Secure Configuration Management Standard

Version No	3.3
Document Type	Standard
Parent Document	Group Information and Cyber Security Policy
Parent Framework	Information & Cyber Security RTF
Document Approver Name	Jamie Cowan
Document Approver Job Title	Head, ICS Risk Framework & Governance
Document Owner Name	Ibrahim Gathungu
Document Owner Job Title	Director, ICS Standards
Document Contact Name	Arti Singh
Document Contact Job Title	Assoc. Director, ICS Standards
Business Scope	All Businesses
Function Role	All Functions
Geography Scope	Global
Effective Date	16-Dec-24
Approval Date	4-Dec-24
Next Review Date	30-Jun-2027

Table of Contents

Version Control Table

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Arti Singh [ICS Standards]	Administrative changes introduced to update document template, references, roles and ownership.	Non-material	Jamie Cowan Head, ICS Risk Framework & Governance	3.3	04-Dec-24	16-Dec-24

1 INTRODUCTION AND PURPOSE

This Information and Cyber Security Standard defines the minimum set of requirements for the Secure Configuration and Management [SCM] of Information Systems and Technology Infrastructure.

In the context of Information Security, configuration management is the application of appropriate configuration settings to utilise existing security features and functionality and to limit security vulnerabilities. This is mainly derived by deploying those configurations firstly during the build and thereafter managing those settings into production and on an on-going basis.

This Standard defines the governance for developing and maintaining documented security configuration requirements and the reviews required of those configuration settings for the hardening and secure management of Information Systems and Technology Infrastructure.

Secure Configuration Management is important as these settings provide a key control in protecting Information both in transit and whilst being stored within the Group's environment. Applying the correct settings reduces the likelihood of unauthorised access to those Information Systems and Technology Infrastructures.

1.1 Risks

Failure to use cryptography appropriately and correctly may lead to a breach to the confidentiality and/or integrity of data which may result in:

- 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.

1.2 Scope

This Standard must be read, and controls deployed in conjunction with all other ICS Standards.

The Standard is mandatory and applies to the Group businesses, functions, countries, and regions except where explicitly prohibited by local Law or Regulation [assessed as per section 4.2. Reporting Non-Compliance].

Note: In case of any Country specific LRM requirement, the approach defined in ERMF (Chapter Eleven, Part B, section 4.2 "Country-level Host Regulatory Obligations") must be followed.

The Standard covers all Group Information Assets which are processed and or used by the Group's Information System [wherever the term 'Systems' or 'Information System' is used in a control statement it refers to both Information System and Technology Infrastructure].

Where the Control Statements include Information Asset [IA] or Security-Business Impact Assessment [S-BIA] ratings, they are applicable only to those rated Systems. All other Control Statements apply to all Systems regardless of ratings and hosted environments [Production or Non-Production unless stated otherwise].

The Systems owned and or managed by the Third Parties [including Cloud Systems, Vendor Systems, Regulatory Systems, Self Service Terminal [SST] and similar], must additionally refer to the ICS Standards for Security in Interactions with Third Parties and Secure Configuration Management.

Please note, any Systems which are deemed as 'Standalone Machines' must be assessed using the Security – Business Impact Assessment [S-BIA] and controls must be applied accordingly in line with applicable ICS controls defined in ICS Standards.

2 ROLES & RESPONSIBILITIES

All Staff

All Staff are responsible for the safety of Group Technology Assets under their care, the security of Group Information allowed for accessing via the Technology Assets and for compliance with the applicable Control Statements defined in this Standard.

Information System Owner

A named individual accountable for the protection of owned Information System and for compliance with applicable Control Statements defined in this Standard.

Technology Infrastructure Owner

A named individual accountable for the protection of owned Technology Infrastructure and for compliance with applicable Control Statements defined in this Standard.

People Leader

People Leaders must comply with the requirements and ensure that their Staff are made aware of their responsibilities in complying to this standard.

Process Owner

POs (as defined by Enterprise Risk Management Framework) are Business or Function managers responsible for the end-to-end business or function processes as identified within the Group's Process Universe.

