Secure Asset Management Standard

Version No	1.2
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	Katarzyna Wencka
Document Contact Job Title	Director, ICS Standards
Business Scope	All Businesses
Function Role	All Functions
Geography Scope	Global
Effective Date	16 December 2024
Approval Date	4 December 2024
Next Review Date	30 June 2027

Table of Contents

Version Control Table

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Katarzyna Wencka **[ICS Standards]**	Administrative changes introduced to update document template, references, roles and ownership.	Non-material	Jamie Cowan Head, ICS Risk Framework & Governance	1.2	04-Dec-24	16-Dec-24

1 INTRODUCTION AND PURPOSE

For the Group, to ensure the ICS Risk is managed within the Group defined risk appetite, thus to make informed, business and risk-driven decisions regarding the owned Technology Assets, information about what Assets the Group possesses and what is their status, is critical. The Information and Information Systems (with underlying Technology Infrastructure) that enable the organisation to achieve business purposes must be identified and managed consistent with their relative importance to organisational objectives and the organisation's ICS risk strategy.

Another key consideration is the ability of the Group to demonstrate the compliance with regulatory aspects, which might be significantly impacted without relevant, accurate and up to date Asset Inventory.

All industry standards and best practises list the Asset inventory and management related controls as primary and fundamental to effective and comprehensive ICS strategy delivery in the organisation.

Asset Management is critical to safeguard each and every ICS risk management activity is effective, timely and produces reliable outcomes by:

1) ensuring more effective and comprehensive ICS risk identification through identification of the Assets, their criticality and ownership,
2) supporting timely risk mitigation and containment through enabling faster identification & response to security threats and issues,
3) increasing cyber resilience through applying right focus to most critical Assets,
4) reducing the attack surface through effective identification of applicable security measures and Asset status, characteristics, and compliance,
5) facilitating better discovery of Assets misuse or unauthorised Assets based on the existing inventory, criticality of the Assets and their acceptable use.

The purpose of the Standard is to:

1) define the required data elements and attributes to be recorded and maintained in the Asset Inventory, to ensure the ICS risk management goals and objectives can be sufficiently supported,
2) mandate key ICS Asset Management aspects and controls, to support existing Technology & Operations standards and processes and ensure the ICS aspects are being addressed accordingly,
3) document the requirements and key security considerations to enable the ongoing ownership and effective management of the Group Information Assets,
4) address the operational requirements to meet the ICS strategic objectives,
5) outline the key ICS aspects within the Asset lifecycle and management.

1.1 Risks

This Standard mandates the Asset Management approach is implemented to protect the Information Assets and Information Systems that comprise the Group's network and support accurate, timely and effective ICS risk identification and management. When the Assets are not documented and tracked, the cybersecurity strategy and ICS risk management processes are likely to fail due to lack of vital knowledge regarding the Assets when the risk can arise or materialise.

Failure to adopt and implement this Information Security Standard may expose the Group to Risk 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 scope of the Standard is to supplement and address the ICS requirements within the Asset Management area.

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 Systems [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 in line with applicable ICS controls defined in ICS Standards.

1.3 Out of Scope

No Information Systems and Technology Infrastructure (as listed in section 1.2 'Scope') are considered out of scope of the Standard. However, in the case where certain ICS controls cannot be deployed due to tangible process or technology limitations specific for some hosting models (for example: Information Systems delivered in SaaS model), equivalent contractual or compensating controls must be in place to ensure the controls objectives are met.

2 ROLES & RESPONSIBILITIES

Group Chief Information Security Officer (Group CISO)

The Group CISO is accountable for establishing a Process(es) to ensure that the Group approach to Information Asset Management is delivered in a consistent and comprehensive manner, across various business and functions. In addition to that, Group CISO must appoint Process Owner(s) and ensure a model for Process effectiveness validations is in place.

Group Technology (Technology)

The Technology & Operations is accountable for establishing a Process(es) to ensure that the Group approach to IT Asset Management is delivered in a consistent and comprehensive manner, across

various business and functions. In addition to that, T&O must appoint Process Owner(s) and ensure a model for Process effectiveness validations is in place.

