# Security Logging and Monitoring

| | |
|---|---|
| **Version No** | 4.3 |
| **Document Type** | Standard |
| **Parent Document** | Group Information and Cyber Security Policy |
| **Parent Framework** | Information and Cyber Security |
| **Document Approver Name** | Jamie Michael Cowan |
| **Document Approver Job Title** | Head, Frameworks, Reporting & Governance, T&O Risk & Control |
| **Document Owner Name** | Ibrahim Gathungu Munyori |
| **Document Owner Job Title** | Director, ICS Standards Formulation |
| **Document Contact Name** | Arti Singh |
| **Document Contact Job Title** | Assoc Dir, ICS Standards |
| **Business Scope** | All Businesses |
| **Function Role** | All Functions |
| **Geography Scope** | GLOBAL |
| **Approval Date** | 29/01/2025 |
| **Effective Date** | 16/03/2025 |
| **Next Review Date** | 13/09/2027 |

## Table of Contents

## Version Control Table

| Name | Changes made | Materiality | Approved by | Version number | Approval Date | Effective Date |
|---|---|---|---|---|---|---|
| Arti Singh | Security Logging and Monitoring | Non-Material | Jamie Michael Cowan | 4.3 | 29/01/2025 | 16/03/2025 |

The full version history is included at the end of the document.

# 1. INTRODUCTION AND SCOPE

Secure logging and monitoring establish systematically capturing, storing, and analysing relevant security event data from various IT systems, networks, and devices. The outcome is to enhance the security posture of an organization by providing real-time visibility into potential threats, detecting security incidents, and facilitating effective incident response.

This Information Security Standard will define the minimum set of requirements for:

a) Group-wide approach to security logging and monitoring for Information Systems and Technology Infrastructure.

b) Required baseline configuration of Information Systems (including Application and Technology Infrastructure Components) to support Group ICS logging and monitoring capabilities and objectives.

c) Enhanced ICS logging and monitoring requirements for mission-critical IT Assets, i.e. Information Systems and Technology Infrastructure of certain importance to Groups operations and processes;

d) The importance of threat intelligence in the light of ICS logging and monitoring approach.

## 1.1. RISKS

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 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. Policy Non-Compliance].

Legal and regulatory provisions require that systems do a minimum level of logging.

***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 including components managed or hosted by Third Parties:

1) which are impact rated L4 or L5[1],

2) where potential impact propagation could arise in the case of the security breach (i.e. the Asset is rated <L4, but impact propagation can lead to L4 or L5 impact)

3) where identified threat profile may expose the Asset to increased risk of ICS incidents or result in L4-L5 impact propagation.

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].

[1] L1-L5 impact rating refers to S-BIA rating of Level 1 to 5 throughout the document

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, Security Incident Response and Management and Secure Configuration Management as well as Technology Events Management Standard.

## 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 logging and monitoring solutions cannot be deployed due to tangible process or technology limitations specific for some hosting models (for example for Information systems delivered in SaaS which are off premise), equivalent contractual controls must be in place to ensure the controls objectives are met.

## 2. ROLE AND RESPONSIBILTIES

**Information Asset / System Owner [includes Owner of underlying Application(s)/Product and Technology Infrastructure]**

The Information Asset/System Owner is accountable for the protection of their Information Assets and Information Systems and with complying to the Control Statements applicable to them.They are also responsible for ensuring that the Application and Technology Infrastructure Owners correctly apply the controls as set out in this standard.

As first line role holders they must have in place a model for validation of control existence and effectiveness.

**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.

**Application Owner**

Application Owners are responsible for complying with the control areas of this Information Security Standard which are applicable to them to ensure that logging and monitoring requirements are embedded or configured on the Application level (when applicable and required).

**Process Owner [SLM Process / Group Threat Management Process]**

As defined in Enterprise Risk Management Framework [ERMF] and appointed by Group CISO, in line with applicable requirements of ICS Standards.

**CISO ICS Standards and Controls**

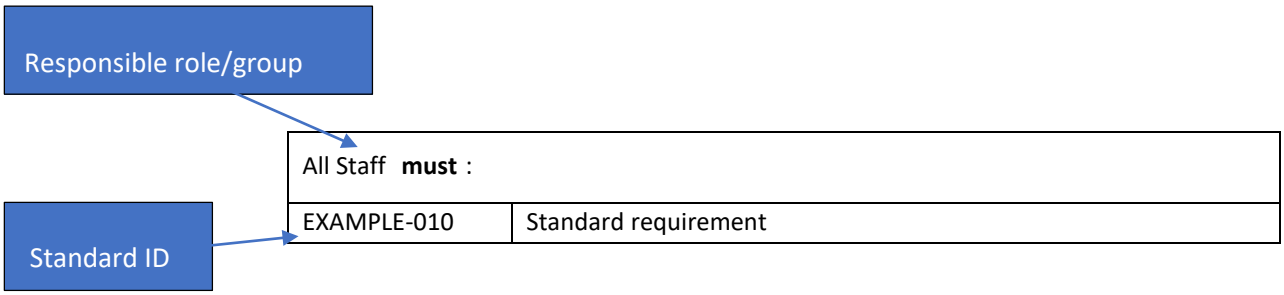
The CISO is the owner of this Security Standard and will ensure the document is updated to an agreed schedule.

