Group Information and Cyber Security Policy

Version No	6.1
Document Type	Policy
Parent Document	Enterprise Risk Management Framework
Parent Framework	Information and Cyber Security
Document Approver Name	Mark Jeffery Strange
Document Approver Job Title	Global Head, OTCR, TTO
Document Owner Name	Paul Robert Hoare
Document Owner Job Title	Head, OTCR, Policy & Regulatory Management
Document Contact Name	Bali Chandramouli
Document Contact Job Title	VP, OTCR, Policy & Regulatory Management
Business Scope	All Businesses
Function Role	All Functions
Geography Scope	GLOBAL
Approval Date	29/11/2024
Effective Date	02/12/2024
Next Review Date	30/06/2025

Table of Contents

Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Bali Chandramouli	Migration to Inline format- Non Material Change(No change to document content)	Non-Material	Mark Jeffery Strange	6.1	29/11/2024	02/12/2024

The full version history is included in *Appendix.*

1. PURPOSE AND SCOPE

This Policy sets out the Group's direction on, and commitment to, Information and Cyber Security ["ICS"]. The Group Information and Cyber Security Policy ["GICSP"] sets out the principles and objectives for a robust and effective ICS approach to protect, preserve and manage the Confidentiality, Integrity and Availability ["CIA"] of the Group's Information, Information Assets and Technology Assets[1]. Adherence to this Policy, its Standards and the interconnected Policies, Standards will enable the Group to maintain Client confidence, protect the Group's commercial interests and reputation and to comply with applicable Legal, Regulatory and Mandatory ["LRM"] requirements emanating from the Group Core Regulators[2] as identified, relevant, applicable and defined in the Group ICS Managing Regulatory Change ("MRC") Process.

The objectives of the Policy are to:

- Ensure that the Group can operate competitively across complex and highly regulated environments whilst adequately protecting its Information and Technology Assets.
- Set out principles for all those directly and/or indirectly involved in the ICS Risk Management of Group Information and/or Technology Assets.

The GICSP comprises a detailed set of mandatory requirements that are aligned to international standards and LRM requirements. This alignment not only provides assurance that the rule set is comprehensive and fit-for-purpose; it also helps facilitate the Group Third Parties/Vendors when needing to demonstrate compliance with the Group's ICS requirements.

The requirements in this Policy are supported by the Group ICS Standards and ICS Methodologies:

- Information and Cyber Security [ICS] Standards
  These standards define the minimum control requirements for specific control disciplines or domains and support higher level statements in this policy.
- Information and Cyber Security [ICS] Methodologies

  The Information Asset [IA] impact assessment and Security Business Impact Assessment [S-BIA] methodologies have been adapted for to assess the impact to the Group if the CIA of an Information Asset or Information System is compromised respectively. The underlying Technology Infrastructure can be impact assessed independently only when it cannot inherit the impact rating from the Information System hosted.

The GICSP statements are applicable to all Group Information regardless of medium [e.g., paper, electronic/digital], Information processing systems and Geographies. Please refer to Section 3 for an overview of Roles and Responsibilities.

This policy is mapped to the ICS Risk Type Framework ["RTF"] v1.0 (Chapter 11 of Group ERMF v6.2) and applies for the management of ICS Risk. Any variations to this ICS Policy must be discussed with the Policy Owner or Policy Contact.

2. MANDATORY POLICY STATEMENTS

For further guidance to the Policy statements in this section [i.e., related security standards and mapping to industry standards e.g., ISO 27001, NIST and PCI-DSS], please refer to the Appendix: Section 9.2.

[1] Information Systems, Applications and Technology Infrastructure.

[2] Group Core Regulators are in line with Standard for Managing Regulatory Change by Conduct, Financial Crime and Compliance (CFCC)

2.1. Requirements Applicable to All Staff

a. All Staff must have the relevant ICS risk awareness by adopting the secure working practices and Rules of Behaviour defined in the ICS Acceptable Use Standard.

b. Each member of Staff, regardless of their work location, is responsible for maintaining the security [Confidentiality, Integrity and Availability] of the Group Information and or Information Assets they are authorised to use, handle and for the safety, usage of the Group approved IT Equipment and/or Technology Assets entrusted to their care.

c. All Staff must report all Information and Cyber Security incidents and any suspicious emails that they identify as soon as possible to Cyber Defence Centre [CDC].

d. All Staff must retain Group Information in accordance with the Group retention requirements and or to destroy securely in accordance with ICS Acceptable Use Standard.

2.1.1 Requirements Applicable to People Leaders

a. People Leaders must ensure their awareness, compliance to the Rules of Behaviour, and secure working practices in conjunction with the ICS Acceptable Use Standard. People leaders must also ensure their Staff's compliance with same.

2.2. Asset Management

2.2.1 Inventories of Assets

a. All Process Owners must identify their Information Assets and Information Systems, appoint Owners to them and ensure an inventory of their Information Assets, Information Systems are maintained and is up to date.

b. Information Asset Owners must maintain an updated inventory of all Information Assets that they own.

c. Information System Owners, Application Owners, Technology Infrastructure Owners must maintain an updated inventory of all Technology Assets that they own.

2.2.2 Acceptable Use of Information Systems

a. Information System Owners must ensure that the Group ICS Standards applicable to their Information Systems are enforced and adhered to.

b. Application Owners, Technology Infrastructure Owners must maintain owned Technology Assets in consideration with the manufacturer's default security specifications where security specifications are higher than the Group's ICS Standards requirements.

2.2.3 Information Classification and Criticality

a. Information Asset Owners must rate their Information Assets through employment of the Group Information Asset ["IA"] Methodology.

b. Information System Owners and Technology Infrastructure Owners must rate their Information Systems and Technology Infrastructure through employment of the Group Security-Business Impact Assessment ["S-BIA"] Methodology.

c. Information System Owners, Application Owners and Technology Infrastructure Owners must choose and apply security risk mitigation controls from the ICS Policy and Standards in accordance with the S-BIA rating of Technology Assets they own.

d. Information Asset Owners must review rating of their Information Assets and Information System, Technology Infrastructure Owners must review rating of their Information Systems, Technology Infrastructure to the frequency mandated by the respective ICS Methodologies [IA or S-BIA].

2.3. Information Handling

2.3.1 Protecting Information

a. Information System Owners, Application Owners, Technology Infrastructure Owners must maintain the Confidentiality, Integrity and Availability of Group Information and or Information Assets processed or stored within the Technology Assets they own commensurate with its S-BIA or IA rating.

2.3.2 Removable Media Handling

a. Technology Infrastructure Owners must prevent unauthorised access to and control the use of Removable Media to prevent Group Information from loss or disclosure through such media.

b. Information Asset Owner must authorise the use of Removable Media for their Information Asset(s).

2.3.3 Physical Media Transfer

a. Technology Infrastructure Owners must protect Removable Media and IT Equipment containing Group Information or Information Asset during physical transfer.

2.4. System Acquisition, Development and Maintenance

2.4.1 Secure Development

a. Technology Infrastructure Owners must separate the Production and non-Production environments for Information Systems and Technology Infrastructure.

b. Application Owners and Technology Infrastructure Owners must develop/deploy code and test the data in such a way that the risk of introducing security vulnerabilities is mitigated.

c. Information System Owners, Application Owners and Technology Infrastructure Owners must adhere to security requirements in accordance with ICS Policy and Standards when designing Technology Asset.

2.4.2 Change Control

a. Application Owners, Technology Infrastructure Owners must adhere to the Group's IT change management processes when owned Technology Asset has a change implemented impacting its security state.

b. Application Owners, Technology Infrastructure Owners must ensure any modification to software packages must not reduce the security of software in Production.

2.4.3 Outsourced Development

a. Application Owners, Technology Infrastructure Owners must ensure that the security of outsourced developments are commensurate with the ICS Policy and Standards required for internally developed Systems.

2.4.4 Testing

a. Application Owners, Technology Infrastructure Owners must enforce ICS Policy and Standards for the Technology Assets owned and ensure adherence. This would include emerging technologies and innovations.

b. Information Asset Owners must authorise use of owned Information Assets in testing and Information System Owners, Application Owners, Technology Infrastructure Owners must protect Production Information, when used in test environment corresponding to its S-BIA rating.

c. Application Owners, Technology Infrastructure Owners must perform security testing for their Technology Assets. This would include emerging technologies and innovations.

