Baseline Security Controls

Version 2.0

05 February 2020

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction

1.1 Background

Mobile Network Operators provide the backbone for mobile telecommunication technologies. At enterprise level the industry offers a wide array of services, diversifying from traditional connectivity into content and managed services. At the same time 5.1 billion [1] users depend on Operators to maintain their connectivity; an item considered a basic human right under UN Article 19 [2]. This results in a mixed threat landscape of traditional IT, radio and mobile related threats.

Based on this position the industry has a responsibility to secure customer information and services. The GSMA has developed the following baseline security controls to help Operators understand and develop their security posture to a foundation (base) level.

These controls are not binding; this is a voluntary scheme to enable an Operator to assess and understand their own security controls. The GSMA do not require access to the results but are suitably positioned to discuss specific output and identify remedial resources if desired.

1.2 Scope

This document outlines a specific set of security controls that the mobile telecommunications industry should consider deploying. The solution description identifies specific advice that would allow the Operator to fulfil the control objectives.

These controls stand separate to, but may be supported by, local market legislation and regulation. They do not replace or override local regulations or legislation in any territory. Their purpose is to enhance and supplement security levels within the mobile telecommunications industry.

1.3 Intended Audience

This document has been created as a list of controls, supported by a checklist of questions related to the controls (Annex A). It is recommended that the checklist be completed by a person, or team, associated with the controls. The overarching output is intended for use by the senior security personnel to understand the Operator’s internal security posture.

1.4 How to use this Document

Operators utilising these controls should compare the control(s) listed to their deployed internal security controls, identify and assess potential gaps, then respond to highlighted gaps within their organisation(s). The assessment can be completed using the checklist included in Annex A. Table 1 outlines the potential responses to the questions in Annex A. These responses are aligned to recognize levels of maturity of information security and business controls. Levels 1 through to 5 represent recognition of the control and progress in development of its maturity. Level 0 has been added to reflect the stage prior to recognition of the need for implementation of the control. Controls can also be identified as Not Applicable (N/A) provided that the control has been reviewed and there is a justification as to why it is not applicable within a given context.

NOTE Failure to populate the checklist with accurate information will reduce its effectiveness.

How the controls are implemented is the responsibility of the Operator and specifics are not covered in this document. It is expected that internal implementation documentation or solutions are understood and approved by the Operator's Chief Information Security Officer (CISO) or equivalent. These are baseline (minimum) controls; if the assessed Operators have already implemented security controls that are considered more secure than those listed in this document the GSMA does not recommend reducing the security level implemented.

The GSMA provides supporting documentation, by way of Permanent Reference Documents (PRD), that outline specific details of some controls and recommendations, these are located on the InfoCentre. These may be beneficial to an Operator that identifies a gap in its technical controls.

The GSMA recognises the industry standard work by the Centre for Internet Security (CIS) Controls [3] and has aligned to these wherever appropriate. Where the controls have been used this is referenced into the Reference field. It should be noted that as CIS is focussed upon general computing cyber-security, therefore not all CIS controls are incorporated within the baseline: only those relevant to typical Operator systems.

It is also not rational to universally adopt a target maturity of Level 5 for all controls: only what is appropriate and proportionate for each of those controls. Typically, an organisation will first identify a strategic plan for maturity improvement over time. For instance, a limited set of the most significant controls could be targeted for improvement in Year 1, further controls improved in Year 2, within a strategic five-year plan aiming for an eventual target level of maturity profile tuned for each of the controls. An example is provided in the companion Annex A Excel tool, which is used to self-assess maturity.

Maturity Marking	Definition
N/A: Not Applicable	The GSMA baseline security control objective does not apply to the Operator. All 'N/A' responses should be supported with an explanation in the corresponding 'Notes' column.
Level 0: None	Control not present and has not yet been considered for implementation by the Operator. All 'Level 0' responses should be supported with an explanation in the corresponding 'Notes' column.
Level 1: Initial	The Operator has considered the control for implementation and has undertaken a gap analysis of the control against current policy and practice. There may be ad-hoc or localised implementation of the control, but the control is not supported strategically. A control improvement road map has been prepared to increase the level of maturity to an applicable target level of maturity. An outline of the road map and/or reference to it should be recorded in the corresponding 'Notes' column.
Level 2: Repeatable	The control has started to be adopted within the Operator's policies and practices. Progress has been made on its implementation and is included within a detailed programme of work which is underway. Progress is regularly reviewed by a programme board and where the control is implemented it is to a consistent, repeatable, standard. Progress of implementation of the control on the road map and programme plans should be recorded in the 'Notes' column.

Maturity Marking	Definition
Level 3: Defined	The control has been fully adopted within the Operator’s policies and practices. The control has started to be embedded in governance and management processes, but this is not yet complete. Resourcing and training plans cover oversight of the control and these have started to be implemented. Progress of implementation of the control on the road map, programme and resourcing/training plans should be recorded in the ‘Notes’ column.
Level 4: Managed	The governance and management processes that oversee and operate the control are now fully in place and largely resourced by appropriately skilled and trained personnel. Plans are developed to monitor the effectiveness of the control and to put into place a process of regular review and improvement of the control. This includes considering feedback on control effectiveness from incident investigations and reviews. Progress of implementation of the control on the road map, programme/resourcing/training plans and review/improvement plans should be recorded in the ‘Notes’ column.
Level 5: Optimized	The control review/improvement processes are embedded and operating effectively (this level of maturity should not be claimed until those processes have undertaken several review cycles, e.g. six months or more). The control oversight has moved from the programme mode to business-as-usual status. Current control effectiveness status and improvement plans should be recorded in the ‘Notes’ column.

Table 1: Response to Security Controls/Maturity Levels

1.5 Terms of Use

This document is provided by the GSMA for information and Members internal use only. It is provided “as is” without any warranty and liability to the GSMA and its Members. The GSMA and its Members cannot be held accountable or liable for the use of the document.