***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- Operational Approach Definition and Maintenance

### 3.1.1 Process definition and governance

| Process Owner [SLM Process] **must**: | |
|---|---|
| SLM-002<br>[Prev.SLM003] | Define an operational approach to ICS logging and monitoring by:<br>a) Defining BAU and operational process procedures to ensure the controls of the Standards are met.<br>b) Defining the scope of the technologies covered<br>c) Defining the scope of the logging and monitoring activities in line with:<br>(i) the baseline requirements of the Standard; and<br>(ii) risk-based (threat-led approach) - Considering criticality of the asset monitored and applicable risk/ threat factors<br>d) Determining operational requirements and procedures for Information System/Technology Infrastructure/Application Owners, essential to ensure predefined compliance level (with the Standard requirements).<br><br>*[Reference: Appendix: ICS threat and risk factors – example recommendations]*<br>*[Objective: SLM is delivered and executed in a defined, consistent and effective manner to enhance the organization's ability to detect and respond to security threats effectively]* |

### 3.1.2 Operational capability delivery

| Process Owner [SLM Process] **must**: | |
|---|---|
| SLM-006 | Deliver operational capacity to ensure that: |
| [Prev SLM-009] | a) Security Event logs are recorded, available when required and retained to meet the regulatory and Group's data retention requirements<br>b) The Information Systems (and underlying Technology Infrastructure) scoped can be covered by (central) logging and monitoring capabilities in line with pre-defined objectives (scope, accuracy, completeness, data quality, alert timing, etc).<br>c) Security Event logs are received from the IT Assets in scope in a timely manner.<br>d) The security event logs received are complete and protected from unauthorised alteration and disclosure to unauthorised personnel.<br>e) Required retention is ensured and security event logs are destroyed securely when no longer required.<br>f) Identification of data quality problems or Information gaps and reporting them to responsible stakeholders.<br>g) Effective response procedures to address identified issues are established and executed.<br>Note: The operational approach supports required flexibility that can meet increased logging and monitoring requirements (due to the scope or approach change, new technologies acquired, etc).<br>*[Reference: Group Records Keeping Standard]*<br>*[Objective:*<br>1.) *SLM is delivered and executed in a defined, consistent and effective manner.*<br>2.) *Ensure timely, complete and accurate recording of security event logs and audit records; maintaining required retention and disposal securely]* |

## 3.2. Control Area- Security Event Logging

### 3.2.1 General Logging Requirements

| Process Owner [SLM Process] **must**: | |
|---|---|
| SLM-007a | Deliver and maintain operational and configuration guidelines for technology and products used in the Bank in the scope and context of the SLM Process.<br>*[Objective: SLM is delivered and executed in a defined, consistent and effective manner]* |
| SLM-007b | Ensure that the guidelines:<br>a) consume baseline logging requirements of the Standard (see the Appendix section);<br>b) include (optional) enhanced logging requirements (together with the guideline for their applicability);<br>c) do not interfere with the monitored hosts operational capacity.<br>d) are aligned with vendor specification and recommendations.<br>e) are embedded in the standard technology build (if feasible);<br>f) include required network/communication configuration and compatibility list/issues, required local log retention and data and reconciliation schedules;<br>g) are tested before communicated for deployment.<br>In addition to the above technical or operational procedures must be shared to ensure maintenance and oversights over required configuration for events logging<br>*[Reference: Group Records Keeping Standard]*<br>*[Objective: SLM is delivered and executed in a defined, consistent and effective manner]* |
| SLM-007a | Deliver and maintain operational and configuration guidelines for technology and products used in the Bank in the scope and context of the SLM Process.<br>*[Objective: SLM is delivered and executed in a defined, consistent and effective manner]* |
| SLM-008<br>[Prev SLM-008b] | Support identification and definition of enhanced logging requirements across different levels of Information System and Technology Infrastructure components (such as OS, network, data, application) (if required) based on:<br>a) criticality of the IT Assets (CIA impact rating as defined through the S-BIA) and the Standard requirements (see Appendix section);<br>b) ICS risk exposure of respective technologies and architecture<br>c) Specific business or technology context of Information System (or Technology Infrastructure) operations.<br>*Note: Enhanced logging requirements can also be formulated by certain scope expansion (to include specific technology, type of IT Assets or level of logging – OS, application, network, data, etc.).*<br>*[Objective: To ensure that process owners are aware of any specific / additional logging needs and necessary arrangements can be made to meet those requirements.]* |

| Information System Owner **must**: | |
|---|---|
| SLM-010 [Prev SLM-011; SLM - 020; SLM-021] | Ensure security event logging requirements are:<br>a) Supported and incorporated at the early design for Information Systems (and Application and Technology Infrastructure) in line with the configuration guidelines provided by Process Owner.<br>b) enabled by the Technology Infrastructure Owners for the Information Systems (and underlying Technology Infrastructure) in line with the Process configuration guidelines.<br>c) Identified and inform Process Owner about additional or enhanced logging requirements specific owned Information System (due to business or regulatory context).<br>*[Reference: Appendix: Security Event Logging Baseline Requirements for Consideration]*<br>*[Objective: To ensure compliance with configuration guidelines and proactive threat detection capabilities.]* |