2.5. Access Control

2.5.1 Access Control and User Access Management

a. Information Asset Owner must permit access to owned Information Assets and Information System Owners, Application Owners, Technology Infrastructure Owners must design and manage access to owned Technology Assets in accordance with ICS Identity and Access Management Standard.

2.5.2 Secure Log On

a. Application Owners, Technology Infrastructure Owners must protect Group Information used to authenticate to Technology Assets. For example: Password, PIN, One Time Password ["OTP"].

2.5.3 Use of System Utilities

a. Application Owners, Technology Infrastructure Owners must restrict privileged access and the use of tools, services that are potentially capable of overriding system controls only to individuals where access is essential to perform their role.

b. Application Owners, Technology Infrastructure Owners must remove or disable unnecessary software, protocols, services and ports from Technology Assets they own.

2.6. Operations Security

2.6.1 Security Architecture and ICS Controls Adoption

a. Chief Security Architect must support the governance of the ICS risk through definition and maintenance of security architecture principles, capabilities, and strategy for embedding ICS requirements into the Group's enterprise architecture layers.

b. Chief Security Architect reviews and approves cyber security architecture design, roadmaps and ensure the cyber security solution design is aligned to the approved.

c. Process Owners, providing and delivering ICS services and capabilities must ensure effective, compliant adoption and delivery of applicable ICS controls that delivers the objectives of the Policy, ICS controls and security architecture principles and strategy.

2.6.2 Operational Procedures and Responsibilities

a. Technology Infrastructure Owners must ensure technical security baselines are documented and available for owned Technology Assets.

2.6.3 Protection from Malware

a. Information System Owners, Application Owners, Technology Infrastructure Owners must protect Technology Assets they own from Malware in accordance with ICS Anti-Malware Standard.

2.6.4 Backup

a. Technology Infrastructure Owners must secure back-ups of Technology Assets that they support in accordance with ICS Data Storage and Backup Standard.

b. Information System Owners, Technology Infrastructure Owners must ensure that backed-up Information is recoverable and useable.

c. Technology Infrastructure Owners must retain the back-ups in a location separate from the business operations location.

2.6.5 Logging and Monitoring

a. Information System Owners, Application Owners, Technology Infrastructure Owners must configure the Technology Assets that they own with the ability to record audit Information to logs, retain or secure

them for any analyses, monitor for security events and incidents in accordance with ICS Security Logging and Monitoring Standard.

2.6.6 Threat Identification

a. Application Owners, Technology Infrastructure Owners must monitor their Technology Assets and internal, external Threat Intelligence [TI] sources/advisories [e.g., regulators] for any security threats which may have potential impact to Technology Assets they own and/or support.

2.6.7 Control of Operational Software

a. Application Owners, Technology Infrastructure Owners must only use software or tools where support is in place to ensure security patches are available for deployment.

2.6.8 Technical Vulnerability Management

a. Application Owners, Technology Infrastructure Owners must assess available security patches and apply them according to the S-BIA rating of owned Technology Assets and patch severity.

b. Application Owners, Technology Infrastructure Owners must ensure that security testing and vulnerability scanning are carried out on a regular basis and commensurate with the S-BIA rating of owned Technology Assets.

c. Application Owners, Technology Infrastructure Owners must ensure all identified vulnerabilities are remediated to the timescale defined within ICS Vulnerability and Security Patch Management Standard.

2.6.9 Mobile Devices and Remote Working

a. Technology Infrastructure Owners must ensure the secure management of Group Information accessed or held on Mobile Devices.

2.6.10 Cryptography/Encryption

a. Information System Owners, Application Owners, Technology Infrastructure Owners must protect Group Information with cryptographic/encryption controls commensurate with the highest of IA rating or the highest of Classification level applied to the Group Information processed by the owned Technology Assets.

b. Application Owners, Technology Infrastructure Owners must protect cryptographic/encryption keys throughout their lifecycle.

c. Application Owners, Technology Infrastructure Owners must ensure that the Digital Certificates used in their Technology Assets are managed throughout its lifecycle in accordance with ICS Digital Certificate Management Standard.

2.7. Network Security

2.7.1 Network Security Management

a. Technology Infrastructure Owners must ensure that all access to and from the Group networks is controlled and monitored.

b. Technology Infrastructure Owners must ensure that network security architecture and associated documentation is maintained.

2.7.2 Segregation of Networks

a. Technology Infrastructure Owners must segregate the network to protect the Group Information Assets and Technology Assets commensurate with their IA or S-BIA rating.

2.7.3 Information Transfer

a. Technology Infrastructure Owners must protect the Confidentiality and Integrity of Group Information commensurate to its rating whenever transmitted across networks both internally and externally.

2.8. Supplier Relationships

a. Outsourcing Owner/Contract Manager must ensure that the Third Party/Vendor arrangements include relevant security requirements and that an applicable Third Party Security Assessment ["TPSA"] is completed.

b. Information System Owners, Technology Infrastructure Owners must document and enforce specific procedures for granting Third Party/Vendor access to their Technology Assets.

c. Information Asset Owners must, at the minimum, ensure that Restricted or Confidential Information and or Information Assets rated 4 or 5 owned is protected when it is handled or processed by Third Parties/Vendors.

2.9. Information Destruction

a. Information System Owners, Technology Infrastructure Owners must securely decommission their owned Technology Assets and dispose of all storage media by ensuring the Group Information Assets within are securely destroyed.

b. Information Asset Owners must authorise and ensure secure destruction of owned Information Assets in accordance with ICS Secure Decommissioning and Destruction Standard.

2.10. Incident Management

Information Asset Owners for owned Information Assets, Information System Owners, Technology Infrastructure Owners for owned Technology Assets must manage identified security events and incidents, restore the affected and prevent recurring incidents.

3. RESPONSIBLE ROLES FOR IMPLEMENTING THE MANDATORY POLICY STATEMENTS

The Policy Owner responsibility is defined in the Enterprise Risk Management Framework ["ERMF"].

Role	Requirement	Responsible Group
All Staff	Staff are required to read and comply with the requirements of the GICSP which are directly relevant to them.	All Staff
People Leaders	People Leaders are responsible for overseeing their Staff adherence to the GICSP requirements and to comply with the requirements which are directly relevant to them.	All People Leaders
Information Asset Owners ['IAO"], Information System Owners ["ISO"]	o IAO is accountable for the inventory of owned Information Assets and impact assessments. o ISO is accountable for the inventory of owned Information Systems and impact assessments.	The Information Asset Owner, Information System Owner is generally the business or global functions role who has accountability for the protection, existence and

	o To ensure that change activities have controls which achieve compliance with ICS Policy. o To ensure owned Information Assets, Information Systems are accurate and up to date in relevant registers. o To implement ICS controls across Information Assets and Information Systems under their ownership. o To assist in raising risk treatment plans and mitigating identified ICS Risks and ensure controls in compliance with Policy and Standards.	permissible use of a set of information or an Information System and who would be impacted should the Confidentiality, Integrity and Availability of owned Information Asset or Information System be compromised. They may delegate responsibility for day to day activities to a nominated role within their team. In this instance where this happens, the recipient becomes the Information Asset/Information System Delegate. However, the Owner retains overall Accountability. [i.e., Business/Global Function Manager, Heads of Business Unit]
Application Owners, Technology Infrastructure Owners	o Technology Infrastructure Owners are responsible for performing S-BIA assessment against Technology Infrastructure where it is not suitable to be inherited from the Information System assessment. o To ensure owned Applications and Technology Infrastructure are accurate and up to date in the CMDB. o To implement ICS controls across Technology assets under their ownership. o To assist in raising risk treatment plans and mitigating identified ICS Risks and ensure controls in compliance with Policy and Standards. o To ensure that change activities have controls which achieve compliance with ICS Policy.	The role who has responsibility for the processing of Information Assets and the provision of Information Systems and Technology Infrastructure. The role applies controls commensurate with the impact rating and/or as instructed by the Information Asset/Information System Owner. [i.e., The Group Chief Information Officer [CIO, TTO], Technology Domain Owners].
Contract / Service Owners	o Appointed individual by the First Line Business / Function who is responsible to manage the performance and risk arising from the use of a Third Party arrangement throughout its lifecycle. At times this role is also referred to as the Contract	Contract/Service Owners w.r.t Group Third Party Risk Management Policy framework

	Manager and / or Outsourcing Owner. o To ensure all ICS requirements are met during the establishment, duration and termination of the business relationship with the Group's service provider [Third Party/Vendors].	
Process Owners	o Implementing ICS controls relevant to the Processes under their ownership. o Ensuring ownership is assigned for all Information Assets, Information Systems and Technology Infrastructure under their process ownership. o To define and maintain the adoption of applicable ICS controls in line with the predefined objectives and security architecture principles.	Global Process Owners [GPO]/Process Owners [PO] defined within Process Universe [PU].
Security Architecture	o To support governance of ICS risk.	Chief Security Architect
CISO Business/Functions/Markets	o To support the Information Asset, Information System Owners for their area by cascading changes to the ICS Policy and Standards to them and other required business stakeholders and ensure the changes are understood. o To support Information Asset, Information System Owners in identifying their assets under their authority. o To support Business Application Owners in identifying Information Systems and endorses impact rating adjustments for Information Systems under their authority. o To support their areas in adhering to Third-Party onboarding controls within ICS Policy and Standards.	CISOs of Business, Functions and Regions/Countries.