Process Owner
Process Owners (of Asset Management and ITSM/ITAM Processes) are accountable for defining and implementing operational approach to Asset Management in line with the Standard requirements. In addition to that, PO is accountable for providing operational capability to support Information System/Technology Infrastructure/Application/Information Asset Owners to deliver required objectives of the Standard.

Process Owners (as appointed within Process Universe) are accountable for identification of Assets supporting their Processes and appointing Asset Owners as well as overall oversight of the Asset related records accuracy.

Information Asset Owner
Information Asset Owners are accountable for complying with the control areas of the Standard, which are applicable to them, to ensure the Group approach to Information Asset Management is effective and meets predefined objectives.

Information System/Technology Infrastructure/Application Owners[1]
Information System/Technology Infrastructure/Application Owners are accountable for complying with the control areas of the Standard, which are applicable to them, to ensure the Group approach to IT Asset Management is effective and meets predefined objectives.

All Staff
All Staff are required to read and comply with the requirements of this Security Standard which are directly relevant to them.

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

CISO ICS Standards & Controls
The CISO is the owner of this Information Security Standard and will ensure the document is updated to an agreed schedule.

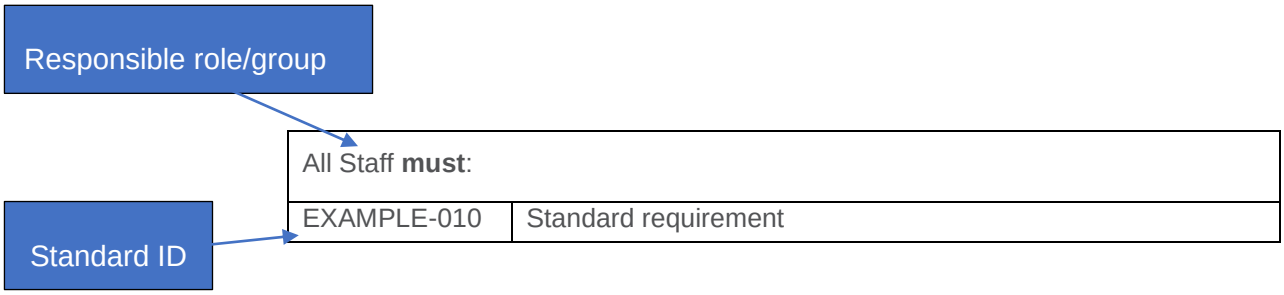
***Note**: The Responsible role who **'must'** execute against this standard can do so either directly or by delegation. Where this is the case and a delegate exercises the control, the named role remains accountable.*

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.

[1] The agreed mapping of the ICS to Technology roles is listed in section 7.2.2 "ICS and Technology Terminology References"

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: Technology Assets – Information Systems, Applications, Technology Infrastructure

3.1.1 Secure Asset Management – Process Definition, Delivery, Maintenance and Governance

Group Technology **must**:	
SAM-010	Own, define and maintain the relevant Standard(s) addressing key aspects of the Technology Asset Management requirements with the (applicable) controls of the Standard embedded.
SAM-020	Establish an operational definition to the approach to Technology Asset Management by: 1) establishing Process(es) for Technology Asset Management, 2) appointing Process(es) Owner(s), 3) defining a model for Process effectiveness, oversight, and compliance validation. *[Reference: ERMF – Process Owner definition]*

Process Owner [Technology Asset Management] **must**:	
SAM-030	Define, deploy, and maintain an operational approach to Technology Asset Management (thought the relevant Standard controls adoption) by: 1) defining, delivering, and maintaining BAU and operational Process procedures to ensure the controls of the Standards are met, 2) determining and communicating requirements and procedures for Information System/Technology Infrastructure/Application Owners/All Staff, essential to ensure predefined compliance level (with the Process level requirements) 3) ensuring that approach scope considers Information Systems, Technology Infrastructure and Applications.
SAM-040	Deliver operational capability to ensure Technology Asset Management accountabilities of the Information System/Technology Infrastructure/Application Owners can be fulfilled by identifying, deploying, and maintaining resources required to support Process objectives (such as tooling, operational procedures, etc.).

