR) – IRRs contain information that has been submitted and maintained by internet service providers or other entities, about Autonomous System Numbers (ASNs) and routing IP number prefixes. IRRs can be used to develop routing plans.

Intrusion Detection System (IDS) – A security management system for computers and networks. An IDS gathers and analyses information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

Intrusion Prevention System (IPS) – Intrusion Prevention Systems (IPS) commonly employ countermeasures to prevent intruders from gaining further access to a computer network.

IP Exchange (IPX) – A set of packet-switching and packet-sequencing protocols designed to function in small and large networks.

Key Performance Indicators (KPIs) – A quantifiable measure of performance over time for a specific objective.

Key Risk Indicators (KRIs) – Key risk indicators monitor changes in the levels of risk exposure and contribute to the early warning signs that enable organizations to report risks, prevent crises and mitigate them in time.

Least Privilege – This is the principle of allowing users or applications the lowest amount of permissions necessary to perform their intended function.

Local Area Network (LAN) – A local area network is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building.

Long-Term Evolution (LTE) – A standard for wireless broadband communication for mobile devices and data terminals, based on the GSM/EDGE and UMTS/HSPA standards. It improves on those standards' capacity and speed by using a different radio interface and core network improvements.

Low-Level Diagram (LLD) – Detailed design depicting in depth information of the HLD.

Management and Network Orchestration (MANO) – Management and Network Orchestration for NFV networks. MANO is the collection of systems that control and orchestrate the deployment of virtual machines in the NFV network.

Mobile Network Operator (MNO) – An entity that provides mobile network services and operates its own physical infrastructure.

Multi-access Edge Compute (MEC) – A computing framework to leverage the features of a 5G network and deliver edge computing in the 5G RAN.

Multi-Factor Authentication (MFA) – MFA is multiple levels of authentication in which an individual authenticates not only with a password (something they know), but some type of unique code or device they have.

Multimedia Messaging Service (MMS) – MMS is a way to send messages on mobile devices, which include media objects.

National Institute of Standards and Technology (NIST) – An agency of the United States Department of Commerce whose mission is to promote American innovation and industrial competitiveness.

Network Equipment Security Assurance Scheme (NESAS) – GSMA scheme to facilitate improvements in network equipment security levels, across the mobile industry. Providing one universal and global security assurance framework.

Network Exposure Function (NEF) – The standardized API gateway in the 5G architecture.

Network Function Virtualization (NFV) – A network architecture concept that leverages IT virtualization technologies as the building blocks of the network.

Network Time Protocol (NTP) – NTP is an internet protocol that's used to synchronize the clocks on computer networks to within a few milliseconds of universal coordinated time (UTC). It enables devices to request and receive UTC from a server that, in turn, receives precise time from an atomic clock.

New Radio (NR) – Also called 5G NR, is a new radio access technology developed by the 3rd Generation Partnership Project (3GPP) for the 5G (fifth generation) mobile network.

NIST Cybersecurity Framework – Voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk.

NIST Risk Management Framework – The Risk Management Framework provides a process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle.

North American Network Operators' Group (NANOG) – An educational and operational forum for the coordination and dissemination of technical information related to backbone/enterprise networking technologies and operational practices.

Open Authorization (OAUTH) – An open standard for the delegation of access to systems.

Open Worldwide Application Security Project (OWASP) – An online community that produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security.

Over-the-Air (OTA) – A technology that updates and changes data in the SIM card without having to reissue it.

Packet Network Data Gateway (PGW) – Acts as the interface between the LTE network and other packet data networks, such as the Internet or SIP-based IMS networks.

Penetration Testing (PT) – Penetration testing is used to test the external perimeter security of a network or facility.

Personal Data Protection Law – Safeguarding of information in any form which identifies an individual, to prevent breach of and protect his/her privacy, especially in light of digital challenges.

Privileged Access Management (PAM) – Computer access with higher access rights than those of a standard user in an enterprise

Privileged identity management (PIM) – Part of privileged access management (PAM) process. PIM involves a set of security controls to monitor, control, and audit access to privileged enterprise identities including service accounts, database accounts, passwords, SSH keys, digital signatures, and so on.