4. POLICY RELATED AUTHORITIES

4.1 Delegation of Authorities

The ICS RTF is the formal mechanism through which the delegation of ICS Risk Authorities is made. Through this Policy, the ICS RFO appoints Head, OTCR Policy & Regulatory Management as the Policy Owner for Policy management.

The Policy Owner delegates the ownership, approval authority and life cycle management of underlying Standards (ref. Section 8) to the Group CISO function. The delegation entails the underlying Standards will be managed as per ERMF defined Standard Owner responsibilities. The Standard Owner/approver must inform the Policy owner of any material changes to the ICS Standards and highlight the impact to the policy and traceability. In case of inconsistencies between Policy and underlying Standards, Policy statements will prevail.

4.2 Policy Periodic Refresh and Change Requests

This Policy is refreshed annually. This Policy is valid until the release of a refreshed version via GovPoint. Any changes to this Policy require a request to be submitted to the Policy Owner/Contact.

4.3 Non-Compliance to ICS Policy

Compliance with the GICSP is required for all parts of the Group. Where compliance is not possible, as a general guideline, any non-compliance against the Applications and underlying Technology Infrastructure in CMDB should follow the ICS Non-Compliance Register (ICS NCR) process. Further assessment of these non-compliance should follow the issue management process i.e., iTrack for issues with remediation plan or ICS Dispensation when there is an explicit decision not to remediate the issue.

4.5 Policy Breaches

a. Failure to comply with this Policy may result in formal disciplinary action under the Group Disciplinary Standard.

b. Any actual or suspected breaches must be reported immediately to your People Leader, to your Compliance representative or via other breach reporting channels.

c. Any breaches to the Policy must be reported to the Policy Owner.

5. CONNECTED PROCESSES AND ACTIVITIES

All Mandatory Statements within this Policy are relevant to all the processes and Technology Assets that process Group Information.

6. POLICY EFFECTIVENESS REVIEW

The Policy Owner will rely on and seek responses, data inputs from the ICS Risk Authorities, as defined within the ICS RTF and other sources included below for measuring compliance/effectiveness against this policy:

- Control effectiveness (control sample tests, key control indicators) will be gathered through the RCSA or otherwise [non-RCSA], for the key controls that implement the requirements set out in this Policy.
- Output of second line oversight and challenge activities (including assurance testing as applicable).
- Findings from third line and regulatory reviews including level of compliance with regulatory obligations, any breaches.
- Volume of approved Elevated Residual Risks [ERR] and ICS Dispensations where compliance is exempted from measurement.
- Oversight activities by Policy Owner.

7. INTERCONNECTED POLICIES & STANDARDS

Policy Name	Risk Type/Risk	Policy Owner	Area of connection
Group Health, Safety and Security Policy	Operational & Technology Risk – Physical Safety and Security	Global Head Safety & Security	The physical security of people, property and premises.
Group Contracts Policy	Operational & Technology Risk – Legal Enforceability	Director, Risk & Policy Legal, Client Segments	Applicable to all Contracts entered into by the Group. This Policy Sets the mandate for Contract executing Staff to ensure the Contract is approved by Legal or in a Standard form approved by Legal. This is very relevant in a Third Party engagement Contracts.
Group Technology Policy	Operational & Technology risk – Technology Risk	CRO Functions, Technology & Innovation	ICS places a reliance on the connected technology policy to cover: - Ensuring an inventory of technology assets and associated configuration items. - Establishment of build and run IT processes covering the end-to-end technology lifecycle, where specific ICS controls from the ICS policy and standards can be inserted. - Principles covering technology incidents, change management (for security related change deployments) and problem management, of which a subset may be an ICS nature. - Principles covering IT continuity, that may be leveraged in the event of outages caused ICS threats.
Group Staff Screening Policy	Operational & Technology Risk – People Risk	Head, T&R, Quality Assurance	Staff screening, background verification.

Client Service Resilience Policy	Operational & Technology Risk – Client Service Disruption	Group Resilience Risk & Governance	ICS threats can cause business disruption and crisis and must be managed in conjunction with the requirements of the CSR Policy which ensure the Bank's services, particularly the Important Business Services ("IBS"), remain operationally resilient.
Group Data Conduct Policy	Compliance – Data Risk	Global Head, Data Conduct, CFCC	The Group Data Conduct Policy and all its underlying Standards (Privacy, Record Keeping, Data Sovereignty, Responsible AI) must be adhered to in respect of embedding and operationalising of data conduct requirements.
Group Third Party Risk Management Policy	Operational & Technology Risk – Third Party Risk Management	Executive Director, Third Party Risk Management	TPRM Policy provides the end to end framework for in-scope Third Parties/Vendors – to enable Businesses and Functions to identify applicable risks, engage with the necessary Risk Groups and complete key control activities of respective Risk Groups at each stage of the Third Party lifecycle. Also refer for Definition of Third Party/Vendor & Contract/Service Owner.
Digital Asset Risk Management Policy	ERMF	Global Head Digital Assets Risk Management	Digital Assets initiatives to refer to DA policy for DA specific risk management, identification and assessment. BAU risk assessments continue to apply for ICS.

Standard Name	Risk Type / Risk	Standard Owner	Area of connection
Group Disciplinary Standard	Operational & Technology Risk – People Risk	Global Head, Employee Relations	**Disciplinary Standard** sets out the Bank's approach to handling disciplinary matters, where an employee's behaviour and/or conduct does not meet the expected standards (which may include Policy or Standard breaches).
People Leader Standard	Operational & Technology Risk – People Risk	Global Head, Organisation and People Capability	**People Leader Standard** sets minimum standards for People Leaders for on-boarding and off-boarding of Staff and their managing conduct and risk issues. They and their team members assist keeping the Group's Systems and Information secure.
Group Electronic and Voice Communications Standard	Compliance Risk – Regulatory Conduct	Executive Director, Framework and Policy	Defines Business Communications and sets out the minimum requirements for all Business Communications across the Group's Businesses and Functions. Any use of unauthorised Group Communication and Collaboration Tools ("CCT") for Business Communications is strictly prohibited, with the exception of regulator communications by authorised individuals, where use of a particular non-approved CCT is local practice by the Regulator, and Staff must comply with the Group Communications with Regulators Standard.

8. STANDARDS MAPPED TO THIS POLICY

Standard Name	Risk Type	Standard Owner	Standard Approver
1. Anti-Malware 2. Applications Security 3. Acceptable Use Standard 4. Cryptography 5. Digital Certificate Management 6. Data Leakage Prevention 7. Data Storage and Backup 8. Identity and Access Management 9. Information Classification 10. Information Handling 11. Information Security Awareness and Training 12. Mobile Device Security 13. Network Security Management 14. Payment Card Data Management 15. Secure Configuration Management 16. Secure Decommissioning and Destruction 17. Security Incident Response and Management 18. Security Logging and Monitoring 19. Standalone Machine Management 20. Secure Handling of Production Data 21. Security in Interactions with Third Parties 22. Secure Asset Management 23. Unstructured Data Storage 24. Vulnerability and	Information & Cyber Security	Director, ICS Standards Formulation	Head, ICS Risk Framework & Governance

Security Patch Management 25. Web Filtering			

9. APPENDIX

9.1 Regulatory Requirements

The applicable ICS Legal, Regulatory and Mandatory [LRM] Obligations are available in ICS Obligation Register.