They are responsible for identification and management of the end-to-end process as defined in the Group's Process Universe and associated risks, including ICS related activities as mandated by the Standard.

The PO is responsible for ensuring the provision of quality, timely, and adequate data, and management information to measure appropriate coverage and performance of control points (and subsequent measurement) against ICS Policy and Standards.

CISO ICS Standards & Controls

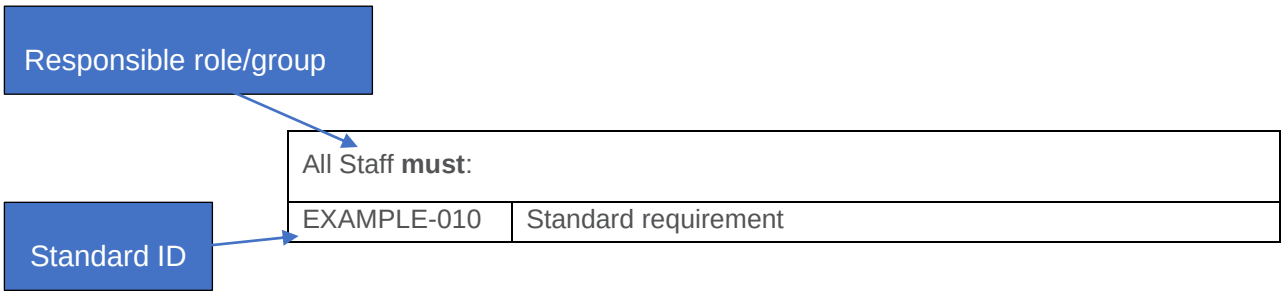
The CISO is the owner of this Security Standard and will ensure the document is updated to an agreed schedule.

***Note**: The Responsible role who 'must' execute against this standard can do so either directly or by delegation. Where this is the case and a delegate exercises the control, the named role remains accountable.*

All roles & responsibilities including their corelations within ICS risk management activities are defined in Chapter Eleven, Part B, section 2 "Three LoD Responsibility and Governance Committee Oversight" of the Enterprise Risk Management Framework.

3 STANDARD REQUIREMENTS

This section outlines minimum mandatory requirements that apply to this Standard. The requirements are set out in the following format:



3.1 Control Area: On-Boarding

Information System Owner and/or Technology Infrastructure Owner **must:**	
SCM-010	Ensure their Information Systems and Technology Infrastructure are on-boarded as per the Group Technology & Operations [T&O] Asset Management section within the Group IT Policy and ownership is defined. *[Reference: Group Technology Policy]*
SCM-020	Ensure their Technology Infrastructure are S-BIA for criticality and ratings assigned. *[Reference: S-BIA Methodology]*

3.2 Control Area: Secure Design and Configuration

Process Owner [Security Architecture] **must:**	
SCM-030	Develop, document and maintain minimum security baseline control requirements for Information System(s) and Technology Infrastructure. *[Note: the controls could be applicable to both Application and Technology Infrastructure layers]*

Process Owner [CAT-SIA] **must:**	
SCM-028	Execute and document minimum security baseline control requirements verification and ensure any identified deviation (from the expected control compliance for Information System) is documented, tracked and handed over to respective risk management processes.

Technology Infrastructure Owner **must:**	
SCM-031	Devise mechanisms to logically apply and maintain security baseline configuration (as per minimum security baseline control requirements) on Information System and Technology Infrastructure.

Application Owner [Technology Product Owner] **must:**	
SCM-032	Ensure that identified security requirements (as per minimum security baseline control requirements) are embedded (if required) in Application (layer) as standard builds or customised for specific Information System deployments.

Information System Owner **must:**	
SCM-033	Ensure that identified security requirements for the owned Information System(s) are deployed in line with pre-defined approach and scope.

Information System Owner and/or Technology Infrastructure Owner **must:**	
SCM-050	Ensure the Security Configuration settings of their Information Systems and Technology Infrastructure have addressed all known security configuration vulnerabilities before production on-boarded.