| Technology Infrastructure Owner **must**: | |
|---|---|
| SLM-030 | Ensure the required configuration and operations (as shared by Process Owner) are deployed and maintained effectively for owned Technology Infrastructure to meet the logging requirements.<br>*[Objective: To ensure compliance with logging requirements and robust security.]* |
| SLM-040 | Allocate sufficient Technology Infrastructure capacity (storage and computing power) for auditing and storing security event log records locally (in line with Process Owner configuration guideline).<br>*[Objective:*<br>1.) *To reduce the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of audit logging capability as well as negative impact to the host operations.]*<br>2.) *Security logging and monitoring do not impact Technology Asset operations. Security event logs (from Technology Assets) are complete and consistent to ensure effective audit tail and monitoring activities.]* |
| SLM-041 | Technology and products onboarded provides required ability to ensure compliance with Group's approach to logging and monitoring (non-functional requirements)<br>*[Objective: To ensure compliance with logging requirements.]* |

| Application Owner **must**: | |
|---|---|
| SLM-080 | Ensure the required configuration and operations (as shared by Process Owner) are embedded, deployed, and maintained effectively on the Application level to meet the logging requirements.<br>*[Objective: Effective implementation and maintenance of required logging configurations and operations within applications, contributing to comprehensive threat detection and incident response capabilities.]* |

| Application Owner/Technology Infrastructure Owner **must:** | |
|---|---|
| SLM-088<br>[Prev SLM-070] | Ensure the security event logs do not contain Information Assets rated as 5 or 4 in clear text.<br>For Example: Passwords, PINs, Customer Personal Information or Card Information.<br>*[Reference: Information Asset Methodology]*<br>*[Reference: Information Classification Standard]*<br>*[Objective: Protect sensitive Information from unauthorized disclosure stored or transmitted insecurely within security event logs mitigating the risk of data breaches and ensuring compliance with relevant regulations.]* |
| SLM-042<br>[Prev. SLM 086] | Inform Process Owner about specific logging requirement for the owned Technology Infrastructure / Application (if any).<br>*[Objective: Proactively identify and communicate specific logging needs for owned Information Systems, ensuring comprehensive threat detection and regulatory compliance.]* |
| SLM-050<br>[Prev. SLM – 087] | Report to Process Owner any issues or problem identified that can impact hosts / Application logging capability.<br>*[Objective: Ensure reporting of the host noncompliance so that it can be mitigated.]* |

### 3.2.2 Activities to be Logged and Elements of Log

| Process Owner [SLM Process] **must**: | |
|---|---|
| SLM-090 | Ensure the security event logs are received, processed securely and available in the Groups central log repository for Information Systems and Technology Infrastructure in scope of central log storage.<br>*[Objective: To have the comprehensive record of security related events across the systems to facilitate identification of suspicious activity and investigate the potential incidents.]* |
| SLM-100 | Ensure that respective configuration guidelines are reviewed and updated to ensure the logging requirements of the Standards are met.<br>*[Objective: Maintain accurate and verifiable audit trails for all security events by ensuring configuration guidelines and event log attributes comply with the Standards.]* |
| SLM-110 | Define the necessary attributes to be captured for all security event types / security logs and ensure that at minimum (where technically feasible) attributes below are captured: |

| Process Owner [SLM Process] **must**: | |
|---|---|
| [Prev SLM-100] | a) Event type and ID<br>b) Event source;<br>c) User Identifier<br>d) Date and time stamp;<br>e) Host Identifier<br>f) Event description;<br>g) Event severity;<br>h) Task category;<br>i) Log type/name.<br>*[Objective: Capture essential event data for ensuring that activity can be attributed to a specific source, user and date / time enabling comprehensive security analysis and incident response.]* |

| Application Owner **must**: | |
|---|---|
| SLM-111 | Ensure that application audit meets the requirements defined by the Standard (i.e. event types and attributes) and supports operational and technology requirements are defined by Process Owner.<br>*[Objective: Compliance with standard requirements and the operational and technology needs defined by the Process Owner.]* |

| Information Asset Owner **must**: | |
|---|---|
| SLM-112 | Communicate specific logging requirements for the Information Assets use to Information System Owners (so these can be embedded, if required, in overall configuration guidelines).<br>*[Objective: Ensure that Information System Owners are aware and understand the specific logging requirement for Information Assets under their remit so that they can be embedded into overall configuration guidelines.]* |