9.2 ICS Policy Mappings to RTF & External/Industry Sources

The Group internal Policy mapping to External/Industry sources illustrate the control objective/area level alignments.

#	Policy Statements	ICS RTF Control Domains	Related Minimum ICS Standards	Industry Standards Reference				ICS Risk Objective(s)	ICS RTF Risk Category(s)/ L3 Risks	ICS Threat Vector(s)
				ISO 27001: 2013	NIST CSF v1.1	PCI-DSS 3.2	Swift CSCF 2020 [Control Objective]			
2.1 Requirements Applicable to All Staff										
2.1a	All Staff must have the relevant ICS risk awareness by adopting the secure working practices and Rules of Behaviour defined in the Acceptable Use Standard	Security Awareness and Training	• Acceptable Use Standard • Information Classification • Information Handling • Unstructured Data Storage • Applications Security [Developers Training] • Information Security Awareness & Training • Identity and Access Management [Privileged/Administrator Users Training]	7.2.1 8.1.2 8.2.1 8.2.2 7.2.2 11.2.9 13.2.1	ID[GV-2] PR[IP-11] ID[AM-5] PR[AC-1] PR[DS-1] PR[DS-2] PR[DS-5] PR[AT-1]	12.3 12.6 9.5 9.9 11.1 .1 3.4 4.1 4.2 4.3	3.1 5.1 7.2	Preventative	• Disclosure of Sensitive Information by External Attacker and/or Trusted Insider • Disruption of Business Operations by External Attacker and/or Trusted Insider	• Malware • Phishing and Social Engineering • Privilege Misuse • Supply Chain Compromise

			• Payment Card Data Management [Security Breach handling Training]							
2.1b	Each member of Staff, regardless of their work location, is responsible for maintaining the security [Confidentiality, Integrity and Availability] of the Group Information and or Information Assets they are authorised to use, handle and for the safety, usage of the Group Approved IT Equipment and/or Technology Assets entrusted to their care.	Security Awareness and Training	• Acceptable Use Standard • Secure Decommissioning and Destruction • Unstructured Data Storage	6.1.1	ID[AM-6] PR[AT-2]	12.6	3.1 5.1 7.2	Preventative	• Disclosure of Sensitive Information by External Attacker and/or by Trusted Insider • Disruption of Business Operations by External Attacker and/or Trusted Insider	• Privilege Misuse • Vulnerability Exploitation
2.1c	All Staff must report all Information and Cyber Security incidents and any suspicious emails that they identify as soon as possible to Cyber Defence Centre [CDC].	Security Awareness and Training	• Acceptable Use Standard • Payment Card Data Management [Security Breach handling Training]	7.2.2	RS[CO-2]	9.9.3 12.3 12.4 12.6	7.1 7.2	Detective	• Disclosure of Sensitive Information by External Attacker and/or Trusted Insider	• Malware • Phishing and Social Engineering
2.1d	All Staff must retain Group	Security Awarene	• Acceptable Use Standard • Secure	8.2.3 8.3.1	PR[IP-6]	3.1 9.8	7.2	Prevent	• Disclosure of Sensitiv	• Malware

	Information in accordance with the Group retention requirements and or destroy securely in accordance with ICS Acceptable Use Standard.	ss and Training	Decommissioning and Destruction	8.3.2 11.2.7				ative	e Information by External Attacker and/or Trusted Insider	
2.1.1 Requirements Applicable to People Leaders										
2.1.1.a	People Leaders must ensure their awareness, compliance to the Rules of Behaviour, and secure working practices in conjunction with the ICS Acceptable Use Standard. People leaders must also ensure their Staff's compliance with same.	Security Awareness and Training	• Acceptable Use Standard • Identity and Access Management • Unstructured Data Storage	7.2.1 7.2.2 11.2.9 6.1.2 7.3.1 9.1.2 9.2.6	PR[AT-1] PR[AC-1] PR[DS-1] PR[DS-2] PR[AC-4] PR[DS-5]	12.6 9.5 7.2 8.1	7.2 3.1 5.1	Preventative	• Financial Loss by External Attacker and/or Trusted Insider • Disclosure of Sensitive Information by External Attacker and/or Trusted Insider • Disruption of Business Operations by External Attacker and/or Trusted Insider	• Malware • Phishing and Social Engineering • Privilege Misuse • Vulnerability Exploitation
2.2 Asset Management										
2.2.1 Inventories of Assets										

2.2.1a	All Process Owners must identify their Information Assets and Information Systems, appoint Owners to them and ensure an inventory of their Information Assets, Information Systems are maintained and is up to date.	Secure Asset Management	• Information Classification • Standalone Machine Management • Secure Asset Management • Unstructured Data Storage	8.1.1	ID[AM-1] ID[AM-2] ID[AM-3]	2.4 11.1 .1	-	Preventative	• Disruption of Business Operations by External Attacker and/or Trusted Insider	• Vulnerability Exploitation
2.2.1b	Information Asset Owners must maintain an updated inventory of all Information Assets that they own.	Secure Asset Management	• Information Classification • Secure Asset Management • Standalone Machine Management • Unstructured Data Storage	8.1.1	ID[AM-1] ID[AM-2]	2.4 11.1 .1	-	Preventative	• Disruption of Business Operations by External Attacker and/or Trusted Insider	• Vulnerability Exploitation
2.2.1 c	Information System Owners, Application Owners, Technology Infrastructure Owners must maintain an updated inventory of all Technology Assets that they own.	Secure Asset Management	• Information Classification • Secure Asset Management • Standalone Machine Management • Unstructured Data Storage	8.1.1	ID[AM-1] ID[AM-2]	2.4 11.1 .1	-	Preventative	• Disruption of Business Operations by External Attacker and/or Trusted Insider	• Vulnerability Exploitation
2.2.2 Acceptable Use of Information Systems										
2.2.2a	Information System Owners must ensure that the Group	Secure Asset Manage	• Applications Security • Cryptography • Information	8.1.3	ID[AM-6]	12.3 12.4	1.1 2.3 2.10	Preventative	• Disclosure of Sensitive	• Privilege Misuse

	ICS Standards applicable to their Information Systems are enforced and adhered to.	ment	Classification • Information Handling • Identity and Access Management • Network Security Management • Secure Configuration Management • Secure Decommissioning and Destruction • Security Logging and Monitoring • Unstructured Data Storage						Information by External Attacker and/or Trusted Insider • Disruption of Business Operations by External Attacker and/or Trusted Insider	
2.2.2b	Application Owners, Technology Infrastructure Owners must maintain owned Technology Assets in consideration with the manufacturer's default security specifications where security specifications are higher than the Group's ICS Standards requirements.	Secure Asset Management	• Applications Security • Network Security Management • Secure Configuration Management	11.2.4	PR[IP-1]	6.2 6.4.2 7.1 7.2 8.1 8.2 12.3	2.3 2.10	Preventative	• Disruption of Business Operations by External Attacker and/or Trusted Insider	• Lateral Movement • Vulnerability Exploitation
2.2.3 Information Classification and Criticality										
2.2.3a	Information Asset Owners must rate their Information Assets through employment of the Group Information	Secure Asset Management	• Information Classification • Unstructured Data Storage	8.1.2 8.2.1 8.2.2	ID[AM-5] ID[RA-4]	9.6.1 12.2	-	Preventative	• Disclosure of Sensitive Information by External Attacker and/or	• Privilege Misuse

	Asset ["IA"] methodology.								Trusted Insider	
2.2.3b	Information System Owners and Technology Infrastructure Owners must rate their Information Systems and Technology Infrastructure through employment of the Group Security-Business Impact Assessment ["S-BIA"] methodology.	Secure Asset Management	• Information Classification	8.1.2 8.2.1 8.2.2	ID[AM-5] ID[RA-4]	9.6.1 12.2	-	Preventative	• Disruption of Business Operations by External Attacker and/or Trusted Insider	• Vulnerability Exploitation
2.2.3c	Information System Owners, Application Owners and Technology Infrastructure Owners must choose and apply security risk mitigation controls from the ICS Policy and Standards in accordance with the S-BIA rating of Technology Assets they own.	Secure Asset Management	• Applications Security • Information Classification • Information Handling • Identity and Access Management • Network Security Management • Secure Configuration Management • Secure Decommissioning and Destruction • Unstructured Data Storage	7.2.1 7.2.2	ID[AM-6] PR[AT-5]	12.3 12.4 12.6	7.4A	Preventative	• Disruption of Business Operations by External Attacker and/or Trusted Insider	• Vulnerability Exploitation
2.2.3d	Information Asset Owners must review rating of their	Secure Asset Management	• Information Classification • Unstructured Data Storage	8.1.2 8.2.1 8.2.2	ID[AM-5]	9.9 12.2	7.4A	Preventative	• Disclosure of Sensitive Informati	• Privilege Misuse • Vulnerability