1.6 Abbreviations

Term	Description
3DES	Triple Data Encryption Standard
3GPP	3rd Generation Partnership Project
AES	Advanced Encryption Standard
API	Application programmable interface
AUSF	Authentication Server Function
BAU	Business as Usual
BC	Business Continuity
BCM	Business Continuity Management
BSI	British Standards Institute
BSS	Business support services
BSIMM	Building Security in Maturity Model
CA	Certificate Authority
CAB	Change Approval Board

Term	Description
CASB	Cloud Access Security Broker
CIS	Centre for Internet Security
CISO	Chief Information Security Officer
CKMS	Cryptographic Key Management System
CPE	Customer Premise Equipment
CRL	Certificate Revocation List
CSIRT	Computer Security and Incident Response Team
DES	Data Encryption Standard
ECIES	Elliptic Curve Integrated Encryption Scheme
EIR	Equipment Identity Register
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
eUICC	Embedded UICC
FASG	Fraud and Security Group
FFG	Fire, Flood and Gas
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
GGSN	Gateway GPRS support node
GPRS	General Packet Radio Services
GRC	Governance, Risk and Compliance
GSM	Global System for Mobile – 2G Network
GSMA	GSM Association
GT	Global Title
GTP	GPRS Tunnelling Protocol
HLR	Home Location Register
HSM	Hardware Security Module
HSS	Home Subscriber Server
HTTPS	Secure Hypertext Transfer Protocol
HVAC	Heating, Ventilation and Air Conditioning
IDPS	Intrusion detection and prevention services
IETF	Internet Engineering Task Force
IMEI	International Mobile Equipment Identity
IoT	Internet of Things
IP	Internet Protocol
IPsec	Internet Protocol Security
IPX	Internetwork Packet Exchange
iUICC	Integrated UICC
LTE	Long Term Evolution - 4G Network

Term	Description
MAP	Mobile Application Part
MME	Mobility Management Entity
MMS	Multimedia Messaging Service
MMSC	Multimedia Messaging Service Centre
NAS	Non-Access Stratum
NE	Network Element
NESAS	Network Equipment Security Assurance Scheme
NFV	Network Function Virtualisation
NIST	National Institute for Science and Technology (US)
NR	New Radio
OEM	Original equipment manufacturer
OSINT	Open Source Intelligence
OTA	Over the air
PAM	Privileged Account Management
PDN GW	Packet Data Network Gateway
PIN	Personal Identity Number
PKI	Public Key Infrastructure
PMN	Public Mobile Network
PRD	Permanent Reference Document
RAEX	Roaming Exchange
RAN	Radio Access Network
RCS	Rich Communication Services
RFC	Request for Comment
RSA	Rivest–Shamir–Adleman
SAE	System Architecture Evolution
SAML	Security Assertion Mark-up Language
SAS	Security Accreditation Scheme
SDLC	Software Development Lifecycle
SFTP	Secure File Transfer Protocol
SGSN	Serving GPRS Support Node
SGW	Serving Gateway
SIEM	Security Information and Event Management
SIGTRAN	Signalling Transport
SIM	Subscriber Identity Module
SLT	Security Leadership Team
SMS	Short Message Service
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Centre

Term	Description
SS7	Signalling System 7
SSL	Secure Sockets Layer
STP	Signal Transfer Point
SUCI	SUbscription Concealed Identifier
T-ISAC	Telecommunication Information Sharing and Analysis Centre
TDE	Transparent Data Encryption
TMSI	Temporary Mobile Station Identity
TRE	Tamper Resistant Element
UE	User equipment
UICC	Universal integrated circuit card
UMTS	Universal Mobile Telecommunication Service - 3G Network
UTRAN	UMTS Terrestrial RAN
VLAN	Virtualised Local Area Network
VPN	Virtual Private Network

1.7 Definitions

Term	Description
Anomaly	A deviation from the common rule.
Authentication Server Function (AUSF)	The AUSF performs UE authentication in 5G networks.
Cloud Access Security Broker (CASB)	Technology used to control access to cloud tenants and users in a distributed cloud computing environment. Typically incorporated single-sign on and ticketing methods such as SAML to control access to cloud resources and direct requests over load balanced infrastructures.
Core Network	According to 3GPP the core network consists of different technology and infrastructure depending on the generation of mobile telecommunications network: GSM: Circuit switching network elements (NE) UMTS: Packet switching and Circuit Switching NE GPRS: Packet switching NE LTE: Evolved packet core (EPC) NE 5G: 5G NE
Cryptographic Key Management System	A framework and services that provide for the generation, establishment, control, accounting, and destruction of cryptographic keys and associated management information. It includes all elements (hardware, software, other equipment, and documentation); facilities; personnel; procedures; standards; and information products that form the system that establishes, manages, and supports cryptographic products and services for end entities (NIST SP 800-57).
Evolved Packet Core	LTE's core network, consisting of the Home Subscriber Server (HSS), serving Gateway (SGW), Packet Data Network Gateway (PDN GW) and Mobility Management Entity (MME) [4].

Term	Description
Embedded UICC (eUICC)	A UICC which is not easily accessible or replaceable, is not intended to be removed or replaced in the Device and enables the secure changing of subscription Profiles.
GSMA Fraud and Security Group (FASG)	A working group focused on the fraud and security needs of the mobile ecosystem.
Gateway GPRS Support Node (GGSN)	The GGSN is responsible for the internetworking between the GPRS network and external packet switched networks.
General Packet Radio Service (GPRS)	GPRS is a protocol used to carry packet-switched data traffic on mobile telecommunications networks.
GPRS Tunnelling Protocol (GTP)	GTP is a set of protocols used to carry GPRS signalling and user plane traffic within the mobile telecommunications network.
Hardware Security Module (HSM)	A HSM is a dedicated hardware component used to securely manage key material and/or sensitive processing
Home Subscriber Server (HSS)	A Home Subscriber Server (HSS) is a database within an LTE network that contains user-related and subscriber-related information [4].
Interception	Interception attacks include any attacks (passive or active) where the attacker attempts to intercept or re-route traffic/data for their own gains.
IPX Provider Network	The part of the IPX Network that is operated by one IPX Provider. All IPX Provider Networks together build the global IPX Network.
Integrated UICC (iUICC)	A UICC implemented on a Tamper Resistant Element (TRE) that is integrated into a System-on-Chip (SoC), optionally making use of remote volatile/non-volatile memory
Know your customer	Implement appropriate customer relationship management, accounting and utilisation systems to understand customer requirements and behaviours. It can also refer to due diligence in establishing and operating customer accounts and monitoring for breaches of usage conditions.
Maturity Model	A broadly recognized tool, with increasing levels, that assesses the maturity of the implementation of business strategies and controls (including information security management). The model proposed for the purposes of this document is defined in Table 1 on page 5.
Mobility Management Entity (MME)	The MME handles the signalling related to mobility and security for E-UTRAN access in LTE networks. The MME is responsible for the tracking and the paging of UE in idle-mode. It is the termination point of the Non-Access Stratum (NAS) [4].
Multimedia Messaging Service Centre (MMSC)	The multimedia messaging service is a standard way to send messages that include multimedia content to and from a mobile phone over a cellular network. The MMSC acts as a relay or forwarding station for these messages.
Mobile Network Operator (MNO)	A mobile network Operator carries out provisioning, billing and engineering for mobile services. A full member of the GSMA.
New Radio	5G’s radio interface