### 3.2.3 Protection of Log Information

| Process Owner [SLM Process] **must**: | |
|---|---|
| SLM-120 | Ensure all security event logs processed in a centralised log management solution are protected against unauthorised access, deletion, or modification.<br>*[Objective: Ensure the integrity and confidentiality of all security event logs processed.]* |
| SLM-130 | Ensure archived logs are protected from deliberate or accidental tampering.<br>*NOTE: The appropriate media formats for storing the logs must also be defined and periodically reviewed.*<br>*[Objective: Ensure the integrity and confidentiality of all security event logs processed.]*<br>*[To support full restoration during investigation and monitoring.]* |
| SLM-140 | Ensure additional data privacy related logging controls are implemented on Information Systems which store, process or access customer or personal Information.<br>*[Reference: Group Privacy Standard]*<br>*[Objective: Enhance data privacy protection by implementing additional data privacy-related logging controls on Information Systems (IS) that store, process, or access customer or personal information, exceeding the baseline security requirements and aligning with data privacy regulations.]* |

| Process Owner [SLM Process] **must**: | |
|---|---|
| SLM-150 | Document and maintain the following systems and infrastructure in scope of central log storage:<br>a) Privileges for accessing logs;<br>b) Process for enabling and configuring logs;<br>c) Process for maintaining continuity of logging services.<br>*[Objective:*<br>1. *To ensure only authorized individuals have access reducing risk of unauthorized access, modification or disclosure.]*<br>2. *Logging is consistently enabled and configured for all systems]*<br>3. *Logging services remain operational and available in event of any system failure, outages or disruptions.]* |
| SLM-170 | Log, monitor and review any changes to time settings on systems and infrastructure in scope of central log storage.<br>*[Objective: Ensure accurate and reliable timekeeping across all systems and preventing unauthorized manipulation.]* |

| Technology Infrastructure Owner **must**: | |
|---|---|
| SLM-171 | Ensure all security event logs processed locally are protected against unauthorised access, deletion, or modification.<br>*[Objective: Ensure the integrity and confidentiality of all security event logs.]* |
| SLM-173 | Log, monitor and review any changes to time settings and logging configuration on owned Technology Infrastructure.<br>*[Objective: Maintain the integrity and reliability of timekeeping and logging across owned technology infrastructure ensuring timely detection and investigation of potential unauthorized modifications and preventing disruptions.]* |

## 3.3. Control Area- Security Event Monitoring

### 3.3.1 Monitoring Requirements

| Process Owner [SLM Process] **must**: | |
|---|---|
| SLM-180 | Ensure security event monitoring is in place for the Information Systems and Technology Infrastructure:<br>a) In line with the baseline requirements of the Standard (see Appendix section 7.3 Security Monitoring – Baseline Requirements);<br>b) Aligned with the threat intelligence and threat-profiles of the monitored hosts;<br>c) Effectively supporting identification of ICS events and incidents that can impact the security of the monitored environment;<br>d) Accommodating specific monitoring requirements reported by Information System Owners;<br>e) Generating alerts and notifications in the case of ICS events or incident identification.<br>*[Objective: Implement a comprehensive security event monitoring system for all Information Systems (IS) and Technology Infrastructure (TI) within the organization, ensuring robust threat detection, incident response, and regulatory compliance.]* |

| Process Owner [SLM Process] **must**: | |
|---|---|
| SLM-200 | Communicate any local monitoring requirements that must be executed by Information System or Technology Infrastructure Owners to support the Group approach to ICS monitoring.<br>*[Objective: Ensuring their collaboration and contribution to a unified approach to ICS monitoring, significantly enhancing the Group's overall security posture.]* |

| Information System Owner and/or Technology Infrastructure Owner **must**: | |
|---|---|
| SLM-210 | Ensure that required local monitoring activities are performed and aligned with Process Owner defined requirements.<br>*[Objective: Establish and ensure the consistent execution of required local monitoring activities within Information Systems (IS) and Technology Infrastructure (TI), aligning them with Process Owner defined requirements.]* |
| SLM-220 | Report any ICS events or incidents identified as a result of the local monitoring to the Process Owner.<br>*[Objective: Enabling timely detection, analysis, and response to potential security threats.]* |

### 3.3.2 Independent Review of Logs

| Process Owner [SLM Process] **must**: | |
|---|---|
| SLM-230 | Ensure security event logs from all systems and infrastructure in scope of central log storage are received by the monitoring resources near real-time monitoring.<br>*Note: Real-time monitoring and alerting capabilities must be enabled to provide visibility of the usage and performance of Application Program Interfaces [API] and detect suspicious activities.*<br>*[Objective: Enabling timely detection, analysis, and response to potential security threats.]* |
| SLM-240 | Ensure the security event logs and reports are examined in a timely manner appropriate to the criticality of the events and alerts received from the monitoring solution.<br>*[Reference: Security Incident and Response Management Standard]*<br>*[Objective: Establish and implement a timely and prioritized approach to examining security event logs and reports based on their criticality and the severity of alerts received from the monitoring solution, enabling rapid detection, investigation, and response to potential threats.]* |
| SLM-250 | Ensure security event monitoring operations are established and documented which at minimum covers the following:<br>a) Monitoring scope and prerequisites.<br>b) Tools used for monitoring and correlation.<br>c) Security events covered.<br>d) Frequency of monitoring.<br>e) Clearly defined roles and responsibilities.<br>f) Escalation matrix.<br>*[Objective: Establish and maintain comprehensive and documented security event monitoring operations ensuring efficient detection, analysis, and response to potential threats.]* |
| SLM-261 | Ensure that logs and metadata required are made available for target reviews such as digital investigation purposes, incident management, etc. to authorised personnel.<br>*[Reference SIR-100]*<br>*[Objective: Establish and maintain a secure and controlled process for providing* |

| Process Owner [SLM Process] **must**: | |
|---|---|
| | *authorized personnel with access to required logs and metadata for legitimate purposes, such as digital investigations, incident management, and security analysis, while safeguarding sensitive information and ensuring data privacy compliance.]* |