3.3 Control Area: Secure Configuration Review

Process Owner [CAT-IS] **must:**	
SCM-065	Define, document, and execute an approach to security baselines verification via periodic checks of the Technology Infrastructure components configuration. *Note: frequency of the configuration scans to be aligned with "Vulnerability Identification frequency" as defined in the VIAM Standard.* *Note: automated checks to be executed only against pre-defined security baseline; controls corresponding with respective Information Systems deployment to be checked in line with current assurance and control testing approaches*

Process Owner [CAT-SVLM] **must:**	
SCM-066	Ensure that any deviation from the expected, predefined security configuration is reported to respective Asset Owners for remediation and provide governance, tracking and reporting for identified configuration non-compliances and issues to ensure timely and correct removal of the security gaps.

Information System Owner and/or Technology Infrastructure Owner and/or Application Owner **must:**	
SCM-067	Remediate identified configuration non-compliance in line with predefined deployment definition.

3.4 Control Area: Classify Configuration Information

Information System Owner and/or Technology Infrastructure Owner **must:**	
SCM-090	Define the rating of Configuration Information on Information Systems and Technology Infrastructure. *[Reference: ICS Information Classification and ICS Information Handling Standards]*

3.5 Control Area: Secure Configurations

3.5.1 To Securely Configure Information Systems and Technology Infrastructure

Information System Owner and/or Technology Infrastructure Owner **must**:	
SCM-100	Synchronise the clocks of all Information Systems and Technology Infrastructure to the Group's central time source and protect from tampering.
SCM-120	Limit the ability to read or write Configuration Information and the ability to access and use System Utilities to authorised administrators. Administrative access via non-console must be encrypted. *[Reference: ICS Cryptography Standard for secure algorithms and protocols]*
SCM-130	Separate system related Information from business Information and define access. *For Example: system related Information such as event logs, Configuration Files, System Utilities, Database instances.*
SCM-135	Identify and document all software which fall under System Utilities and document appropriate level of access.
SCM-140	Configure software or hardware [physical] tokens to the requirements defined by this Standard. *[Reference: Appendix 7 – Table: Points 17 to 21]*
SCM-150	Implement a firewall between guest virtual machines to separate Payment Card data from other security domains [non-payment card data] if they are both hosted on the same hypervisor.
SCM-170	Configure Access Warning messages.
SCM-180	Closely monitor the end of support dates of hardware and software and proactively manage the lifecycle of the products in use to ensure all products are supportable, so as to mitigate information security risks, such as those arising from the non-availability of security patches. Where any hardware or software products are approaching end of support or will continue to be used after end of support, assess the risks associated and ensure appropriate risk management.

3.5.2 To Securely Configure OS, Databases and Network Devices

Information System Owner and/or Technology Infrastructure Owner **must**:	
SCM-210	Only use secure protocols for configurations. *Examples of insecure protocols includes FTP, Telnet, POP3, IMAP, SNMP V1 and V2, SSL 3.0 and below versions and TLS 1.1 and below versions.*

3.5.3 To Securely Configure Web Browsers

Information System Owner and/or Technology Infrastructure Owner **must**:	
SCM-220	Restrict Staff from changing any software security settings and ensure global enforcement of security policies for laptops and end-user devices.

3.5.4 To Securely Configure Messaging Systems

Information System Owner and/or Technology Infrastructure Owner **must**:	
SCM-240	Define maximum number of recipients, message size, attachments per email and limit storage size.
SCM-250	Configure filtering at the email application server [the server hosted with email application].
SCM-260	Configure client systems security settings at the email application server end and access defined.
SCM-280	Configure the following conference settings on Instance Messaging application: a) Allow only trusted servers; b) Encrypt server connections.

3.5.5 To Securely Configure Web Infrastructure Services

Information System Owner and/or Technology Infrastructure Owner **must**:	
SCM-290	Separate web servers and database servers and limit access permissions between the two.
SCM-300	Disable web server file directory listing and browsing. The files must be saved in a defined path which is access defined.
SCM-310	Use secure techniques to prevent Group web sites from web and spam bot attacks.
SCM-320	Ensure the error output messages do not reveal Configuration Information.
SCM-330	Enable security features that come pre-built with the web services application.
SCM-340	Define: a) Number of web server processes and/or network connections; b) Size of HTTPS request and response headers.