Term	Description
Network Element	Any active component on the network involved in sending, receiving, processing, storing, or creating data packets and/or voice traffic. In the mobile network, components like the Serving GPRS Support Node (SGSN), Gateway GPRS Support Node (GGSN), Mobility Management Entity (MME), Serving Gateway (SGW), Packet Data Network Gateway (PGW), Home Location Register (HLR), Home Subscriber Server (HSS), and GTP firewall, as well as routers and gateways, are network elements.
Network Equipment Security Assurance Scheme (NESAS)	NESAS is a voluntary network equipment security assurance scheme operated and maintained by GSMA, with contributions from 3GPP, covering the methodology and security targets for equipment under test. It defines a globally applicable security baseline that network equipment vendors can meet.
Organization	This is a term that can apply to any member, manufacturer, Operator or business entity within the scope of the GSMA membership.
Packet Data Network Gateway (PDN GW)	The PDN GW provides connectivity from mobile devices to external packet data networks in LTE networks.
Physical security	Security controls to protect physical components of a network.
Privileged Account Management (PAM)	System that controls access to and accounts for use of privileged user functions and security critical functions. It can also add additional rules-based authentication layers for exercise of privileges.
Security Orchestration, Automation and Response (SOAR)	SOAR represents a combination of technology and disciplines to control security operation of resource allocation (compute, storage, network and peripheral access) and mobility within virtualized, containerised, compartmentalized, cloud computing and/or distributed data centre environments.
Security Accreditation Scheme (SAS)	The SAS is a GSMA certification scheme providing assurance that suppliers manufacture and/or manage UICCs, eUICCs and iUICCs in a secure way.
Serving Gateway (SGW)	The SGW is the point of interconnect between the radio-side and the LTE EPC; the gateway serves the UE by routing the incoming and outgoing IP packets [4].
Serving Gateway (SGW)	The SGW is the point of interconnect between the radio-side and the EPC; the gateway serves the UE by routing the incoming and outgoing IP packets [4].
Short Message Service (SMS)	Also known as text messaging that uses standardised communication protocols to exchange short text messages
Short Message Service Centre (SMSC)	A SMSC is a network element in the mobile telephone network which delivers SMS messages.
Signalling System 7 (SS7)	SS7 is a protocol allowing phone networks to exchange information needed for managing subscriber mobility and connections, and routing calls and text messages.
Signal Transfer Point (STP)	A STP is a router that relays SS7 messages between certain network elements.

Term	Description
User Equipment (UE)	Devices used by the end user.
Universal Integrated Circuit Card (UICC)	The UICC is the smart card used in mobile terminals to manage subscriber credentials and network access.
Vendors	An organisation offering a product or service used by the mobile telecommunications industry.
Virtual Private Network (VPN)	A VPN extends a private network across a public network.
Vulnerability	A vulnerability is generally a set of conditions that allow the violation of an explicit or implicit security policy.

1.8 References

Ref	Document	Link
[1]	GSMA Intelligence Global Mobile Trends	GSMAi
[2]	UN Human Rights Council	Article 19
[3]	Centre for Internet Security (CIS) Controls	CIS Controls
[4]	The Evolved Packet Core	3GPP EPC
[5]	NIST SP 800-57 Recommendation for Key Management Part 2	NIST SP 800-57
[6]	GSMA Coordinated Vulnerability Disclosure (CVD) Programme	GSMA CVD
[7]	Bringing science to software security	BSIMM
[8]	Effective Business Continuity Management Guidelines for Mobile Network Operators	GSMA BCM Guidelines
[9]	GSMA Network Equipment Security Assessment Scheme (NESAS)	GSMA NESAS
[10]	IMEI Security Technical Design Principles	GSMA
[11]	Requirements for Mobile Device Software Security Updates	PRD FS.25
[12]	SG.15 Guidance for Operators on security mechanisms	PRD SG.15
[13]	Anti-Theft Device Feature Requirements	PRD SG.24
[14]	GSMA IMEI Database	GSMA IMEI Database
[15]	SAS Certified Sites	SAS Certified Sites
[16]	SIM Alliance S@T Specifications	S@T Specifications
[17]	GSMA Security Manual	PRD FS.30
[18]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators	NIST SP 800-90A
[19]	FS.28 Security Guideline for UICC credential protection	PRD FS.28
[20]	Security Requirements for Cryptographic Modules (FIPS140-2)	FIPS1402
[21]	GSMA eUICC Compliance	eUICC Compliance

Ref	Document	Link
[22]	Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model	ISO 15408
[23]	IoT Security Guidelines Overview Document	GSMA CLP.11
[24]	IoT Security Guidelines for IoT Service Ecosystem	GSMA CLP.12
[25]	IoT Security Guidelines Endpoint Ecosystem	GSMA CLP.13
[26]	IoT Security Guidelines for Network Operators	GSMA CLP.14
[27]	IoT Security Assessment Process	GSMA CLP.19
[28]	GSMA IoT Security Assessment Checklist	GSMA CLP.17
[29]	IoT Device Connection Efficiency Guidelines	GSMA TS.34
[30]	IoT Device Connection Efficiency Test Book	GSMA TS.35
[31]	FF.21 The Fraud Manual	PRD FF.21
[32]	Small Cell Forum Comprehensive overview of small cell security	Small Cell Forum: SCF171
[33]	FS.20 GPRS Tunnelling Protocol (GTP) Security	PRD FS.20
[34]	IR.88 LTE and EPC Roaming Guidelines	PRD IR.88
[35]	FS.11 SS7 Interconnect Security Monitoring and Firewall Guidelines	PRD FS.11
[36]	FS.07 SS7 and SIGTRAN Network Security	PRD FS.07
[37]	IR.77 InterOperator IP Backbone Security Req. For Service and Inter-Operator IP backbone Providers	PRD IR.77
[38]	IR.21 GSM Association Roaming Database, Structure and Updating Procedures	PRD IR.21
[39]	IR.85 Roaming Hubbing Provider Data, Structure and Updating Procedures	PRD IR.85
[40]	3GPP Confidentiality algorithms	3GPP
[41]	IR.88 LTE and EPC Roaming Guidelines	PRD IR.88
[42]	SG.20 Voicemail Security Guidelines	PRD SG.20
[43]	Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture	ETSI TS 133 102
[44]	3GPP System Architecture Evolution (SAE); Security architecture	3GPP 33.401
[45]	SMS Firewall Best Practice and Policies	PRD SG.22
[46]	GSMA IMEI Blacklisting	GSMA IMEI Blacklisting
[47]	SG.15 Guidance for Operators on security mechanisms	PRD SG.15
[48]	Small Cell Forum Comprehensive overview of small cell security	Small Cell Forum: SCF171
[49]	Security Recommendations for Server-based Hypervisor Platforms	SP 800-125A Rev. 1