## 3.4. Control Area- Threat Intelligence Management

### 3.4.1 General Provision

| Process Owner [Group Threat Management] **must**: | |
|---|---|
| *SLM-310* | Ensure that the operational approach is delivered through documented process for the end-to-end Cyber Threat Intelligence (CTI) lifecycle, that:<br>a) Includes threat intelligence collection and information sharing goals and objectives, that support business processes and security policies,<br>b) identifies and establishes the criteria for evaluating and selecting the relevant threat intelligence sources:<br>I. based on credibility, accuracy, and timeliness,<br>II. mapped to intelligence requirements of internal stakeholders and intelligence consumers,<br>III. considering multiple internal and external sources<br>c) specifies the scope of threat intelligence production activities such as a,<br>I. information collection rules/methods,<br>II. participating in information sharing efforts<br>III. defining the final Threat Intelligence products<br>IV. frequency of their delivery<br>V. intended recipients and use<br>VI. the scope and content of the threat intelligence included in the Threat Intelligence products<br>VII. proactive agreements for threat information sharing<br>VIII. providing ongoing support for information sharing activities<br>d) define the approach for threat information analysis, enrichment and normalization to ensure accurate, consistent and comprehensive intelligence is produced and delivered (to intended stakeholders)<br>e) uses secure workflows and centralized approach to collect, process, analyse , maintain and disseminate cyber threat intelligence,<br>f) ensures clear, concise and timely threat intelligence communication.<br>g) defines the acceptable use and handling requirements for Threat Intelligence being shared.<br>*[Objective:*<br>1. *Uniformity of the ICS risk management is supported by consistent, accurate and consolidated ICS threat information.*<br>2. *ICS threat related information is acquired from authorized, unified, and uniform sources to ensure that ICS risk assessment and management activities are conducted in a consistent and comprehensive manner.*<br>3. *The Threat intelligence program is tailored to specific ICS threat landscape and relevant threats faced by Group.]* |
| SLM-350 | Deliver operational capability (together with required resources, such as tooling, |

| Process Owner [Group Threat Management] **must**: | |
|---|---|
| | staff, operational procedure to support the Threat Intelligence Management Process approach, strategy and objectives (as defined in SLM-310).<br>*[Reference: SLM-310]*<br>*[Objective:*<br>1. *ICS threat related information is acquired from authorized, unified and uniform sources to ensure that ICS risk assessment and management activities are conducted in a consistent and comprehensive manner.*<br>2. *Threat Intelligence is delivered and executed in a defined, timely, consistent and effective manner enhancing the organization's resilience against potential threats.*<br>3. *Relevant resources are present to ensure continuous, consistent and effective delivery of the Threat Intelligence management process.]* |
| SLM-360 | Establish an operational approach to Threat Intelligence based on:<br>a) current ICS Threat Landscape,<br>b) Group ICS footprint and its exposure to the ICS threats (due to technology, business, geo-presence, risks present, etc.)<br>c) identified and applicable threat intelligence information sources.<br>*[Objective:*<br>1.) *ICS threat related information is acquired from authorized, unified and uniform sources to ensure that ICS risk assessment and management activities are conducted in a consistent and comprehensive manner.*<br>2.) *The Threat intelligence program is tailored to specific ICS threat landscape and relevant threats faced by Group.]* |

### 3.4.2 Threat Intelligence Collection and Acquisition

| Process Owner [Group Threat Management] **must**: | |
|---|---|
| (New) SLM-375 | Ensure that Threat Intelligence information is acquired without undue delay from authorized and validated sources, as defined in SLM-310.<br>*[Objective: ICS risk management efforts are timely supported with a reliable and adequate threat intelligence.]* |
| SLM-380 | Ensure that Intelligence Collection process identifies threat events likely to be used to attack the Group (i.e., the methods and techniques used by attackers to perform reconnaissance, gain access, maintain control, compromise information and exploit information).<br>*[Objective:*<br>1.) *ICS threat related information is acquired from authorized, unified and uniform sources to ensure that ICS risk assessment and management activities are conducted in a consistent and comprehensive manner.*<br>2.) *The Threat intelligence program is tailored to specific ICS threat landscape and relevant threats faced by Group.]* |

### 3.4.3 Threat Intelligence Processing and Analysis

| Process Owner [Group Threat Management] **must**: | |
|---|---|
| (New) SLM-385 | Develop and maintain a taxonomy for classifying, prioritizing, and organizing threat intelligence data for effective analysis and correlation.<br>*[Objective:*<br>1.) *Threat Intelligence information is consistent, uniform and with predefined structure, granularity and taxonomy that categorizes threat intelligence data based on relevant attributes including threat type, actor, TTP's and IOC's.*<br>2.) *ICS threats are classified and prioritized to ensure the most critical ICS risk can be managed first.]* |