3.1.2 Technology Assets Inventory

Process Owner [Technology Asset Management] **must**:	
SAM-050	Define, implement, and maintain the Technology Asset Inventory: 1) in line with the predefined Process approach, 2) that defines mandatory data and attributes recording and retaining requirements for specific Asset categories, such as outlined in section 7.1 “Technology Asset Inventory & CMDB – mandatory data elements”, 3) that support operational and cyber resilience requirements thought capturing information regarding Assets supporting Important Business Services – to be moved under CMDB 4) supporting key asset management activities such as: a. service catalogues for Asset related requests, b. reporting and MI’s c. IT Asset audit d. maintenance, monitoring, planning and scheduling operations for an IT Asset or group of Assets.
SAM-060	Define and deploy data quality and governance requirements to ensure completeness and factual accuracy of the Inventory (such as periodic reviews, records completeness checks, etc.).
SAM-070	Ensure that the Inventory is facilitated by a tooling supporting the approach to Technology Asset Inventory and providing functionalities to the Asset Owners and key stakeholders allowing them to discharge their accountabilities[2].

3.1.3 Configuration Management

Group Technology **must**:	
SAM-072	Ensure that: 1) Process(es) for Technology Assets Configuration Management required to maintain and manage Technology Assets configuration is defined and maintained, 2) the Process is supported with a configuration management database [CMDB], 3) Process(es) Owner(s) is appointed, 4) a model for Process effectiveness, oversight and compliance validation is in place.

Process Owner [Configuration Management] **must**:	
SAM-074	Support Technology Asset Management Process by maintaining CMDB and corresponding operations which: 1) records the information regarding configuration items [CI] for Technology Assets, 2) keeps the required level of attributes, as defined in section 7.1 “Technology Asset Inventory & CMDB – mandatory data elements” 3) supports the status and lifecycle management of the Technology Assets, 4) keeps and maintains the information regarding Technology Assets/CIs dependencies and architecture attributes.
SAM-076	Communicate (applicable) configuration guidelines to impacted Asset Owners.

[2] The functionalities are considered as end-user features that support the Asset Inventory workflow and use-cases (adding, updating, removing Assets) as well as reporting/MI/data feed capabilities to support corelated processes and key stakeholders

Process Owner [Technology Asset Management] **must**:	
SAM-080	Support Asset identification & inventory data accuracy through aggregation and correlation of applicable external data sources or live data feeds (such as CMDB or host identification/monitoring solutions/agents).

3.1.4 Technology Assets Identification

All Process Owners[3] **must**:	
SAM-100	Ensure that the Information Systems supporting owned Processed are identified, with ownership assigned.
SAM-110	Oversee the accuracy of the information regarding the Information Systems in the Technology Asset Inventory.

Information System Owner **must**:	
SAM-115	Ensure that the ownership of underlying the Technology Infrastructure and Application components of the Information System is assigned.

Information System Owner and/or Technology Infrastructure Owner and/or Application Owner **must**:	
SAM-120	Ensure, that owned Technology Asset is onboarded to Technology Asset Management Process, in line with the Process level requirement (as communicated by [Technology Asset Management] PO) and corresponding (applicable) requirements of Configuration Management Process.
SAM-130	Maintain the completeness and accuracy of the Inventory records for owned Technology Asset by: 1) registering owned Assets, 2) ensuring that the Inventory records for the owned Assets are accurate and up to date and retain required level of details, as determined by the [Technology Asset Management] Process Owner 3) reporting to [Technology Asset Management] Process Owner Asset changes, applicable incidents, and issues, in line with operational requirements and approach predefined on Process level.