	Information Assets and Information System, Technology Infrastructure Owners must review rating of their Information Systems, Technology Infrastructure to the frequency mandated by the respective ICS Methodologies [IA or S-BIA].								on by External Attacker and/or Trusted Insider • Disruption of Business Operations by External Attacker and/or Trusted Insider	Exploitation
2.3 Information Handling 2.3.1 Protecting Information										
2.3.1a	Information System Owners, Application Owners, Technology Infrastructure Owners must maintain the Confidentiality, Integrity and Availability of Group Information and or Information Assets processed or stored within the Technology Assets they own commensurate with its S-BIA or IA rating.	Information Protection	• Applications Security • Cryptography • Data Backup and Storage • Data Leakage Prevention • Identity and Access Management • Information Classification • Information Handling • Security Logging and Monitoring • Unstructured Data Storage	8.3.2 9.1 10.1.1 12.3 14.1	PR[AC-5] PR[DS-1] PR[DS-2] PR[DS-3] PR[DS-4] PR[DS-6] PR[IP-6] PR[PT-2] DE[CM-7] DE[CM-	3.1 3.2 3.3 3.4 9.8 10.7	2.3 2.10 7.4A	Preventative	• Disclosure of Sensitive Information by External Attacker and/or Trusted Insider • Disruption of Business Operations by External Attacker and/or Trusted Insider	• Denial-of-Service • Malware • Privilege Misuse • Vulnerability Exploitation

					8]					
2.3.2 Removable Media Handling										
2.3.2a	Technology Infrastructure Owners must prevent unauthorised access to and control the use of Removable Media to prevent Group Information from loss or disclosure through such media.	Information Protection	• Data Leakage Prevention • Data Backup and Storage • Information Handling • Mobile Device Security • Secure Handling of Production Data • Secure Decommissioning and Destruction	8.3	PR[DS-5] PR[PT-2]	3.4.1	3.1 5.1	Preventative	• Disclosure of Sensitive Information by External Attacker and/or Trusted Insider • Disruption of Business Operations by External Attacker and/or Trusted Insider	• Malware • Supply Chain Compromise
2.3.2 b	Information Asset Owner must authorise the use of Removable Media for their Information Asset(s).	Information Protection	• Data Leakage Prevention • Data Backup and Storage • Information Handling • Mobile Device Security • Secure Handling of Production Data • Secure Decommissioning and Destruction	8.3	PR[DS-5] PR[PT-2]	3.4.1	3.1 5.1	Preventative	• Disclosure of Sensitive Information by External Attacker and/or Trusted Insider • Disruption of Business Operations by External Attacker and/or Trusted Insider	• Malware Supply Chain Compromise
2.3.3 Physical Media Transfer										

2.3.3a	Technology Infrastructure Owners must protect Removable Media and IT Equipment containing Group Information or Information Asset during physical transfer.	Information Protection	• Cryptography • Digital Certificate Management • Data Leakage Prevention • Data Backup and Storage • Information Classification • Information Handling • Mobile Device Security • Secure Handling of Production Data • Unstructured Data Storage	8.3	PR[PT-2] PR[DS-3]	9.5	3.1 5.1	Preventative	• Disclosure of Sensitive Information by External Attacker and/or Trusted Insider	• Privilege Misuse • Supply Chain Compromise
2.4 System Acquisition, Development and Maintenance										
2.4.1 Secure Development										
2.4.1a	Technology Infrastructure Owners must separate the Production and non-Production environments for Information Systems and Technology Infrastructure.	System Lifecycle Security (including Vulnerability Management)	• Applications Security • Network Security Management	12.1.4 14.2.6	PR[DS-7]	6.4	1.1	Preventative	• Disclosure of Sensitive Information by External Attacker and/or Trusted Insider • Disruption of Business Operations by External Attacker and/or Trusted Insider	• Lateral Movement • Vulnerability Exploitation
2.4.1b	Application Owners and Technology Infrastructure Owners must develop/deploy	System Lifecycle Security (including Vulnerab	• Applications Security • Anti-Malware • Vulnerability Identification and Management	14.2.1 14.2.5	PR[IP-2]	6.3 6.5	6.1	Preventative	• Disclosure of Sensitive Information by External	• Malware • Vulnerability Exploitation

	code and test the data in such a way that the risk of introducing security vulnerabilities is mitigated.	ility Manage ment)							Attacker and/or Trusted Insider	
2.4. 1c	Information System Owners, Application Owners and Technology Infrastructure Owners must adhere to security requirements in accordance with ICS Policy and Standards when designing Technology Asset.	System Lifecycle Security (includin g Vulnerab ility Manage ment)	• Applications Security • Secure Configuration Management	14.2.1	PR[I P-2]	6.3	2.2 2.3 2.10	Prevent ative	• Disclosu re of Sensitiv e Informati on by External Attacker and/or Trusted Insider • Disruptio n of Busines s Operatio ns by External Attacker and/or Trusted Insider	• Malware • Vulnera bility Exploita tion
2.4.2 Change Control										
2.4. 2a	Application Owners, Technology Infrastructure Owners must adhere to the Group's IT change management processes when owned Technology Asset has change implemented impacting its security state.	System Lifecycle Security (includin g Vulnerab ility Manage ment)	• Applications Security • Network Security Management • Secure Configuration Management	14.2.2.	PR[I P-3]	6.4. 5 6.4. 5.1 6.4. 5.2 6.4. 5.3 6.4. 5.4 6.4. 6	6.2 6.3	Prevent ative	• Disclosu re of Sensitiv e Informati on by External Attacker and/or Trusted Insider	• Vulnera bility Exploita tion • Web-based attacks
2.4.	Application	System	• Applications	14.2.3	PR[I	6.4.	6.2		• Disclosu	• Vulnera

2b	Owners, Technology Infrastructure Owners must ensure any modification to software packages must not reduce the security of software in Production.	Lifecycle Security (including Vulnerability Management)	Security • Network Security Management • Secure Configuration Management	14.2.4	P-3]	5 6.4.5.1 6.4.5.2 6.4.5.3 6.4.5.4 6.4.6	6.3	Preventative	re of Sensitive Information by External Attacker and/or Trusted Insider	bility Exploitation • Web-based attacks
2.4.3 Outsourced Development										
2.4.3a	Application Owners, Technology Infrastructure Owners must ensure that the security of outsourced developments are commensurate with the ICS Policy and Standards required for internally developed Systems.	Third Party Security Management	• Applications Security • Security in Interactions with Third Parties	14.2.7	PR[IP-2]	6.1 6.2 6.3 6.4 6.5 6.6 6.7	2.3 2.10	Preventative	• Disruption of Business Operations by External Attacker and/or Trusted Insider	• Supply Chain Compromise
2.4.4 Testing										
2.4.4a	Application Owners, Technology Infrastructure Owners must enforce ICS Policy and Standards for the Technology Assets owned and ensure adherence. This would include	System Lifecycle Security (including Vulnerability Management)	• Applications Security • Cryptography • Information Classification • Information Handling • Identity and Access Management • Network Security Management • Secure Configuration Management	14.2.8 14.2.9	PR[DS-6] PR[IP-2]	6.4.5 12.10.1 12.10.2	2.3 2.10	Preventative	• Financial Loss by External Attacker and/or Trusted Insider • Disclosure of Sensitive Information by External Attacker and/or	• Vulnerability Exploitation