Ref	Document	Link
[50]	BSI TR-02102 Cryptographic Mechanisms	BSI TR-02102
[51]	NIST SP 800-57 Recommendation for Key Management Part 1	NIST.SP.800-57
[52]	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	RFC3647
[53]	EV SSL Certificate Guidelines	CAB Forum
[54]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	RFC5280
[55]	NIST SP 800-57 Recommendation for Key Management Part 2	NIST SP 800-57
[56]	Telecommunication Information Sharing and Analysis Centre	T-ISAC
[57]	ISO/IEC 27035:2016 — Information technology — Security techniques —Information security incident management	ISO27035
[58]	GSMA Anti-Theft Device Feature Requirements	GSMA Kill Switch
[59]	Diameter Interconnect Security	PRD FS.19
[60]	5G Security Edge Protection Proxy Technical Specification	3GPP TS 33.501

2 Baseline Security Controls

This section defines the Baseline Security Controls. It is divided into several sub-sections and tables that are organized depending on the applicability of the types of GSMA Operator members and other stakeholders.

Operators should complete the corresponding Annex A sub-sections according to the relevance to the services they provide.

Each table is organised into three columns:

- **Reference** – the unique reference for Baseline Security Control set;
- **Objective** – the objective that is to be achieved by implementation of each control set;
- **Solution Description** – the envisaged set of controls and standards applicable to each control objective. Where greater detail is available in external standards and documents these are referenced in square brackets (refer to the References Table within sub-section 1.8).

NOTE The numbered items given under the Solution Description do not correspond to the maturity levels used to score the controls. Rather, these indicate a sequence of controls that can be applied to each Objective.

2.1 Business Controls

Business controls are controls that relate to how the overarching enterprise manages security. They are not necessarily technical in nature and may relate to reporting or communication procedures that are essential for an Operator to support business objectives regarding security.

These controls are likely to be understood and managed by the security leadership team (SLT), this team would be able to comment on how these controls are implemented.

Reference	Objective	Solution Description
BC-001	**Board Level Engagement**, where organisations fail to recognise security at Board level there is likely to be a gap in the way the organisation understands their success, risk posture, priorities and future investment on programmes. This gap introduces unnecessary security and fraud risks.	1. Regular security briefing to Board Level 2. Specific security strategy with direct senior level reporting 3. Clear board level ownership of information security risks and issues 4. Sponsorship for information security risk management funding and resourcing
BC-002	Organisations should have a **role formally recognising security** as a responsibility, CISO's often fulfil this role. Alternatively, it can be any person of senior standing, their role must be able to influence and direct enterprise level investment and change.	1. Named, accountable role 2. Formally recognised integration with organisation 3. Responsibility includes regular briefing into senior leadership 4. Formal mandate and budget
BC-003	**Organisational policies** are a set of rules that the organisation should abide by. Specific policies will be constructed in relation to security and should map to the overarching security strategy and principles of the organisation; essentially policy should underpin the organisation's security objectives.	Specific policies pertaining to (at least): a. 3rd party data/supply chain security management b. Access Control c. Asset management; including architectural design, in life management, and decommissioning d. Business continuity management e. Cloud security f. Cryptographic material management [5] g. Device, system and network asset security h. Information classification and handling i. Personnel security j. Physical security k. Risk management l. Security incident management; including breach notification m. Security monitoring; including reporting to compliance programme n. Software security update management o. Staff training and awareness p. Vulnerability disclosure management [6]

Reference	Objective	Solution Description
		Further details are provided in Annex B.
BC-004	**Governance, risk and compliance** (GRC) are three functions that complement each other, providing reporting processes to detail operational progress against strategic requirements. Governance should align to organisation policy; reporting is shared with senior leadership to explain the delivery success of the entire security programme.	1. Defined security compliance reporting to business 2. Formal security audit programme 3. Formal security governance programme that aligns with organisational policy 4. Security risks aligned to business risks 5. Programme(s) exist to implement strategy and plans for the maturity of information security risk management controls 6. Appropriate escalation paths for significant information security risks and issues 7. Security is embedded within the organisation culture and business-as-usual practices 8. Regular audits and inspections of compliance against security policies 9. Regular information security risk management improvement reviews
BC-005	Ensure all projects go through a **security assessment** to confirm they are **secure by design**.	1. Project design process with defined security acceptance stage including active verification (e.g. pen testing vulnerability scans, red team exercises, etc.) 2. Threat modelling based on project prioritisation and purpose 3. Select appropriate technical and non-technical controls for implementation based upon the outcome of an information security risk assessment and management activity
BC-006	Ensure all projects go through a **data protection/privacy assessment**. This assessment should align to local policy, industry regulation and relevant legislation. These will inform local data management principles.	1. Local data protection principles applied 2. Personal data identification 3. Meeting of regulatory requirements for data protection, subject access, telecommunications regulation and freedom of information requirements
BC-007 / CIS-007	**Secure Software Development Life Cycle (SDLC) implemented**, this lifecycle should include quality control stages, with code review at module and system level, including both static and dynamic testing. Code language choice considers	1. Application Programmable Interface (API) development and implementation included in SDLC 2. Open source and purchased software included in SDLC

Reference	Objective	Solution Description
	security issues such as type safety and vulnerable functions.	3. Recognised, industry standard set of secure coding practices enforced e.g. BSIMM [7]
BC-008	**Business Continuity Management** (BCM) improves the resilience of the organisation. Developing and organisation's **ability to detect, prevent, minimise and deal with the impact of disruptive events**. In the aftermath of an incident the BCM plan will enable critical activities within the organisation to continue. In the longer term it will help the business to recover and return to Business as Usual (BAU).	1. Crisis communication measures in place 2. Operator BCM process, exercised annually [8] 3. Service specific documented BCM process, exercised annually 4. Effective backup processes (with regular tests of recovery) 5. Capacity planning and management controls to prevent avoidable network outages 6. Disaster recovery facilities, planning and testing 7. Architectures designed to eliminate single-points of failure with redundancy, cut-over management and load-balancing
BC-009	**Physical security controls.** To reduce the risk of a physical attack being used to facilitate a logical attack an Operator's security strategy should consider physical and logical security controls holistically.	1. Environmental controls such as fire, flood and gas (FFG) and heating, ventilation, and air conditioning (HVAC) interlinked with security management 2. Facilities maintenance reporting interlinked with security management 3. Site access management controls implemented a. Include cell and customer premise equipment (CPE) sites where possible 4. Physical security standards and risk assessments depending on the class of sites (office environments, data centres, operations centres, remote sites (manned/unmanned/lights-out), public access)
BC-010	Operators should implement effective supply-chain and **procurement controls** to ensure the services they operate and provide comply with legal requirements and manage supply-chain threats.	1. Security hygiene expectations e.g. patching 2. Ownership of the service and infrastructure 3. Industry standard assessment programmes to assure vendor products e.g. NESAS [9] 4. Mapping planned logical interconnects 5. Mapping planned physical interconnects 6. Life-time support arrangements