| Process Owner [Group Threat Management] **must**: | |
|---|---|
| SLM-390 | Ensure that the Analysis process of threat information examines relevant information or intelligence using reasoning, analytical techniques and considers the following:<br>a) emerging and changing threat techniques and methods used against the Group,<br>b) different types of threat events associated with threats to the Group,<br>c) details about past, present and predicted attacks,<br>d) information security incidents experienced by other organizations (including types of incidents and origin of the attack, preceding threat events, frequency of occurrence and resulting business impact),<br>e) impact being experienced by similar organizations,<br>f) defined intelligence requirements.<br>*[Objective:*<br>1. *ICS threat related information is acquired from authorized, unified and uniform sources to ensure that ICS risk assessment and management activities are conducted in a consistent and comprehensive manner.*<br>2. *The Threat intelligence program is tailored to specific ICS threat landscape and relevant threats faced by Group.]* |
| (New) SLM - 386 | Prioritize threats based on threat intelligence collected in line with the Group exposure to applicable threats and corresponding risks, i.e.: based on:<br>1) threat severity,<br>2) likelihood of the threat materialization (due to specific vulnerability presence),<br>3) criticality of the Technology Assets potentially impacted.<br>*[Objective:*<br>1. *Prioritize Threat Intelligence data to ensure that most critical threats are addressed first.*<br>2. *The Threat intelligence program is tailored to specific ICS threat landscape and relevant threats faced by Group.]* |

### 3.4.4 Threat Intelligence Dissemination and Sharing

| Process Owner [Group Threat Management] **must**: | |
|---|---|
| (New) SLM - 387 | Implement a secure and controlled mechanisms for sharing threat intelligence with external partners and within the organization.<br>*[Objective: To establish a secure and controlled way of sharing Threat Intelligence with external partners and within the organization to ensure that the Information is shared securely, and without violation of any data privacy laws or regulations, or any internal data protection policies.]* |
| SLM-400 | Ensure that, finished Intelligence product:<br>a) is shared with relevant stakeholders in a timely manner and, if feasible, provides an early warning system to identify threat that are likely to target the Group,<br>b) determines the motivation, capabilities, and commitment of identified threats,<br>c) determines the prevalence of threat events used at different stages of the cyberattack chain,<br>d) identifies techniques used by attackers to maintain control of compromised systems and conceal their activity.<br>e) is:<br>• relevant, related to the protection of the Group's assets,<br>• insightful, so the Group is provided with an accurate and detailed understanding of the threat landscape,<br>• contextual, to provide situational awareness,<br>• actionable, so the Group can act on information quickly and effectively.<br>*[Objective: Collaborate and cooperate closely with relevant stakeholders timely in combating cyber threats and sharing of threat intelligence so that the mitigating measure can be determined.]* |

| Information System Owner / Application Owner/ Technology Infrastructure Owner **must:** | |
|---|---|
| (New) SLM-389 | Ensure that threat detection, analysis and mitigation activities rely on the Group Threat Management products as the primary source for consuming threat information.<br>*[Objective: To ensure that all relevant stakeholders consuming the threat information have access to single reliable and trusted source to promote consistency in threat detection, analysis and mitigation measures to be determined.]* |

### 3.4.5 Threat Intelligence Monitoring and Update

| Process Owner [Group Threat Management] **must**: | |
|---|---|
| (New) SLM-391 | Establish a continuous monitoring process to track the evolution of threat intelligence, ensuring its relevance and timeliness.<br>*[Objective: To establish a robust and continuous monitoring process to track the threat landscape ensuring its relevance, timeliness and accuracy to make well informed decision and mitigate emerging threats.]* |
| (New) SLM-392 | Regularly update threat intelligence products and library based on new threats, vulnerabilities, changes in the Group ICS footprint, lesson learnt from incidents and emerging security trends.<br>*[Objective: To maintain a comprehensive and up to date Threat Intelligence repository by regularly incorporating new threat data, vulnerability assessments and emerging security trends, ensuring the organization's defence remain effective against evolving threats.]* |

### 3.4.6 Threat Intelligence Compliance and Audit

| Process Owner [Group Threat Management] **must**: | |
|---|---|
| SLM-410 | Review the method or process of Threat Intelligence on regular basis to:<br>a) improve the effectiveness of Group's Threat Intelligence lifecycle,<br>b) measure and assess the extent to which the intelligence is delivering value in informing decisions and actions,<br>c) obtain feedback about the value of the threat intelligence and the effectiveness of the Group's threat intelligence capability.<br>*[Objective: The Threat Intelligence process shall be reviewed and assessed ensuring their relevance and effectiveness, to uphold a proactive and adaptive security posture against evolving threats.]* |

# 4. INFORMATION AND 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 OR INDUSTRY REFERENCES

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

## 7. APPENDIX

### 7.1. ICS threat and risk factors - example recommendations

Risk-based approach to determining the scope and approach to security logging and monitoring, should at least consider:

1) Threat modelling for standalone threat factors:
   a) external connectivity;
   b) hosting location and delivery model;
   c) development model (in-house/of the shelf);
   d) core/non-core data processing;
   e) 3rd party maintenance model.
2) Granular approach to impact factors, i.e. threats/risk mapping to particular CIA aspects of key importance and expected impact:
   a) Confidentiality - > for example: data leakage, information disclosure;
   b) Integrity - > for example: tampering, loss of funds;
   c) Availability - > loss of service, denial of service.
3) Threat identification and mapping to particular IT Assets attributes/function and attack vectors to allow more effective and tailored approach to issues and incidents detection or prevention, for example:
   a) End user infrastructure - > increased likeliness of malware infection;
   b) Active directory (or other authentication and authorisation services) - > data tampering, privileges escalation;
   c) Databases - > data infiltration, data mining.