	emerging technologies and innovations.		• Secure Decommissioning and Destruction • Security Logging and Monitoring • Unstructured Data Storage						Trusted Insider • Disruption of Business Operations by External Attacker and/or Trusted Insider	
2.4.4b	Information Asset Owners must authorise use of owned Information Assets in testing and Information System Owners, Application Owners, Technology Infrastructure Owners must protect Production Information, when used in test environment corresponding to its S-BIA rating.	System Lifecycle Security (including Vulnerability Management)	• Applications Security • Network Security Management • Secure Configuration Management • Secure Handling of Production Data	14.3.1	PR[AC-4] PR[DS-7]	6.4.1 6.4.2	-	Preventative	• Disclosure of Sensitive Information by External Attacker and/or Trusted Insider	• Malware • Web-based attacks
2.4.4c	Application Owners, Technology Infrastructure Owners must perform security testing for their Technology Assets. This would include	System Lifecycle Security (including Vulnerability Management)	• Applications Security • Secure Configuration Management • Vulnerability Identification and Management	14.2.3 14.2.9	PR[IP-3]	6.4	2.7 7.3A	Preventative	• Disruption of Business Operations by External Attacker and/or Trusted Insider	• Vulnerability Exploitation

	emerging technologies and innovations.									
2.5 Access Control										
2.5.1 Access Control and User Access Management										
2.5.1a	Information Asset Owner must permit access to owned Information Assets and Information System Owners, Application Owners, Technology Infrastructure Owners must design and manage access to owned Technology Assets in accordance with ICS Identity and Access Management Standard.	Identify and Access Management	• Identity and Access Management • Information Classification • Information Handling • Unstructured Data Storage	9.2.4 9.2.5 9.4.1 9.4.2	PR[AC-4]	8.1 8.2 8.3 8.4 8.5 8.6 8.7	5.1	Preventative	• Disclosure of Sensitive Information by External Attacker and/or Trusted Insider	• Privilege Misuse
2.5.2 Secure Log On										
2.5.2a	Application Owners, Technology Infrastructure Owners must protect Group Information used to authenticate to Technology Assets. For example:	Identify and Access Management	• Applications Security • Cryptography • Digital Certificate Management • Identity and Access Management • Information Classification • Information Handling • Unstructured	9.2.3 9.3.1	PR[AC-1] PR[AC-4] PR[DS-5]	8.1 8.2 8.3 8.4 8.5 8.6 8.7	4.1 4.2 5.1	Preventative	• Disclosure of Sensitive Information by External Attacker and/or Trusted Insider	• Phishing and Social Engineering • Privilege Misuse

	Password, PIN, One Time Password [“OTP”].		Data Storage							
2.5.3 Use of System Utilities										
2.5.3a	Application Owners, Technology Infrastructure Owners must restrict privileged access and the use of tools, services that are potentially capable of overriding system controls only to individuals where access is essential to perform their role.	Identify and Access Management	• Applications Security • Identity and Access Management • Secure Configuration Management • Vulnerability Identification and Management	9.4.4	PR[AC-4]	8.3 11.5	1.2 4.1 4.2 5.1 6.2 6.3	Preventative	• Disclosure of Sensitive Information by External Attacker and/or Trusted Insider • Disruption of Business Operations by External Attacker and/or Trusted Insider	• Privilege Misuse
2.5.3b	Application Owners, Technology Infrastructure Owners must remove or disable unnecessary software, protocols, services and ports from Technology Assets they own.	Secure Configuration Management	• Applications Security • Data Leakage Prevention • Secure Configuration Management • Vulnerability Identification and Management	9.4.4 12.7.1 13.1	PR[DS-5] DE[CM-7]	2.1 2.2 2.3 2.6	2.3 2.5A 2.10	Preventative	• Disclosure of Sensitive Information by External Attacker and/or Trusted Insider • Disruption of Business Operations by External Attacker and/or Trusted Insider	• Malware
2.6 Operations Security										
2.6.1 Security Architecture and ICS Controls										

Adoption										
2.6.1a	Chief Security Architect must support the governance of the ICS risk through definition and maintenance of security architecture principles, capabilities, and strategy for embedding ICS requirements into the Group's enterprise architecture layers.	Secure Configuration Management	• Applications Security • Cryptography • Data Leakage Prevention • Identity and Access Management • Network Security Management • Secure Configuration Management • Secure Asset Management • Vulnerability and Security Patch Management	14.2.1 14.2.5	PR[IP-1]	1.1	2.3 2.10	Preventative	• Financial Loss by External Attacker and/or Trusted Insider • Disclosure of Sensitive Information by External Attacker and/or Trusted Insider • Disruption of Business Operations by External Attacker and/or Trusted Insider	• Denial of Service • Privilege Misuse • Lateral Movement • Vulnerability Exploitation • Supply Chain Compromise
2.6.1b	Chief Security Architect reviews and approves cyber security architecture design, roadmaps and ensure the cyber security solution design is aligned to the approved.	Secure Asset Management	• Identity and Access Management • Network Security Management • Secure Configuration Management • Secure Asset Management • Security in Interactions with Third Parties	14.2.1 14.2.5	PR[IP-1]	1.1	2.3 2.10	Preventative	• Financial Loss by External Attacker and/or Trusted Insider • Disclosure of Sensitive Information by External Attacker and/or Trusted Insider • Disruption of Business Operations by	• Denial of Service • Privilege Misuse • Lateral Movement • Vulnerability Exploitation • Supply Chain Compromise

									External Attacker and/or Trusted Insider	
2.6.2 Operational Procedures and Responsibilities										
2.6.2a	Technology Infrastructure Owners must ensure technical security baselines are documented and available for owned Technology Assets.	Secure Configuration Management	• Identity and Access Management • Network Security Management • Secure Configuration Management	12.1.1	PR[IP-1]	1.1.2 2.5 3.7 4.3 5.4 6.7 7.3 8.8 9.10 10.9 11.6 12.11	2.3 2.10	Preventative	• Disruption of Business Operations by External Attacker and/or Trusted Insider	• Lateral Movement • Vulnerability Exploitation
2.6.3 Protection from Malware										
2.6.3a	Information System Owners, Application Owners, Technology Infrastructure Owners must protect Technology Assets they own from Malware in accordance with ICS Anti-Malware Standard.	Secure Configuration Management	• Anti-Malware • Secure Configuration Management • Security Patch Management • Vulnerability Identification and Management	12.2.1	DE[CM-4] DE[CM-5]	5.1 5.2 5.3	6.1	Preventative	• Financial Loss by External Attacker and/or Trusted Insider • Disclosure of Sensitive Information by External Attacker and/or Trusted Insider • Disruption of Business Operations by External Attacker and/or Trusted Insider	• Malware

2.6.4 Backup										
2.6.4a	Technology Infrastructure Owners must secure back-ups of Technology Assets that they support in accordance with ICS Data Storage and Backup Standard.	Secure Configuration Management	• Data Storage and Backup	12.3.1	PR[IP-4]	9.5.1 12.10.1	2.5A	Corrective	• Disruption of Business Operations by External Attacker and/or Trusted Insider	• Denial-of-Service • Malware
2.6.4b	Information System Owners, Technology Infrastructure Owners must ensure that backed-up Information is recoverable and useable.	Secure Configuration Management	• Data Storage and Backup	12.3.1	PR[IP-4]	9.5.1 12.10.1	2.5A	Corrective	• Disruption of Business Operations by External Attacker and/or Trusted Insider	• Denial-of-Service • Malware
2.6.4c	Technology Infrastructure Owners must retain the back-ups in a location separate from the business operations location.	Secure Configuration Management	• Data Storage and Backup	12.3.1	PR[IP-4] PR[PT-2]	3.4 9.5.1 12.10.1	2.5A	Corrective	• Disruption of Business Operations by External Attacker and/or Trusted Insider	• Denial-of-Service • Malware
2.6.5 Logging and Monitoring										
2.6.5a	Information System Owners, Application Owners, Technology Infrastructure Owners must configure the Technology	Secure Logging and Monitoring	• Applications Security • Security Logging and Monitoring • Secure Configuration Management • Security Incident Response	12.4 12.4.1 16.1	DE[CM-3] DE[CM-6] DE[CM-7] DE[	10.1 10.2 10.3 10.4 10.5 10.6 10.6.1 10.7 11.1	6.4 7.1	Detective	• Financial Loss by External Attacker and/or Trusted Insider • Disclosure of Sensitive	• Denial-of-Service • Lateral Movement • Malware • Phishing and Social Enginee