Reference	Objective	Solution Description
BC-11	Operators should implement **3rd party** access and **outsourcing controls** to ensure the risks of information sharing and outsourcing are effectively managed.	1. Processes to identify, prioritize and assess suppliers and partners of critical systems, components and services using a supply chain risk assessment process. 2. Procedures exist to identify and manage the risks associated with third-party access to the organization's systems and data. 3. Security controls required of internal staff and resources, including privileged access (NO-005 / CIS-004), are mirrored with prioritized suppliers 4. Contract and due diligence checks for prioritized suppliers, these should be based on a pre-procurement risk assessment 5. Breach notification from supplier
BC-12	**Decommissioning of equipment** should consider secure sanitization or disposal controls to avoid the risks of consequent data leaks.	1. Testing accounts, removing access 2. Deleting and sanitizing data, configurations and memory 3. Policy for reuse, selling, and disposal/destruction of equipment 4. Compliance with environmental, recycling, reuse and disposal regulations

2.2 Technological Controls

Each of the technical controls outlined are required to secure a mobile telecommunications network. The sections represent the operational team who may manage the control's area of responsibility. This team, or area, is likely to be able to comment on the Operator's solution within their network.

2.2.1 User Equipment and Mobile Equipment Controls

These controls are likely to be understood and managed by the mobile device team.

Reference	Objective	Solution Description
DC-001	Source devices that have **secure IMEI implementations**.	Purchase devices with secure IMEI implementations, that comply with the GSMA's IMEI security design principles [10]
DC-002	**Deliver security critical software updates** to vulnerable mobile devices with minimal delay.	Deliver security patches to vulnerable devices within 2 weeks of receipt from original equipment manufacturers (OEM) [11]
DC-003	**Prevent the connection and use** of stolen, defective or counterfeit devices.	1. Block duplicate or invalid IMEI numbers 2. IMEI checks should be carried out to verify that the device is not blacklisted

Reference	Objective	Solution Description
		prior to providing mobile network access [12] 3. Implement and manage an Equipment Identity Register (EIR) [13] 4. Share stolen device data with the GSMA's IMEI Database [14] 5. Encourage implementation of device based anti-theft features by device manufacturers and use of them by customers [58]

2.2.2 (e)UICC Management Controls

These controls are likely to be understood and managed by the SIM management team.

Reference	Objective	Solution Description
SIM-001	Establish, implement and actively manage a rigorous **SIM management programme.** This programme must focus on the secure provisioning and purchase of (e)UICC from reputable vendors.	Confirm that the UICC supplier: a. Sources UICC/eUICC cards from SAS certified production sites [15] b. Implements Over the air (OTA) functions that are not vulnerable to known attacks [16] c. Ensure SIM based web browsers are securely deployed and configured with appropriate minimum security levels enabled d. Implements appropriate authentication algorithms i.e. resistant to brute force attacks [17] e. Implements Authentication counters and similar mechanisms to protect against brute force attacks on physical UICC f. Uses secure random number generators [18] to create the 'seed' material for common and unique (e)UICC credentials [19], [20] g. Implements appropriate protection for subscriber keys in storage and in transit (between SIM vendor and Operator), at record layer (AES), file layer (AES, ECIES or RSA) and in transport (HTTPS, FTPS, SFTP) h. Implements mechanisms to protect against side channel analysis attacks such as differential power analysis
SIM-002	Source eUICCs that comply with the GSMA eUICC specifications, and have declared compliance under the	This requires:

	GSMA eSIM/M2M compliance programmes [21]	a. eUICC production at a SAS accredited site(s) b. Security assurance to GSMA's defined security objectives, with resistance against ISO15408 [22] defined attacks c. Certified functional compliance to the specifications

2.2.3 Internet of Things Controls

The Internet of Things (IoT) is projected to grow rapidly over the next few years. Operators are diversifying and providing managed IoT services as well as hosting data generated from IoT endpoints. IoT services should be deployed and managed in a secure way and the team managing this product set should understand the following controls.

Reference	Objective	Solution Description
IOT-001	IoT service providers shall comply with **security by design** and **privacy by design** industry best practice.	Implement the guidelines stated in GSMA CLP.11 IoT Security Guidelines Overview Document [23]
IOT-002	IoT service platforms shall comply with **IoT security industry best practice**.	Implement the guidelines stated in GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystem [24] document.
IOT-003	IoT device endpoints shall comply with **IoT security industry best practice**.	Implement the guidelines stated in GSMA CLP.13 IoT Security Guidelines Endpoint Ecosystem [25] document.
IOT-004	Networks shall comply with **IoT security industry best practice**.	Implement the guidelines stated in GSMA CLP.14 IoT Security Guidelines for Network Operators [26] document.
IOT-005	IoT services shall subject to a **security assessment**.	Complete of an IoT security assessment as described in GSMA CLP.19 IoT Security Assessment Process [27] document and GSMA CLP.17 GSMA IoT Security Assessment Checklist [28] document.
IOT-006	IoT device endpoints shall comply with **connection efficiency best practices** to protect networks from the risks caused by the mass deployment of inefficient, insecure or defective IoT devices.	Ensure IoT devices comply with the guidelines stated in GSMA TS.34 IoT Device Connection Efficiency Guidelines [29] and test devices according to GSMA TS.35 IoT Device Connection Efficiency Test Book [30].

2.2.4 Radio Network Controls

These controls are likely to be understood and managed by the radio network team.