### 7.2. Security Event Logging Baseline Requirements for Consideration

| Domain/Group | Activity |
|---|---|
| Standard/Host operations | Changes (or attempt to change) to key system/application objects and variables/parameters/resources (ex. Configuration files, Windows registry, system processes and services, access mgmt., crypto key stores and keys, system utilities) |
| | changes to key system components, such as services, installed software/libraries |
| | local network configuration changes including local firewall, if applicable |
| | changes to the host network services |

| Domain/Group | Activity |
|---|---|
| | use of external data media |
| User activities | successful logon/logoff |
| | unsuccessful access attempts (authentication and authorisation) |
| | user activities against key system or network resources |
| | user authorisation |
| | use/attempts to use of privileged ID |
| | user session (including changes) |
| | use and activities performed using generic or service accounts |
| Critical data activities (i.e. representing L4 and L5 Information Assets) | access to critical data (for example in databases, network drives etc.) |
| | modification or attempts to modify critical data |
| | removal/deletion of critical data |
| | downloading/uploading activities re. the critical data |
| | sending/sharing the data using standard and non-standard communication channels and media |
| network/network components | management access to network components (including access attempts) |
| | requests and connection attempts |
| | configuration changes to network devices |
| | mission critical servers and their web/network interfaces (changes to key components, requests served and rejected) |
| Threat/compromise indicators | all activities that can indicate ICS threat materialisation (based on the threat intelligence; vital to enable threat-led monitoring activities) |
| | attempts to vulnerability exploitation (based on the threat intelligence; vital to enable threat-led monitoring activities) |
| | IoCs (where applicable, i.e. activities for IoC creation can be logged) |

## 7.3. Security Monitoring - Baseline Requirements for Consideration

| Domain | Monitoring activity |
|---|---|
| Host monitoring | unusual or non-standard system/user activities, such as modification (or attempt to modify) of key system parameters, resources or objects (for example – configuration files, system utilities, system variables, crypto keys/stores, other system configuration objects) |
| Host monitoring | changes to key host services or processes |
| User activity anomalies | user activity anomalies (such as non-standard hrs activity, multiple user sessions sharing the same ID, logon attempts to disabled or terminated accounts) |
| User activity anomalies | critical data manipulation or access (such as multiple requests from a single source or multiple requests from various sources) |
| Privileged user activity | User activity performed using privileged user IDs or context |
| Data monitoring | data/communication channels use |
| Data monitoring<br>User activity anomalies | attempts or successful use of non-standard communication channels (to infiltrate or send data) |

| Domain | Monitoring activity |
|---|---|
| User activity anomalies | active use of default/generic accounts from non-standard sources |
| Data monitoring | use of external data media |
| User activity anomalies | non-standard use of user accounts |
| Host monitoring | changes (or attempts) to modify the configuration of access management mechanisms |
| User activity anomalies | vendor/3rd party access, activities or unsuccessful access/operations attempts |
| Network monitoring | network traffic patterns indicating/matching known attack vectors and indicators |
| Network monitoring | anomalies in the network traffic which do not match patterns of the Bank operations (such as unexpected, direct or indirect connections/traffic between network segments) |
| Network monitoring | network services that do not match the authorized services list or types |
| Network monitoring | unusual network requests served or rejected by mission-critical network services (such as network gateways servers, proxies) |
| Network monitoring | abnormal requests or operations requested from web-based systems (including the ecommerce, e-banking, etc) |
| Host monitoring<br>Network monitoring | identification of IoC or behavioural patterns matching known attack vectors (based on internal/external Threat-Intelligence |
| Host monitoring | manipulation of configuration or operations of security components of hosts (such as AV/DLP agents) |

Note : *The baseline requirement(s) are defined in line with the industry best practices and regulatory guidelines to ensure secure logging and monitoring. The recommended baseline outlines the key factors that the Secure Logging and Monitoring Strategy and approach must consider and embed where/when relevant. It is acceptable that specific factors or recommendations are not implemented (or implemented on specific assets or partially implemented) if recognised as not relevant to the current IT environment or threat exposure.

## 8. Appendix A - Version Control Table

| Name | Changes made | Materiality | Approved by | Version number | Approval Date | Effective Date |
|---|---|---|---|---|---|---|
| **CISRO ICS Policy** | Annual review includes:<br>1. Migrated existing standard to ERM standard template.<br>2. The existing Security Logging and Monitoring Standard document has been uplifted into this standard.<br>3. Consultation feedback, corrections incorporated | - | Liz Banbury | 1.0 | 30-Sep-19 | 30-Sep19 |
| **CISRO ICS Policy** | The following changes done.<br>- Role and Responsibilities section.<br>- SLM-230 updated.<br>- CISO reference updated to CISRO | - | Liz Banbury [delegate of Group CISRO] | 1.1 | 28-Oct-19 | 28-Oct-19 |
| **CISRO ICS Policy** | The following changes were incorporated:<br>Editorial: Introduction & Purpose section; SLM-310; Glossary<br>Minor: roles & responsibilities; SLM-010-011; SLM-020, SLM-110;<br>Major: Scope redefinition; SLM-030; SLM-040;SLM-050; SLM-080; SLM-090; SLM100; SLM-120-170; SLM-180200; SLM-210-260; SLM-300340 New controls: SLM-001-009; SLM-021; SLM-041-042; SLM-080-088; SLM-111-112; SLM 171-173; SLM-201-202; SLM-261<br>Removed: SLM-270-290; log entry attributes requirements; event types; requirements for non-prod (as covered by new approach); list of systems/product/platforms<br>New content: ICS logging & | - | Liz Banbury [delegate of Group CISRO] | 2.0 | 15-Jan-21 | 15-Jan-21 |