	Assets they own with the ability to record audit Information to logs, retain or secure them for any analyses, monitor for security events and incidents in accordance with ICS Security Logging and Monitoring Standard.		and Management		CM-8] ID[RA-1] ID[RA-5] PR[PT-1] PR[IP-1] PR[DS-2] PR[DS-5] PR[IP-12] RS[AN-1] RS[MI-3]	11.4 11.5 12.1 0.5			Information by External Attacker and/or Trusted Insider • Disruption of Business Operations by External Attacker and/or Trusted Insider	ring • Privilege Misuse • Supply Chain Compromise • Vulnerability Exploitation • Web-based attacks
2.6.6 Threat Identification										
2.6.6a	Application Owners, Technology Infrastructure Owners must monitor their Technology Assets and internal, external Threat Intelligence [TI] sources/advisories [e.g., regulators] for any security threats which may have potential impact to Technology Assets they own and/or support.	Secure Logging and Monitoring	• Security Logging and Monitoring	13.1.1	ID[RA-2] ID[RA-3]	6.6 11.3 12.2	6.4 7.1	Detective	• Financial Loss by External Attacker and/or Trusted Insider • Disclosure of Sensitive Information by External Attacker and/or Trusted Insider • Disruption of Business Operations by External Attacker	• Denial-of-Service • Lateral Movement • Malware • Phishing and Social Engineering • Privilege Misuse • Supply Chain Compromise • Vulnerability Exploitation • Web-based attacks

									and/or Trusted Insider	
2.6.7 Control of Operational Software										
2.6.7a	Application Owners, Technology Infrastructure Owners must only use software or tools where support is in place to ensure security patches are available for deployment.	Secure Configuration Management	• Applications Security • Secure Patch Management • Vulnerability Identification and Management	12.6 12.7.1	PR[IP-12] ID[RA-2]	6.2	2.2	Corrective	• Disruption of Business Operations by External Attacker and/or Trusted Insider	• Vulnerability Exploitation
2.6.8 Technical Vulnerability Management										
2.6.8a	Application Owners, Technology Infrastructure Owners must assess available security patches and apply them according to the S-BIA rating of owned Technology Assets and patch severity.	System Lifecycle Security (including Vulnerability Management)	• Secure Patch Management • Vulnerability Identification and Management	12.6.1	PR[IP-12] ID[RA-2]	6.6 11.1 11.2 11.3 11.6	2.2 6.1	Corrective	• Disruption of Business Operations by External Attacker and/or Trusted Insider	• Vulnerability Exploitation
2.6.8b	Application Owners, Technology Infrastructure Owners must ensure that security testing and vulnerability scanning are carried out on a	System Lifecycle Security (including Vulnerability Management)	• Secure Patch Management • Vulnerability Identification and Management	12.6.1	ID[RA-5] RS[MI-3]	6.1 6.2 11.2	2.7 6.5A 7.3A	Detective	• Disruption of Business Operations by External Attacker and/or Trusted Insider	• Vulnerability Exploitation

	regular basis and commensurate with the S-BIA rating of owned Technology Assets.									
2.6.8c	Application Owners, Technology Infrastructure Owners must ensure all identified vulnerabilities are remediated to the timescale defined within ICS Vulnerability and Security Patch Management Standard.	System Lifecycle Security (including Vulnerability Management)	• Secure Patch Management • Vulnerability Identification and Management	12.6.1	RS[MI-3]	6.1 6.2	2.7	Corrective	• Disruption of Business Operations by External Attacker and/or Trusted Insider	• Vulnerability Exploitation
2.6.9 Mobile Devices and Remote Working										
2.6.9a	Technology Infrastructure Owners must ensure the secure management of Group Information accessed or held on Mobile Devices.	Secure Configuration Management	• Applications Security • Data Leakage Prevention • Information Handling • Mobile Device Security	6.2	PR[AC-3]	4.1 8.1.5 8.3 8.5.1 12.3.8 12.3.9 12.3.10	2.5A 5.1	Preventative	• Disclosure of Sensitive Information by External Attacker and/or Trusted Insider	• Malware • Phishing and Social Engineering
2.6.10 Cryptography/Encryption										
2.6.10a	Information System Owners, Application Owners, Technology Infrastructure Owners must	Information Protection	• Information Handling • Cryptography	10.1.1	PR[DS-1] PR[DS-2]	3.4 3.5	2.1 2.6	Preventative	• Disclosure of Sensitive Information by External Attacker and/or	• Malware

	protect Group Information with cryptographic/encryption controls commensurate with the highest of IA rating or the highest of Classification level applied to the Group Information processed by the owned Technology Assets.								Trusted Insider	
2.6.10b	Application Owners, Technology Infrastructure Owners must protect cryptographic/encryption keys throughout their lifecycle.	Information Protection	• Cryptography	10.1.2	PR[AC-2] PR[PT-3]	3.5 3.6	2.1 2.6	Preventative	• Disclosure of Sensitive Information by External Attacker and/or Trusted Insider	• Phishing and Social Engineering
2.6.10c	Application Owners, Technology Infrastructure Owners must ensure that the Digital Certificates used in their Technology Assets are managed throughout its lifecycle in accordance with ICS Digital Certificate Management Standard.	Information Protection	• Digital Certificate Management	10.1.2 14.1.3	PR[AC-1] PR[DS-2]	4.1 8.6	2.1 2.6	Preventative	• Disclosure of Sensitive Information by External Attacker and/or Trusted Insider	• Web-based attacks

2.7 Network Security										
2.7.1 Network Security Management										
2.7.1a	Technology Infrastructure Owners must ensure that all access to and from the Group networks is controlled and monitored.	Network Security	• Identity and Access Management • Network Security Management • Secure Configuration Management • Web Filtering	9.1.2 13.1.1 12.4.	PR[AC-1] PR[AC-3] PR[AC-5] PR[PT-4]	1.1 10.1 10.2 10.3 10.4 10.5 10.6 10.7 10.8	6.4 6.5A	Preventative	• Disclosure of Sensitive Information by External Attacker and/or Trusted Insider • Disruption of Business Operations by External Attacker and/or Trusted Insider	• Denial-of-Service • Web-based attacks • Malware
2.7.1b	Technology Infrastructure Owners must ensure that network security architecture and associated documentation is maintained.	Network Security	• Network Security Management • Secure Configuration Management	9.1.2 12.4 13.1.1 13.1.2	PR[AC-5] PR[MA-2] DE[CM-7]	1.1 1.2 1.3 1.4 1.5	2.3	Preventative	• Disclosure of Sensitive Information by External Attacker and/or Trusted Insider	• Denial-of-Service • Lateral Movement • Web-based attacks
2.7.2 Segregation of Networks										
2.7.2a	Technology Infrastructure Owners must segregate the network to protect the Group Information Assets and Technology Assets commensurate with their IA or S-BIA rating.	Network Security	• Applications Security • Network Security Management • Web Filtering	13.1.3	PR[DS-2] PR[DS-5]	1.1.4 1.3	1.1	Preventative	• Disclosure of Sensitive Information by External Attacker and/or Trusted Insider	• Lateral Movement

2.7.3 Information Transfer										
2.7.3a	Technology Infrastructure Owners must protect the Confidentiality and Integrity of Group Information commensurate to its rating whenever transmitted across networks both internally and externally.	Network Security	• Information Handling • Cryptography • Network Security Management • Web Filtering	13.2.1 13.2.3 13.2.4	ID[AM-3] PR[AC-3] PR[AC-5] PR[DS-2] PR[DS-5] PR[PT-4]	3.4 4.1 4.2 4.3	2.1 2.5A	Preventative	• Disclosure of Sensitive Information by External Attacker and/or Trusted Insider	• Phishing and Social Engineering • Vulnerability Exploitation • Web-based attacks
2.8 Supplier Relationships										
2.8a	Outsourcing Owner/Contract Manager must ensure that the Third Party/Vendor arrangements include relevant security requirements and that an applicable Third Party Security Assessment [“TPSA”] is completed.	Third Party Security Management	• Security in Interactions with Third Parties	15.1.1	PR[MA-2] PR[AT-3] PR[AC-3] PR[AC-4]	8.1.5 8.3 8.5.1 12.3.9	2.8A	Preventative	• Disclosure of Sensitive Information by External Attacker and/or Trusted Insider	• Supply Chain Compromise
2.8b	Information System Owners, Technology Infrastructure Owners must document and enforce specific procedures for granting Third Party/Vendor access to their	Third Party Security Management	• Applications Security • Identity and Access Management [Third Party, Customer Access] • Security in Interactions with Third Parties	15.1.2	PR[DS-5] PR[IP-6] ID[AM-6] PR[AT-3]	8.1.5 10.8 12.2 12.3.9 12.4.1 12.8	2.8A 5.1	Preventative	• Disclosure of Sensitive Information by External Attacker and/or Trusted Insider	• Privilege Misuse • Supply Chain Compromise