Reference	Objective	Solution Description
RN-001	**Cryptographically protect GSM, GPRS, UMTS, LTE and NR network traffic** to protect against unauthorised interception and	1. Enable the strongest encryption mechanisms defined in standards. For GSM, enable A5/3 and ideally A5/4 as well as A5/1. For GPRS, enable GEA3 and ideally GEA4

Reference	Objective	Solution Description
	alteration of user traffic and sensitive signalling information.	2. Ensure that control plane integrity protection in UMTS, LTE or 5G is correctly enforced 3. Ensure that user plane integrity protection in 5G is enforced 4. Protect the S1 interface between eNodeB/gNodeb and core network e.g. deploy IPsec where appropriate 5. Protect the X2 interface between eNodeBs and gNodeBs e.g. deploy IPsec where appropriate
RN-002	**Prevent user tracking** though the appropriate use of temporary device identities, for instance before the device has authenticated to the network	1. Use 3GPP defined standard temporary identifiers e.g. SUCI, TMSI when transferring unprotected device information across the network
RN-003	Detect attacks that may result in network instability; **locate anomalous activity in the network**	1. Monitor for and respond to traffic fluctuations, unusual handover patterns, dead spots and service disruption that may be due to jammers or false base stations [31] 2. Monitor the distribution of base station equipment 3. Prevent/detect bidding down attacks, authenticate as far as possible using techniques such as in IR.77 [37] and configure radio network components to detect spoofing, mis-addressing/mis-routing and discard mal-formed traffic
RN-005	Ensure RAN sharing initiatives **isolate data, user and control traffic** correctly	1. Design a RAN architecture that incorporates appropriate segregation of the different traffic classes using spectral or logical means 2. Segregate traffic of different Operators 3. Implement utilisation and accounting frameworks for resource sharing 4. Rigorously test all segregation mechanisms 5. Ensure traffic quality-of-service, prioritization and pre-emption characteristics are preserved
RN-006	Ensure **base stations are secured and maintained**	1. Ensure physical site security controls are implemented 2. Secure interfaces and management channels
RN-007	Where **small cells** are deployed in hostile environments compensating	1. Secure interfaces and management channels

Reference	Objective	Solution Description
	controls should be implemented to **manage the risk** [32].	2. Ensure small-cells are tamper resistant and tampering triggers a monitored alarm system 3. Source small-cells with a: a. Trusted environment b. Trusted boot process c. Location verification d. Network isolation capability

2.2.5 Roaming and Interconnect Controls

These controls are likely to be understood and managed by the roaming and interconnect team.

Reference	Objective	Solution Description
RI-001	**Protection of the roaming and interconnect messaging and customers** from attacks including location tracking, eavesdropping, denial of service and fraud over interconnect signalling protocols and links.	1. Block malformed interconnect signalling packets 2. Confirm interfaces are only accessible to the correct external applications and/or networks, internal network elements and business support services (BSS) 3. Deploy Diameter proxies for each Diameter application supported by the public mobile network (PMN), through an Internetwork Packet Exchange (IPX) Diameter agent [33], [34] 4. Deploy message monitoring and filtering capabilities to identify and block malformed, prohibited and unauthorised packets i.e. SS7 for 2/3G [35], [36] Diameter for LTE [**Error! Bookmark not defined.**] and 5G prepare for SEPP deployment [60]. 5. Enable IR.77 binding security requirements for IPX Provider Networks [37] 6. Rate limit interconnect traffic, reducing the risk of a denial of service attack 7. Remediate inappropriate interconnect access by third parties e.g. Global Title (GT) leasing 8. Signalling message traffic filters should be implemented, only accepting incoming traffic from known peer Operators where a roaming agreement exists [34]

Reference	Objective	Solution Description
RI-002	**Protect the roaming and interconnect network elements (NE)** from unauthorised access.	1. Assign disjoint IP address segments for each of the networks [37] 2. Disable the ability to access roaming and interconnect NE from the internet or UE IP addresses [37] 3. Keep networks separated physically by separate connections, or logically separate on layer 2 (e.g. through the use of a VPN or VLAN) [37] 4. Keep networks separated in shared equipment, such as routers or switches, by having independent virtual routing and forwarding instances or VLANs [37] 5. Do not allow shared, default or hardcoded passwords
RI-003	Maintain an **accurate record of roaming information**.	Maintain data recorded in the Roaming Exchange (RAEX) using IR.21 [38] /IR.85 [39]
RI-004	**Monitor and analyse radio network traffic** for potential internal or external attacks.	1. Enable audit logging and deliver data to Security Incident and Event Management (SIEM) for analysis for relevant threat vectors 2. Ensure integrity of audit data e.g. from the use of digital signatures

2.2.6 Core Network Management Controls

The Core Network (CN) definition has been taken from the 3GPP standards[3]. These controls are likely to be understood and managed by the Core Services Management.

Reference	Objective	Solution Description
CN-001	There should be processes for the **secure provisioning and decommissioning of users** to ensure only legitimately subscribing customers have access to services.	1. User ID (no wildcards) 2. Correct linkage between customer and UE 3. Authenticate every user on every network attach, location update, traffic event, etc. 4. Implement know your customer (KYC) systems and initiatives
CN-002	**Protect core network traffic** after it is handed over from the radio path to protect against unauthorised interception and alteration of user traffic and sensitive signalling information.	1. Deploy encryption to protect the interface between eNodeB/gNodeB and the core network e.g. by using IPsec 2. Enable end entity certificates as defined in 3GPP TS 33.310 [40] 3. Actively manage GTP_U and GTP_C firewalls between the EPC and IPX

Reference	Objective	Solution Description
		network, dropping malformed before it leaves the core [41]
CN-003	**Prevent eavesdropping, the unauthorised deletion and modification of voicemail** content, settings and greetings and call break out to generate fraudulent traffic.	1. Enforce use of unobvious, variable length access PINs [42] 2. Notify customers of failed access attempts [42] 3. Require PIN entry for direct access to voicemail from outside home network, except in cases where the Calling Line Identifier can be reliably assured to be correct [42] 4. Restrict the number of PIN access attempts independently from the Calling Line Identifier [42] 5. Securely generate, distribute and manage PINs [42] 6. Set the frequency at which a new or replacement temporary identifier is allocated to provide adequate protection
CN-004	Use **customer anonymization techniques** to protect identifiers that can be used to identify and track individual customers.	Enable the use of temporary identifiers for customers, as defined in the standards [43], [44]
CN-005	**Prevent unsolicited messaging traffic** (RCS, SMS and MMS) reaching unsuspecting customers and causing potential harm to the network, including denial of service against network elements.	1. Configure available SMSCs, STPs and SMS firewalls to reduce risk of OTA SMS attacks [45], [16] 2. Deploy SMS home routing to ensure visibility and control of messaging traffic 3. Deploy traffic filtering capabilities on the network GGSN, MMSC, SMSC and/or STP 4. Provide customer facing spam reporting and blocking capabilities
CN-006	To prevent fraudulent activity **regular reconciliation of systems** is required.	1. Perform regular reconciliation of Call Data Records on switches, billing systems, etc. 2. Perform regular reconciliation of active subscriber profiles on networks and billing systems 3. Perform regular reconciliation of prepaid designated subscriptions on IN platforms
CN-007	**Control which devices can access the network** to protect against the connection of counterfeit, stolen and substandard devices and possible network impacts they may have.	1. Block duplicate or invalid IMEI numbers [46]. 2. Deploy Equipment Identity Register or equivalent technology capable of monitoring and blocking use of

Reference	Objective	Solution Description
		individual devices based on their IMEIs [14] 3. IMEI checks should carried out to confirm the device identify prior to providing mobile network access [47] 4. Validate device IMEIs using other techniques such as browser user agent profile checks.
CN-008 / CIS - 014	The **processes and tools used to track/control/prevent/correct secure access to critical assets** (e.g. core infrastructure) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.	1. Enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. 2. Disable any account that cannot be associated with a business process or business owner. 3. Ensure that all accounts have an expiration date that is monitored and enforced. Automatically disable dormant accounts after a set period of inactivity. 4. Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. 5. Enforce detailed audit logging for access to sensitive data or changes to sensitive data.