Information System Owner and/or Technology Infrastructure Owner **must**:	
SAM-140	Classify owned Technology Assets through impact assessment prior to any deployment works or agreements (including contractual agreements with 3rd parties) to ensure the security requirements are identified and considered in technical design prior implementation. *[Reference: Security BIA Methodology]* *Note: classification of Information Systems and Technology Infrastructure to be evaluated and maintained in line S-BIA assessment.*

[3] Process Owners for the various processes in the Bank, as defined in the Process Universe

3.1.5 ICS Requirements & Gaps Identification

Information System Owner and/or Technology Infrastructure Owner and/or Application Owner **must**:	
SAM-150	Ensure that ICS requirements are identified, deployed, and maintained in line with Security Configuration Management Standard.
SAM-160	Ensure that implementation of applicable ICS requirements is verified before the Asset is “approved for operation”.

Information System Owner and/or Technology Infrastructure Owner **must**:	
SAM-170	Identify and map Information Assets to be processed by owned Assets (including corresponding Critical Data Elements).
SAM-180	Acquire Information Asset Owner consent for scope, purpose, and context of Information Asset processing on owned Assets.

3.1.6 ICS Requirements in the Asset Lifecycle

Information System Owner and/or Technology Infrastructure Owner and/or Application Owner **must**	
SAM-190	Ensure that ICS requirements are reviewed in the case of change of a Technology Asset, its classification (impact assessment) or change of applicable ICS Standards.
SAM-200	If applicable, plan secure Asset decommission and ensure applicable security requirements are applied. *[Reference: Secure Decommissioning and Destruction Standard]*
SAM-210	Ensure that Asset maintenance, removal, transfers, and dispositions are planned, authorised, and logged.

Process Owner [Technology Asset Management] **must**:	
SAM-220	Provide governance for key Technology Asset management activities, such as transfers, removal, disposal, and maintenance.

3.1.7 Other Implementation Aspects

Technology Infrastructure Owner **must**:	
SAM-222	Ensure the required configuration and operations (as shared by Process Owners [Technology Asset Management, Configuration Management]) are deployed and maintained effectively for owned Technology Infrastructure to meet the Asset Management requirements
SAM-224	Allocate sufficient Technology Infrastructure capacity (storage and computing power) for asset management related configuration or services (in line with configuration guideline(s)).
SAM-226	Report to Process Owners [Technology Asset Management, Configuration Management] any issues or problems identified, that can impact hosts management capability.

3.2 Control Area: Information Assets

3.2.1 Process Definition, Delivery, Maintenance and Governance

Group CISO **must**:	
SAM-250	Establish a process for the identification, creation, and maintenance of Information Assets as part of the Bank's Information Asset Register.

Process Owner [Group CISO ICS Operations] **must**:	
SAM-260	Define, deploy, and maintain an operational Process (and related process controls) for Information Asset Management to ensure: 1) accountabilities of the Information Asset Owners can be fulfilled, 2) the Information Asset Register is accurate, up to date and complete (through process governance activities).
SAM-270	Define, implement, and maintain the Information Asset Register that: 1) records and retains required IA details (i.e., mandatory data elements as defined by the Information Asset Process Owner (Group CISO ICS Operations)), 2) supports key Information Asset management activities such as: a. registering, recertifying, and retiring (where appropriate) Information Assets, b. publishing the Information Asset Register, c. Information Asset related audits and reviews.
SAM-280	Review Information Asset record submissions by the IAOs for compliance with the registration process.
SAM-290	Define and manage an escalation process for overdue or non-compliant Information Asset records.
SAM-300	Provide training to Information Asset Owners on their roles and responsibilities for the Information Asset Registration and Assessment Process.

All Process Owners[4] **must**:	
SAM-310	Identify Information Assets created by their process and assign an Information Asset Owner for each Information Asset.