| Name | Changes made | Materiality | Approved by | Version number | Approval Date | Effective Date |
|---|---|---|---|---|---|---|
| | monitoring baselines; threat/risk examples | | | | | |
| **CISRO ICS Policy** | Annual review: Risks, Roles and Responsibilities alignment to RTF. Controls updated: SLM-070, SLM-088, SLM140, SLM-180 | - | Samantha Finan, Global Head, ICS Policy, Standards and Reporting | 2.1 | 10-Dec-21 | 10-Dec-21 |
| **CISRO ICS Policy** | Controls removed: SLM-300, SLM-320, SLM-330, SLM-340 Controls updated: SLM-310 New controls: SLM-350, SLM-360, SLM-370, SLM- 380, SLM-390, SLM-400, SLM-410 | - | Samantha Finan, Global Head, ICS Policy, Standards and Reporting | 3.0 | 24-Jun-22 | 24-Jun-22 |
| **CISRO ICS Policy** | Editorial: Out of scope subsection re-added due to clerical error in version 3.0 | - | Samantha Finan, Global Head, ICS Policy, Standards and Reporting | 3.1 | 28-Jul-22 | 01-July-22 |
| OTCR ICS Policy | Editorial:<br>1. Document template aligned with Template for Group Standards v6.0.<br>2. Document references updated (as per the ICS RTF consolidation under ERMF)<br>Material:<br>1. ICS controls simplification in line with the principles and strategic approach for ICS Standards simplification (ICSCR-08May24-1)<br>2. Consideration of. ICSCR28Sep23-1 Change Requests for establishing a Group | Material | Mark Strange, Global Head, OTCR - TTO | 4.0 | 16-Sep-24 | 16-Mar-25 |

| Name | Changes made | Materiality | Approved by | Version number | Approval Date | Effective Date |
|---|---|---|---|---|---|---|
| | Threat Library<br>3. New Controls : New SLM-375; New SLM-385; New SLM-386; New SLM-387; New SLM-389; New SLM-391;New SLM-392<br>4. Removed Controls : SLM-001; SLM-003 ; SLM-004; SLM-005; SLM-008 b; SLM-009; SLM-011; SLM-020; SLM-021; SLM-060; SLM-070; SLM-085; SLM-160; SLM-171SLM190; SLM-201; SLM-202; SLM-260; SLM-370<br>Updated Controls: SLM-002 [Consolidated SLM-003]; SLM-006 [Consolidated SLM-009]; SLM-008 [Consolidated SLM-008 b]; SLM-010 [ Consolidated SLM-011 ;<br>SLM -020 ; SLM-021]; SLM-110; SLM-310; SLM-350; SLM-360; SLM-007 a; SLM-100; SLM-130; SLM-380; SLM-007 a; SLM-130; SLM-380; SLM-042 [Consolidated SLM-086];<br>SLM-050 [Consolidated SLM-087]; SLM-088 [ Consolidated SLM-070] | | | | | |
| **CISRO ICS Policy** | Editorial: Due to error, version 4.0 with March 2025 Effective Date got published prematurely. Reverting the changes to replace with last live version 3.1. | Non-Material | Jamie Cowan Head, ICS Risk Framework & Governance | 4.1 | 29-Jan-25 | 04-Feb-25 |
| OTCR ICS | Editorial:<br>1. Administrative | Non - Material | Jamie Cowan | 4.2 | 29-Jan-25 | 16-Mar-25 |

| Name | Changes made | Materiality | Approved by | Version number | Approval Date | Effective Date |
|---|---|---|---|---|---|---|
| Policy | changes introduced to update document template, references, roles, and ownership.<br>2. Version Number Change - As V4.0[Eff. Date – March 2025] got published prematurely, the only change in this version is -updated version number [with V4.0 content intended to be effective from March 2025] | | Head, ICS Risk Framework & Governance | | | |

## 9. Version Control Table

| Document Author | Changes made | Materiality | Approved by | Version number |
|---|---|---|---|---|
| OTCR ICS Policy | Editorial:<br>• Administrative changes introduced to update document template, references, roles, and ownership.<br>• Version Number Change - As V4.0[Eff. Date – March 2025] got published prematurely, the only change in this version is -updated version number<br>[with V4.0 content intended to be effective from March 2025] | Non - Material | Jamie Cowan Head, ICS Risk Framework & Governance | 4.2 |

The full version history is included in *Appendix A – Version Control Table*