2.2.7 Network Operations Controls

These controls are likely to be understood and managed by the network operations team.

Reference	Objective	Solution Description
NO-001 / CIS-001	Actively **manage (inventory, track, and correct) all hardware devices on the network** so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.	1. Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. 2. Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network. 3. Use client certificates to authenticate hardware assets connecting to the organization’s trusted network. 4. Utilize port level access control, following 802.1x standards, to control

Reference	Objective	Solution Description
		which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network. 5. Do not allow shared, default or hardcoded passwords
NO-002 / CIS-005 & 011	Establish, implement, and actively **manage (track, report on, correct) the security configuration of network equipment (NE), servers, and workstations, and core infrastructure** using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.	1. Harden NE, and network infrastructure according to local hardening policies, if unavailable to the device manufacturer's hardening guides and/or industry accepted hardening guides [37], [48] maintain images of these builds. 2. Confirm interfaces are only accessible to the correct external applications and/or networks, internal network elements and BSS e.g. GTP's Gp/S8 interface accessible only for roaming partners [37] 3. Close interfaces that are not required (e.g. debugging interfaces) 4. Deploy mechanisms for detecting and reporting differences between master configuration and that of network infrastructure 5. Limit ability for change to occur using account management (e.g. by use of Privileged account management (PAM) system)
NO-003	**Virtualisation/Containerisation controls should be enforced** wherever network elements are virtualised e.g. Network Function Virtualisation (NFV).	1. Use Security Orchestration, Automation and Response (SOAR) technology within operation centres to control management of virtualisation 2. Harden virtualised machines or containers (NO-002) as per industry recommendations [49] 3. Isolate services, processes and tenants via name-spacing or hypervisor controls 4. NFV Infrastructure patching should deployed as a priority, the impact of a successful attacker gaining code execution rights is high.
NO-004 / CIS-009	Manage (track/control/correct) the ongoing **operational use of ports, protocols, and services** on networked	1. Associate active ports, services, and protocols to the hardware assets in the asset inventory.

Reference	Objective	Solution Description
	devices in order to **minimize windows of vulnerability** available to attackers	2. Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system. 3. Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system. 4. Apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. 5. Depreciate and remove usage of: a. Unencrypted, insecure transmission protocols [50] b. Unencrypted, insecure authentication protocols Examples include, but are not limited to: FTP, TFTP, telnet, POP3, IMAP, BGP and SNMP v1/v2. 5. NIST/3GPP recommended cryptographic algorithms shall be used whenever cryptographic services are required [51]
NO-005 / CIS-004	The processes and tools used to **track/control/prevent/correct the use, assignment, and configuration of administrative privileges** on servers, networks, and applications.	1. Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts. 2. Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges. 3. Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not Internet browsing, email, or similar activities. 4. Limit access to scripting tools to only administrative or development users with the need to access those capabilities. 5. Use multi-factor authentication and encrypted channels for all administrative account access.

Reference	Objective	Solution Description
		Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system. 6. Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges. 7. Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.
NO-006 / CIS-003	Continuously acquire, assess, and act on new information in order to **identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.**	1. Enable a centralised vulnerability and patch management programme to remediate vulnerabilities in a prioritised, timely manner 2. Regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner. 3. Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities. 4. Include software, open source and proprietary, in vulnerability assessment programmes. 5. Provenance of software updates should be assured. 6. Patches should be delivered over a secure channel.
NO-007	**Monitor and analyse core, radio and enterprise network traffic** for potential internal or external attacks.	1. Enable audit logging and deliver data to SIEM/log server for analysis for relevant threat vectors 2. Correlate log data to allow cross referencing 3. Enable system logging to include details such as an event source, date, user, timestamp (UTC), source addresses, destination addresses, and other useful elements. 4. On a regular basis, tune SIEM system to better identify actionable events and decrease event noise. 5. Ensure integrity of audit data (e.g. copy to write-once media or apply digital signatures to log collections)

Reference	Objective	Solution Description
NO-008	**Ensure certificate issuing authorities are managed correctly** to avoid the risk of bogus certificates being provided with access to network services.	1. Ensure root certificate issuing machines do not have access to and from the internet 2. Follow IETF RFC pertaining to PKI CA handling [52], [53], [54]
NO-009	**Ensure cryptographic key material is protected correctly** using a Cryptographic key management system (CKMS).	1. Actively manage the storage location, crypto-period and usage of all cryptographic material on the network [55] 2. Ensure HSM key management follows industry best practice, as outlined in FS.28 [19]. 3. Whenever possible key material should be managed via a HSM
NO-010	Ensure **database services and systems are protected** from unauthorised access and misuse.	1. Monitor database systems for unauthorised access, changes and data leakage 2. Monitor for unauthorized changes from privileged users such as administrators 3. Use transparent data encryption (TDE) to ensure data is encrypted all the way to the client, securing data both when it is at rest and in transit.
NO-011	Implement **cloud security principles** for all private, public and hybrid cloud (infrastructure, platform or software) computing based provisioning, whether operated in-house or outsourced, to provide all tenants with an effective risk management of services.	1. Data assessment before multi-tenant etc. 2. Deployment management 3. In life management 4. Procurement management 5. Isolation controls 6. Secure communications with infrastructure/service 7. Supplier security 8. Utilize a Cloud Access Security Broker (CASB) for user management 9. Cover in-life threat modelling as part of the ongoing risk management process

2.2.8 Security Operations Controls

These controls are likely to be understood and managed by the Security Operations Centre (SOC), Computer Security and Incident Response Team (CSIRT) or ethical hacking teams.