Information Asset Owner **must**:	
SAM-320	Define the acceptable use permissions for Information Asset(s) they own (including permissions for digital, physical, on-site and off-premise processing).
SAM-330	Ensure Information Assets are documented in the Information Asset Register as defined by ICS Operations: 1) recording all data required for the Information Asset Register in a timely manner, 2) Rate the owned Information Asset(s) in line with the Impact Assessment Methodology, 3) ensuring that the Register records for the owned Information Assets are accurate and up to date.

[4] Process Owners for the various processes in the Bank, as defined in the Process Universe

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 Leader 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

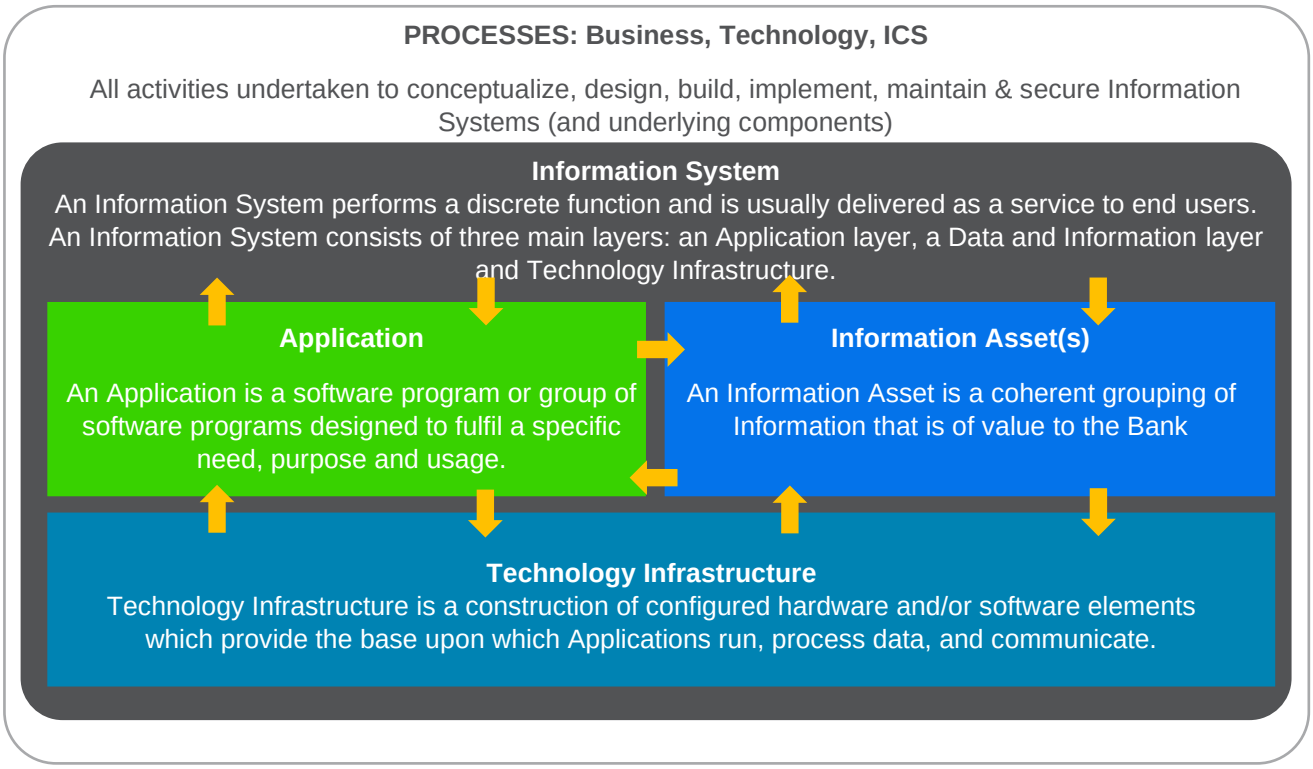
7.1 Technology Asset Inventory & CMDB – mandatory data elements