3.5.6 To Securely Configure Network Devices

Information System Owner and/or Technology Infrastructure Owner **must**:	
SCM-350	Disable IP aliasing and use MAC address filtering for end points that do not support 802.1x authentication with Digital Certificates.
SCM-360	Not expose the Group's network addressing structure and directory Information external to the Group.

3.5.7 To Securely Configure Office Equipment and Mobile Devices

Information System Owner and/or Technology Infrastructure Owner **must**:	
SCM-420	Configure the Office Equipment to ensure that Group Information processed by the equipment are maintained secure and prevented from unauthorised access.
SCM-430	Disable direct printing. *Note: Direct printing prevents user authentication and logging of print jobs. For Example: Wireless printing from user device.*

Information System Owner and/or Technology Infrastructure Owner **must**:	
SCM-440	Authorise Remote Administration of Office Equipment from a non-Group premise. The activities must be time-bound, monitored, and logged. *[Reference: ICS Security in Interactions with Third Parties Standard]*

3.5.8 To Securely Configure Self-Service Terminals

Information System Owner and/or Technology Infrastructure Owner **must**:	
SCM-590	Ensure disk encryption is enabled. Note: This is to prevent the loss of confidential or restricted data in the event of loss of SST hard disk.
SCM-600	Ensure encryption and authentication is enabled between SST PC core and cash dispenser.
SCM-610	Ensure removable media interfaces or ports are disabled.
SCM-620	Ensure application allow list/sandboxing is implemented to run only authorized application executables, DLLs, and binaries. Note: The application allow list policy to be maintained updated and reviewed on an annual basis.
SCM-630	Ensure the administrative access over the internal or external network must be encrypted using Group approved Cryptographic algorithms. *[Reference: ICS Standard Cryptography]*
SCM-640	External users (i.e., vendors): a) do not have direct or remote network access to the SST unless there is a contractual requirement. b) b) if remote access is required for service purposes, then access must be explicitly authorised by the Country SST Channel Manager and/or Country Technology Manager.
SCM-650	Ensure SST Terminal Master Keys [TMK] are unique on each SST and renewed every 3 years.
SCM-660	Ensure that logical separation between multiple applications run on SST is enforced. *Note: It should not be possible that one application interferes or tampers with another application or the OS of the SST.*

3.6 Control Area: Security Assessments

Information System Owner and/or Technology Infrastructure Owner **must**:	
SCM-480	Complete the Group's security risk assessment and ensure that the application of risk mitigation controls has been carried out before production on-boarding. *Note: The security risk assessment includes identification of Security Threats to which a Technology Infrastructure is vulnerable to.*

3.7 Control Area: Security Testing

Information System Owner and/or Technology Infrastructure Owner **must**:	
SCM-510	Record security testing results, track for risk mitigations and address before production on-board.

3.8 Control Area: Implementation

Information System Owner and/or Technology Infrastructure Owner **must**:	
SCM-520	Adhere to Group's change and version control requirements for the protection of configuration settings.
SCM-530	Restrict configuration settings and/or file access only to an administrative account which is vaulted.
SCM-540	Ensure the deployment is performed with minimum required permissions.
SCM-550	Remove all unwanted components before production on-boarding. *[Reference: AS-530]*

3.9 Control Area: On-Going Configuration Changes

Information System Owner and/or Technology Infrastructure Owner **must**:	
SCM-580	Approve or ensure approval by any relevant authorities from the Group for the configuration changes required to be performed at a Third-Party environment impacting Group Information.

4 INFORMATION & SUPPORT

4.1 General Information and Support

For queries relating to this Security Standard please contact the ICS Standards team via: *ICSStandards*.

4.2 Reporting Non-Compliance

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

4.3 Breach of this Standard

- Failure to comply with this Standard may result in formal action under the Group Disciplinary Standard, that for serious breaches could include termination of employment.
- Any actual or suspected breaches must be reported immediately to your People Manager or to your Compliance representative from the Group.
- All breaches of this Standard must be reported to the Document Owner of the Standard.