	Technology Assets.									
2.8c	Information Asset Owners must, at the minimum, ensure that Restricted or Confidential Information and or Information Assets rated 4 or 5 owned is protected when it is handled or processed by Third Parties/Vendors.	Third Party Security Management	• Applications Security • Identity and Access Management [Third Party, Customer Access] • Security in Interactions with Third Parties	15.1.2 15.1.3	ID[AM-6] PR[AT-3]	12.8 12.9 12.11	2.8A 5.1	Preventative	• Disclosure of Sensitive Information by External Attacker and/or Trusted Insider • Disruption of Business Operations by External Attacker and/or Trusted Insider	• Supply Chain Compromise
2.9 Information Destruction										
2.9a	Information System Owners, Technology Infrastructure Owners must securely decommission their owned Technology Assets and dispose of all storage media by ensuring the Group Information Assets within are securely destroyed. destroyed.	Information Protection	• Secure Decommissioning and Destruction	8.3.2 11.2.7	PR[IP-6] PR[DS-3]	3.1 3.2 3.6.5 9.8	-	Preventative	• Disclosure of Sensitive Information by External Attacker and/or Trusted Insider	• Privilege Misuse • Supply Chain Compromise
2.9b	Information Asset Owners must authorise	Information Protectio	• Secure Decommissioning and	8.3.2 11.2.7	PR[IP-6] PR[	3.1 3.2 3.6.	-	Prevent	• Disclosure of Sensitiv	• Privilege Misuse

	and ensure secure destruction of owned Information Assets in accordance with ICS Secure Decommissioning and Destruction Standard.	n	Destruction		DS-3]	5 9.8		ative	e Information by External Attacker and/or Trusted Insider	• Supply Chain Compromise
2.10 Incident Management										
2.10 a	Information Asset/System Owners, Technology Infrastructure Owners must manage identified security events and incidents that affect the Confidentiality, Integrity or Availability of Group Information Assets and Systems to prevent damage, restore the affected and prevent recurring incidents.	Security Incident Management	• Security Incident Response and Management	16.1	DE[AE-1] DE[AE-2] DE[AE-3] DE[AE-4] DE[AE-5]	11.1.2 12.5.3 12.10	7.1	Corrective	• Financial Loss by External Attacker and/or Trusted Insider • Disclosure of Sensitive Information by External Attacker and/or Trusted Insider • Disruption of Business Operations by External Attacker and/or Trusted Insider	• Denial-of-Service • Lateral Movement • Malware • Phishing and Social Engineering • Privilege Misuse • Supply Chain Compromise • Vulnerability Exploitation • Web-based attacks

10. GLOSSARY

The ICS Glossary has been defined and is available via the GovPoint – see the Technology Glossary via the *GovPoint Glossary* reference.

Appendix A – Version Control Table

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISRO ICS Policy	Alignment to ERM/FPGS template. Control statements, control domains restructured, some controls uplifted from underlying standards and a few new controls introduced.	Material	Group CISO	1.0	22-Jan-19	22-Jan-19
CISRO ICS Policy	2019-20 Annual Review changes includes: 1. Alignment to ERMF latest Policy template & ERM review feedback incorporated 2. Alignment to revised ICS RTF. 3. Minor corrections to Policy Statements and updates based on Group CISO, CISRO Organisational changes. 4. Inclusion of NEW Threat Identification [2.6.5]	Non-Material	Group CISRO	2.0	31-Mar-20	31-Mar-20
Liz Banbury	2021 Annual Review changes includes. 1. Alignment to ICS RTF v3.1 for Application Owner, Technology Infrastructure Owner, Policy variation model, Non-compliance model, Policy effectiveness review model.	Non-Material	Darren Argyle, Group CISRO	3.0	03-Jun-21	03-Jun-21

	2. Minor tweaking made to support Group Flexible working approach and restrict Staff from using only Group approved Systems, IT Equipment. 3. Inclusion of a NEW statement 2.2.3 c. Merged previous 2.1 i with revised 2.1 c. Previous 2.1 g. has been separated for Information retention under revised 2.1 i. Removed Mandatory Statements [2.1 a & 2.1.1 d.]. Statements 2.3.1 a, b & c have been merged under 2.3.1 a. 4. Where necessary corrections/minor updates made to certain mandatory Policy statements. 5. Section 4.2 updated to include Policy refresh cycle & its validity. 6. Inter-connected Policies are updated to Group ERM Policy repository. 7. Previous Section 9.2 has been removed but Industry Mappings are merged under enhanced mapping table under Section 9.2. Included mappings to Swift CSCF 2020, ICS RTF					

	Risk Objectives, Risk Categories/Sub-Types, Threat Vectors. 8. Glossary directed to ICS Glossary of Terms.					
CISRO ICS Policy	2022 Annual Refresh includes alignment to ERM Policy template and the following changes: 1. Section 1 – • Technical Information Security Standards [TISS] have been removed from CISRO Policy ownership and maintenance further to ownership handover to Security Architecture [SACA] effective 1Sep2021. • Included ICS Methodologies [IA & S-BIA] 2. Section 2 – • Minor modification to All Staff and People Manager statements in relation to secure working practices [2.1.f & 2.1.1.b]. • Reporting of suspicious phishing email by All Staff [2.1.g] • Removed Information Custodian across Policy statements as an alignment to ICS RTF v4.0 • Throughout mandatory Policy statements &	Non-Material	Darren Argyle, Group CISRO	4.0	30-Jun-22	30-Jun-22

	where relevant, replaced term 'Systems' with 'Technology Assets' • Updated Asset Ownership & Inventory model for alignment with ICS Standards [2.2.1] • Clarity added to IAO role. • Rewritten statement as a result of TISS model changes [2.6.1.a]. • Introduced Process Owner role for ICS operational aspects [2.6.1.b]. • Consolidated Logging and Monitoring in a single statement under 2.6.4.a & removed 2.6.4.b & 2.6.4.c • Removed redundant statements [2.6.8.a & 2.9.a, 2.9.b, 2.9.c] as objectives of Cloud Security already covered in 2.8. • Meaning corrections are made & hyperlinks updated where required. 3. Section 3 – • R&R updated in alignment with ICS RTF v4.0 & its Risk Management and Governance R&R document. • Further clarity added to IAO & ISO roles & removed responsibilities not					

	relevant at Policy level. 4. Section 7 – • CSR, DM Policies are updated for Policy Ownership, Area of Connection & a similar update made to Group Disciplinary Standard. Added DARM Policy. 5. Section 8 – • Included Secure Asset Management & removed Self-Service Terminal in Standards list. 6. Section 9.2 – • Table updated w.r.t. changes proposed in Section 2, ICS RTF Risk Objectives & Categories. 7. Replaced Riskpod references & Inter-connected Policy links updated with ERM GovPoint references.					
CISRO ICS Policy	2023 review includes following key changes: 1. Policy Template updated to ERM Policy Template v7.7 2. Roles updated (People Managers to People Leaders & HICS to CISO Business/Functions/Markets). 3. Section 3.2 - All Staff & People Leader	Non-Material	Darren Argyle, Group CISRO	4.1	02-Jun-23	02-Jun-23

	requirements are consolidated or enhanced w.r.t new ICS Acceptable Use Standard. 4. Added a new ICS Standard (Acceptable Use Standard) 5. Inter-Connected Policy & Standards updated where feedback was to update.					
OTCR TTO ICS Policy	2024 review [ICSCR-21May24-4] includes following key changes: 1. Policy Template updated to ERM Policy Template v7.8 2. Alignment to ICS Organisational changes such as Policy Approval, Ownership & Maintenance from CISRO to OTCR, updated ICS Non-Compliance, Dispensation process. 3. Included ICS LRM baseline to be in line with Group MRC & ICS MRC Process. 4. Proposed Chief Security Architect, Updated Process/Service Owners role	Non-Material	Mark Strange	5.0	26-JUN-2024	01-JUL-2024

	and responsibility. 5. Policy review frequency to be annual to comply with Group LRM [ICSCR-15Apr24-2]. 6. Replaced risk sub-type basis ERM feedback.					
Bali Chandramouli	Template updated to ERM Policy Template v9.0 Updated for OTCR delegation of Group ICS Standards to CISO.	Material	Mark Strange	6.0	29-Nov-24	02-Dec-24