#	Attribute	Description	Data element in	
			ITAM	CMDB
1	ID	Unique identification code or number	x	x
2	Technology Asset Name	Short Name of the Technology Asset	x	x
3	Description	Additional Information regarding Technology Asset and its specifics	x	x
4	Category	Asset category/type	x	x
5	Impact rating/classification information	Information regarding impact rating (as assigned by the Technology Asset Owner)		x
6	Ownership Information	The Information regarding the Asset ownership: • Named individual, i.e., Asset Owner(s), as appointed by PUO/PO Ownership concept is fundamental for ICS approach effectiveness as ensures the accountability for respective actions is determined.	x	x
7	Lifecycle stage	Information tag defining current lifecycle stage of the Asset	x	x
8	Status	Status of the Asset	x	x
9	Relevant vendor/technology information	Required technology or vendor references as defined per Asset category		x
10	IP address	N/A		x
11	Location & hosting model	Asset location and if applicable, information regarding the hosting model	x	
12	IT Asset tag number	Tag assigned in line with the Process level definition and catalogue	x	
13	MAC address	N/A		x
14	Hostname	N/A		x
15	Operating system (if applicable)	N/A		x
16	Licensing information (if applicable)	Information regarding applicable and acquired licenses, such as license type, due date, etc.	x	
17	Configuration baseline	(if applicable) configuration baseline/template applied		x
18	Last patch date	The date of last patching activity successfully executed		x

#	Attribute	Description	Data element in	
			ITAM	CMDB
19	Technology Vulnerabilities identified	Information regarding technology vulnerabilities identified for the Asset		x
20	Maintenance frequency	Predefined maintenance schedule for the Technology Asset		x
21	Architecture	Key information regarding the IT architecture, such as internet facing, externally connected, cloud, etc.		x
22	Dependent Information Systems	Indication of key Technology Asset interdependencies		x

7.2 ICS Taxonomy for Assets

7.2.1 The taxonomy and naming convention used in the ICS Policy and Standards



7.2.2 ICS and Technology Terminology References

The key terms and taxonomy, which the Methodology refers to, is aligned with the ICS and Technology Glossaries. The Technology references to ICS key terms are outlined in the table below:

#	Def type	ICS Term	T&O reference	Additional comments
1	Asset	**Information System**	**Business Application**/Application Service [-> Technology Service]	Information System maps directly to Business Application, but can be indirectly referred to Technology Service Business Application and Information System as defined in the ICS & Technology Glossary

#	Def type	ICS Term	T&O reference	Additional comments
2	Asset	**Information System Instance**	**Application Service** [-> Technology Service]	IS instance maps to Application service, but indirectly can be also referred as a type of Technology Service Application Service and Instance as defined in the ICS & Technology Glossary
3	Asset	**Technology Infrastructure**	**Technical Service**, Technology Infrastructure	Technical Service and Technology Infrastructure as defined in the ICS & Technology Glossary
4	Asset	**Application**	**Application**	Application as defined in the ICS & Technology Glossary

The ICS & Technology glossary of terms – for the terms outlined above the ICS & Technology Glossary and the Group Role Library shall be checked.

Appendix A – Version Control Table

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISRO ICS Policy	First release (inclusive terminology & ICSCR-25Nov2021-1 considered)	Material	Samantha Finan, Global Head, ICS Policy, Standards and Reporting	1.0	22-Jun-22	01-Jul-22
CISRO ICS Policy	Administrative and editorial changes: 1. Document template updated in line with the Template for Group Standards, v5.6 2. The Standard name updated from 'Group Information and Cyber Security Standard: Secure Asset Management' to 'ICS Secure Asset Management Standard' 3. SAM-230, SAM-232, SAM-234 and SAM-236 (All Staff relevant) removed in line with the ICSCR-18Feb2022-1 (introduction of the AUS)	Non-material	Paul Hoare Head, ICS Policy and Best Practice	1.1	28-Sep-23	11-Oct-23

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	Incorrect references updated					
Katarzyna Wencka **[ICS Standards]**	Administrative changes introduced to update document template, references, roles and ownership.	Non-material	Jamie Cowan Head, ICS Risk Framework & Governance	1.2	04-Dec-24	16-Dec-24