Product Security Incident Response Team (PSIRT) – A dedicated team that receives, investigates, and publicly reports security vulnerability information that is related to their product.

Public Key Infrastructure (PKI) – A Public Key Infrastructure (PKI) is used to confirm identity. It does this by proving ownership of a private key. It is a 'trust service' which can be used to verify that a sender or receiver of data are exactly who they claim to be.

Public Switched Telephone Network (PSTN) – The aggregate of the world's telephone networks that are operated by national, regional, or local telephony operators. It provides infrastructure and services for public telecommunication.

Recovery Point Objectives (RPO) – The point in time to which data must be recovered after an outage.

Recovery Time Objectives (RTO) – The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business processes.

Remote Desktop Protocol (RDP) – A system and network protocol to facilitate remote access to a system over a connected network.

Resource Public Key Infrastructure (RPKI) – RPKI is a cryptographic method of signing records that associate a BGP route announcement with the correct originating AS number.

Response Policy Zones (RPZ) – Response policy zones are a way for you to control what your queriers can and can't look up using a recursive DNS server. By understanding the reputation of the servers and services that clients are querying, you can determine actions to take when the recursive server receives queries for certain domain names or sees information in the DNS responses that point to those malicious servers.

Route Origin Authorization (ROA) – ROA is a cryptographically signed object that states which Autonomous System (AS) is authorized to originate a certain prefix. This means ROAs say something about the BGP announcements that are done with your address space.

Secure Email Gateway (SEG) – A SEG is an email security product that uses signature analysis and machine learning to identify and block malicious emails before they reach recipients' inboxes.

Secure Shell (SSH) – An encrypted communication channel for command-line access to systems.

Secure Telephony Identity Revisited (STIR) – Part of the STIR/SHAKEN or SHAKEN/STIR suite of protocols and procedures intended to combat caller ID spoofing on public telephone networks.

Security Edge Protection Proxy (SEPP) – The 5G function that protects the signaling interconnection point between 5G networks.

Security Incident Response Team (SIRT) – SIRT engineers work for companies to monitor for attacks and work on remediation immediately when they are detected.

Security Information and Event Management (SIEM) – Security information and event management (SIEM) technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources.

Security Orchestration and Response (SOAR) – Technology that helps coordinate, execute, and automate tasks between various people and tools all within a single platform. This allows organizations to not only quickly respond to cybersecurity attacks but also observe, understand, and prevent future incidents, thus improving their overall security posture.

Sender Policy Framework (SPF) – Sender Policy Framework, originally Sender Permitted From, is a path-based Email Authentication technique.

Service-Based Architecture (SBA) – The underlying architectural principle for the 5G core network.

Session Border Controller (SBC) – A special-purpose device that protects and regulates IP communications flows. As the name implies, session border controllers are deployed at network borders to control IP communications sessions.

Short Message Service (SMS) – A text messaging service component of most telephone, Internet, and mobile device systems. It uses standardized communication protocols that let mobile devices exchange short text messages.

Signal Transfer Point (STP) – A Signal Transfer Point is used in a SS7 or CC7 network. The STPs transfer SS7 messages between interconnected nodes (signaling end points) based on information contained in the SS7 address fields.

Signalling System No. 7 (SS7) – A set of telephony signaling protocols developed in the 1970s, which is used to set up and tear down telephone calls in most parts of the world-wide public switched telephone network (PSTN). The protocol also performs number translation, local number portability, prepaid billing, Short Message Service (SMS), and other services.

Signature-based Handling of Asserted information using TOKENs (SHAKEN) – Part of the STIR/SHAKEN or SHAKEN/STIR suite of protocols and procedures intended to combat caller ID spoofing on public telephone networks.

Simple Mail Transfer Protocol (SMTP) – Used to send and receive email. SMTP primarily sends messages to a server for forwarding.

Single-Network Slice Selection Assistance Information (S-NSSAI) – A unique identifier in 5G networks that is used to identify a network slice.

Software as a Service (SaaS) – A software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. SaaS is also known as on-demand software, web-based software, or web-hosted software.

Software Bill of Materials (SBOM) – A list of all the software components contained in a software package, including third-party libraries, drivers, and open-source software packages.

Software Defined Local Area Network (SD-LAN) – A type of networking technology that uses software-defined networking (SDN) principles to manage and optimize the performance of local area networks (WANs).