5 GLOSSARY

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

6 REGULATORY / INDUSTRY REFERENCES

All Regulatory/Industry References are available via the *ICS Master Control List* document published on: *Control Framework Library*

7 APPENDIX

7.1 Security Configuration Categories

Categories
1. Set hardware BIOS and boot options. 2. Limit network services and ports and protocols [use only approved services and protocols and remove any not required]. 3. Disable insecure and unnecessary services, ports. 4. Remove unnecessary software. 5. Remove unnecessary accounts. 6. Remove unnecessary compilers and interpreters. 7. Prevent anonymous access. 8. Restrict access to Configuration File. 9. Apply login and session Idle-Timeout restrictions to 15 minutes. 10. Apply security patches. *[Reference: ICS Security Patch Management Standard]* 11. Limit file sharing. 12. Prevent the use of host IP based authentication. 13. Configure logging and monitoring. *[Reference: ICS Security Logging and Monitoring Standard]* 14. Configure clock synchronisation. 15. Configure access control and privileged access. *[Reference: ICS Identity and Access Management Standard]* 16. Change or remove default authentication settings and/or encryption keys. 17. Remove token files after completion of import activities. 18. Define expiration data for tokens and loss of tokens must be disabled. 19. Store PIN or other authentication credentials with one-way encryption to ensure they cannot be read or recovered and matched against a specific account. 20. Bind software tokens with the device. 21. Manage Tokens and protect its data from unauthorised access and changes.

Appendix A – Version Control Table

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISO Policy	Migration to ERM Standard template. This Standard is a consolidation of control statements from following Standard documents. Business & Middleware Applications V4.0, Compliance and Vulnerability Management, Corporate Banking Channels V1.0, Database Management System V4.0, Firewall Standard V3.1, HSM V4.0, Intrusion Detection Standard V3.1, Messaging Application V4.0, Network Devices HLSTS V4.0, Network Services, Application HLSTS V4.0, NSM Standard V3.1, Operating Systems V4.0, System Utilities V4.0, WAF Standard V3.0,		Liz Banbury, Global Head, ICS Policy and Risk.	1.0	14-Feb-20	19-Feb-20

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	Web Infrastructure Services V4.0, Wireless Networks Standard V3.1. & Consultation feedback, corrections incorporated.					
CISRO ICS Policy	Enhancement of SCM-120 & SCM-130; SCM-135 added.		Liz Banbury, Global Head, ICS Policy and Risk.	1.1	15-Jan-21	20-Jan-21
CISRO ICS Policy	Annual review: Risks, Roles and Responsibilities alignment to RTF. Alignment to individual controls and incorporation of ICSCR-17May2021-1: New controls: SCM-031, SCM-065 Modified controls: SCM-030, SCM-060, SCM-180, SCM-190 Removed controls: SCM-040, SCM-070, SCM-080, SCM-110, SCM-160, SCM-200, SCM-370-SCM410, SCM-450-SCM-470,		Samantha Finan, Global Head, ICS Policy, Standards and Reporting	2.0	15-Dec-21	21-Dec-2021

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	SCM-490, SCM-500, SCM-560, SCM-570					
CISRO ICS Policy	Based on Change Requests, additional standard review, and SST Standard termination: New: SCM-028, SCM-032, SCM-033, SCM-066, SCM-067 Modified: SCM-030, SCM-031, SCM-065, SCM-220, Administrative: SCM-550 SST controls: SCM-590-660 Removed: SCM-060, SCM-190, SCM-230, SCM-270		Samantha Finan, Global Head, ICS Policy, Standards and Reporting	3.0	30-Jun-22	02-Jul-22
CISRO ICS Policy	Editorial change: duplicate phrase removed from SCM-640		Samantha Finan, Global Head, ICS Policy, Standards and Reporting	3.1	7-Jul-22	14-Jul-22
CISRO ICS Policy	Editorial changes: 1. Template update (as per the STD Template for Group		Paul Hoare Head, ICS Policy and Best Practice	3.2	24-Apr-23	24-Apr-23

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	Standards v5.6) SCM-028, 065 and 065 role reference update as per the ICSCR-07Mar23-1					