Reference	Objective	Solution Description
SO-001 / CIS-006	**Collect, manage, and analyse audit logs** of events that could help detect,	Collect, manage, correlate and analyse the audit logs of events that could help detect, understand or recover from an attack [3]

Reference	Objective	Solution Description
	understand, or recover from an attack.	Collect, manage, correlate and analyse network traffic flows that could help detect, understand or recover from an attack
SO-002 / CIS-008	**Control the installation, spread, and execution of malicious code** at multiple points in the network, while optimizing the use of automation to enable rapid updating of defence, data gathering, and corrective action.	Collect and manage events triggered by enterprise, mobile network and end point device anti-virus protection [3]
SO-003	**Utilise open source information** (OSINT) and other contextual information to increase awareness of the threat landscape.	1. Carry out Threat Intelligence integration 2. Contribute to relevant sharing communities e.g. GSMA T-ISAC [56]
SO-004 / CIS-019	Protect the organization's information, as well as its reputation, by **developing and implementing an incident response infrastructure** (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and Systems.	1. Create and advertise an incident reporting function (external and internal), allowing suspected incidents to be reported to the appropriate team 2. Plan, prepare and practice incident response activities (including data recovery and forensic capabilities) [57] 3. Assign roles to specific teams and individuals to drive ownership and accountability during an incident 4. Capability to learn and improve based on historic incidents through post incident reviews (PIR) 5. Create processes for any breach notifications required, noting any deadlines included
SO-005 / CIS-020	**Perform security assessment of live systems** to test the overall strength of an organization's defence (the technology, the processes, and the people) by **simulating the objectives and actions of an attacker**.	1. Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. 2. Remediate issues located through security assessments 3. Undertake regular security assessments, e.g. pen testing, of live systems
SO-006	Implement a holistic **protective monitoring** approach that ensures there is a proactive and consistent approach to detection of abnormal behaviour on networks and systems	1. Design an approach to protective monitoring that draws together the available sources of security events and alert when these sources fail to deliver data 2. Appropriately tune available log sources, SIEM and behavioural analysis systems to detect abnormal behaviour

Reference	Objective	Solution Description
		3. Centralise reporting to consoles that are adequately manned 4. Be able to provide forensically sound transaction audit trails 5. Be able to trace actions (especially privileged actions) to individuals and devices 6. Integrate into the system monitoring, audit and fraud management processes 7. Produce regular management and performance reports 8. Undertake regular reviews to adjust and improve practice

Annex A A Security Controls Checklist

A.1 Checklist Spreadsheet

FS.31 Baseline
Security Controls - An

Annex B Policy Outlines

B.1 Policy Document Outline Table

Policy	Outline Description
3rd party data/supply chain security management	3rd party data and supply chain security management will control the information exchanges and remote access for 3rd party to information systems, as well as the correct operation of policy and controls to ensure that vulnerabilities are not introduced within the supply chain.
Access control	Access control policy will cover the process for internal and external access to information systems and data. This includes enrolment and movers/leavers policies, data access controls, network access controls and privilege management.
Asset management	Asset management policies; including architectural design, in life management, and decommissioning of assets, especially those that contain information and data. This ensures that the systems that process those assets can effectively protect those assets and that the data loss is prevented (e.g. following disposal).
Business continuity management	Business continuity management policies and plans are developed based on specialist impact assessments that ensure that critical business processes can be maintained regardless of eventualities (disasters, losses of key personnel and other business disruptions, e.g. industrial action).
Cloud security	Cloud security policies ensure that appropriate security controls are applied to public, private or hybrid cloud computing deployments, with particular regard for protection of assets when they are processed within a multi-tenanted environment within which the tenants are largely dependent upon the security environment delivered by the cloud services provider.
Cryptographic material management	Cryptographic material management policy ensures that there is effective and sustainable management of encryption technology within solutions. This includes proactive key management to ensure that information and data can be encrypted/decrypted as and when required (and only by the legitimate communicating parties) and also that cryptographic techniques that support integrity and trust frameworks (PKIs) operate effectively and can be relied upon.
Device, system and network asset security	Device, system and network asset security policies ensure that appropriate configurations are applied to computing and networking devices to a) help enforce access control policies and b) minimise the exposure of vulnerabilities (e.g. disablement of unused functions/application of build lockdowns).

Policy	Outline Description
Information classification and handling	The information classification and handling policy will define the approach to security classification of information in both paper and electronic forms. It is typical for a hierarchy of security classifications to be identified and for appropriate handling requirements to be defined for each classification.
Personnel security	Personnel security policies cover pre- and during employment checks and also include conditions within both contracts of employment and arrangements with agencies and other contractors. It also covers sanctions for security breaches within disciplinary or contractual processes and procedures as well as management of security clearances for working with 3rd parties (e.g. government agencies).
Physical security	It can be expected there will be applied several physical security policies and standards across the estates of Operator organisations, with appropriate and proportionate standards applied to different sites (data centres, telecommunications centres, offices, cell-sites, etc.).
Risk management	A risk management policy should embody the approach to management of risks to information risks (the confidentiality, integrity and availability of that information). This includes consideration of threats and vulnerabilities present within both physical and electronic environments. This should be integrated with the business approach to risk in order that the SLT has visibility of critical information security risks.
Security incident management	Security incident management policy and processes handles the complete lifecycle of security related incidents (including breaches), should work as a feedback loop to reduce the risk of reoccurrence and should cover all aspects: reporting (actual or suspicious behaviour, weaknesses, etc.), triage, investigation, computer forensics, breach notification (in accordance with local regulations), communication with stakeholders, collaboration with law enforcement, recovery, management reporting/escalation, critical incident management teams and post-incident reviews.
Security monitoring	Security monitoring policy and processes are used to establish the necessary skills, disciplines and framework for monitoring systems for abnormal behaviour indicative of potential cyber-attacks or security breaches. This also includes audit policies for those systems that are not monitored by electronic systems and also log management and analysis.
Software security update management	Software security update management policy defines the required parameters for application of security updates and other patches to software and firmware in

Policy	Outline Description
	equipment. It also considers the solution product lifecycles to ensure that systems are supported with security updates and that end-of-support components are replaced prior to obsolescence.
Staff training and awareness	Staff training and awareness policy covers both specialist training of security and front-line staff and also broader awareness of security matters to all staff and contractors (including induction sessions, regular refresher/update briefings/communications, posters, etc.). It also covers urgent dissemination of security notices following security breaches.
Vulnerability disclosure management	Vulnerability disclosure management policy covers the responsible reporting of vulnerabilities discovered in systems, services and solutions. This prevents details of those vulnerabilities falling into the hands of attackers who would be interested in exploiting them and times releasing of public information in order that it is in conjunction with the availability of remedies.

Annex C Document Management

C.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	23 February 2019	Baseline security control for Mobile Network Operators.	TG	Amy Lemberger, GSMA
2.0	05 Feb 2020	Major review of controls in all sections	FASG	Amy Lemberger, GSMA

C.2 Other Information

Type	Description
Document Owner	Amy Lemberger
Editor / Company	GSMA

It is our intention to provide a quality product for your use. This document is an early version that can be updated with subject experiences and suggested improvements or additions, or if you find any errors or omissions. You may send these via email to us at security@gsma.com