Software Defined Networking (SDN) – An architecture that decouples the network control and forwarding functions, enabling network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services.

Software Defined Wide Area Network (SD-WAN) – A type of networking technology that uses software-defined networking (SDN) principles to manage and optimize the performance of wide area networks (WANs).

Software Development Lifecycle (SDLC) – A formal or informal methodology for designing, creating, and maintaining software (including code built into hardware).

Source Code Analysis (SCA) – An automated process that identifies the open-source software in a codebase. This analysis is performed to evaluate security, license compliance, and code quality.

Static Application Software Testing (SAST) – Used to secure software by reviewing the source code of the software to identify sources of vulnerabilities.

Subscriber Identity Module (SIM) – The SIM is a smart card necessary to make use of a mobile phone for communication. The SIM is an integrated circuit that is intended to securely store the international mobile subscriber identity (IMSI) number, which is used to identify and authenticate subscribers on mobile telephone systems. Memory is also available on the SIM for personalized data, such as a telephone book and messages.

Subscriber Permanent Identifier (SUPI) – The globally unique 5G identifier for an individual subscriber.

Subscription Concealed Identifier (SUCI) – A unique identifier designed to protect the privacy of the subscriber's identity. It's generated by the User Equipment (UE) using an Elliptic Curve Integrated Encryption Scheme (ECIES)-based protection scheme.

Superuser – A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Telecommunication Information Sharing and Analysis Center (T-ISAC) – GSMA’s central hub of information sharing for the Telecommunication Industry.

Telephone Number Mapping (ENUM) – The mapping of telephone numbers with Internet identification and addressing name spaces. E.164 Number Mapping (ENUM) is an Internet Engineering Task Force (IETF) standard for mapping public switched telephone networks (PSTN) in the DNS.

Temporary Mobile Subscriber Identities (TMSI) – A temporary identification number that is used in the GSM network instead of the IMSI to ensure the privacy of the mobile subscriber.

Transaction Signature (TSIG) – A secure method for communicating from a primary to a secondary Domain Name server (DNS).

Transport Layer Security (TLS) – A cryptographic protocol designed to provide communications security over a computer network. The protocol is widely used in applications such as email, instant messaging, and voice over IP, but its use in securing HTTPS remains the most publicly visible.

Unified Extensible Firmware Interface (UEFI) – A specification for a software program that connects a computer's firmware to its operating system.

Uniform Resource Locator (URL) – The global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use, and the second part specifies the IP address or the domain name where the resource is located.

Uninterruptible Power Supplies (UPS) – A device with an internal battery that allows connected devices to run for at least a short time when the primary power source is lost.

Universal Integrated Circuit Card (UICC) – Smart card (integrated circuit card) used in mobile terminals in GSM and UMTS networks. The primary component of a UICC is a SIM card.

Universal Mobile Telecommunications System (UMTS) – A third generation mobile cellular system for networks based on the GSM standard.

User Entity and Behavior Analytics (UEBA) – A cybersecurity solution that uses algorithms and machine learning to detect anomalies in the behavior of not only the users in a corporate network but also the routers, servers, and endpoints in that network.

User Plane Function (UPF) – The data gateway in 5G networks between mobility RAN and external Data Network.

Virtual Machine (VM) – A compute resource that uses software instead of a physical computer to run programs.

Virtual Private Network (VPN) – A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunnelling links of the virtual network across the real network. For example, if a corporation has LANs at several different sites, each connected to the Internet by a firewall, the corporation could create a VPN by (a) using encrypted tunnels to connect from firewall to firewall across the Internet and (b) not allowing any other traffic through the firewalls. A VPN is generally less expensive to build and operate than a dedicated real network, because the virtual network shares the cost of system resources with other users of the real network.

Vulnerability Assessment (VA) – Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Web Application Firewall (WAF) – A WAF or web application firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet.

Wide Area Network (WAN) – A wide area network is a telecommunications network that extends over a large geographic area. Wide area networks are often established with leased telecommunication circuits.

Write Once Read Many (WORM) – Write-Once, Read-Many is a data storage technology mechanism that stores unerasable and/or unmodifiable information after it has been written on a drive.