Security Incident Response and Management

Version No	1.5
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	Bali Chandramouli; Arti Singh
Document Contact Job Title	VP, OTCR, Policy & Regulatory Management; Assoc Dir, ICS Standards
Business Scope	All Businesses
Function Role	All Functions
Geography Scope	GLOBAL
Approval Date	04/12/2024
Effective Date	16/12/2024
Next Review Date	30/06/2027

Table of Contents

1. INTRODUCTION AND SCOPE 4
1.1. Risks 4
1.2. Scope 4
2. ROLES AND RESPONSIBILITIES 4
3. STANDARD REQUIREMENTS 5
3.1. Control Area - Security Incident Handling 6
3.2. Control Area - Coordination and Information Sharing 8
4. INFORMATION AND SUPPORT 8
4.1. General Information and Support 8
4.2. Reporting Non-Compliance 8
4.3. Breach of this Standard 8
5. GLOSSARY 9
6. REGULATORY OR INDUSTRY REFERENCES 9
7. APPENDIX 9
7.1. Remedial Actions 9
7.2. Process References 9
7.3. Appendix A - Version Control Table 10
8. Version Control Table 11

Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Arti Singh	Migration to Inline format- Non Material Change(No change to document content)	Non-Material	Jamie Michael Cowan	1.5	04/12/2024	16/12/2024

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

1. INTRODUCTION AND SCOPE

Security incident response has become an important component of Information and Cyber Security programs. Cybersecurity-related attacks have become not only more numerous and diverse but also more damaging and disruptive. New types of security-related incidents emerge frequently. Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimising loss and destruction, mitigating the weaknesses that were exploited, restoring services and to ensure the prevention of further impacts to the Group.

Security incident management must also include how incidents are investigated and the secure collection and handling of Information so that any Information which is or becomes evidence is legally admissible and sound.

Since performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources. This standard assists in establishing such capabilities and handling incidents efficiently and effectively.

1.1. Risks

The Security Incident Response and Management [SIRM] Standard mandates that adequate security controls are implemented to detect and respond to incidents on all the Information Assets, Information Systems and Technology Infrastructure that comprise the Group's network.

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. 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 accordingly in line with applicable ICS controls defined in ICS Standards.

2. ROLES AND RESPONSIBILITIES

Information Asset Owner

A named individual with accountability for the protection and permissible use of owned information Assets in Information Systems and Technology Infrastructure.

Information System Owner

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

Technology Infrastructure Owner

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

Process Owner (PO)

The PO to embed applicable requirements of this Standard within their process and within any suppliers, joint ventures and outsourced/off-shored activities for which they are responsible for.

The PO is responsible ensuring quality, timeliness and adequacy of provided data, and management information to measure appropriate coverage and performance of control points (and subsequent measurement) against ICS Policy and Standards.

In addition to that PO is accountable for providing operational capability to support Information Asset/System/Technology Infrastructure Owners to deliver required objectives of the Standard.

Group Chief Information Security Office (Group CISO)

The Group CISO is responsible for:

- Complying with the control areas of this Information Security Standard which are applicable to them.
- CISO Awareness team are responsible for ensuring that the Group is provisioned with the appropriate awareness and training tools (messaging, content, strategy and governance and training support).
- Notifying OTCR as and when they become aware of any regulations relevant to ICS issued by non-financial services regulatory authorities;
- Identifying the relevant Process Owners responsible for implementing the regulation in their processes and informing OTCR;
- Implementing ICS Policy and Standards;
- Ensuring mechanisms are in place to demonstrate that necessary documentation and audit trail concerning implementation of ICS LRM requirements are maintained;
- Completing attestations to relevant regulatory authorities to confirm compliance to the relevant regulations; and
- Tracking remediation of gaps identified from LRM attestations in line with remediation programmes.

As first line role holders, the Group CISO will additionally perform effectiveness reviews to monitor first line compliance with this Information Security Standard.

CISO ICS Standards & Controls

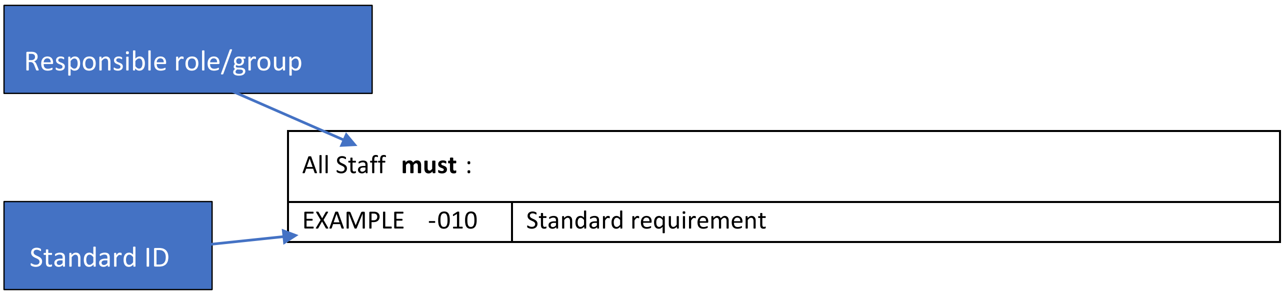
The CISO is the owner of this Information Security Standard and will ensure the document is updated to an agreed schedule.

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.

3. STANDARD REQUIREMENTS

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



Responsible role/group

Standard ID

All Staff **must** :	
EXAMPLE -010	Standard requirement

3.1. Control Area - Security Incident Handling

3.1.1 Preparation

Information Asset/System Owners **must**:	
SIR-010	Ensure that the SIRM process is formally documented, approved and implemented by the Information Custodian.

Process Owner **must**:	
SIR-020	Ensure that a) a Security Incident Response Management ("SIRM") process is formally defined, documented, approved and implemented. b) the SIRM process is reviewed & tested at least on an annual basis and the result is reported to management/risk committee.
SIR-030	Ensure that the SIRM process at a minimum covers the following components: a) The steps required to handle security events and incidents, that is, Identification, Classification, Categorisation and Prioritisation, Investigation and Diagnosis, Resolution and Recovery of incidents along with resolution time lines; b) Specific tools and Information needed to support the management of incidents; c) Types of security events to be logged / recorded in line with Security Logging and Monitoring Standard; d) Roles and responsibilities for both individuals and teams/functions involved in security incident management; e) Escalation and reporting paths; f) Logging incident management activities; g) Methods for handling and storing forensic evidence (chain of custody); h) Internal and External Thresholds for Incident response time; and i) Approval of communication with external agencies including regulators. *[Reference: ICS Security Logging and Monitoring Standard]*
SIR-040	Establish clear guidelines, relationships and lines of communication between the incident response team and key groups, both internal (for example: legal department and external law enforcement agencies).
SIR-050	Establish a relationship between Group and external providers [Third Party Service providers and Product Vendors] of Information Asset and Information System protection capability in case of investigation and containment support.

3.1.2 Detection and Analysis

Process Owner **must**:	
SIR-090	Co-ordinate in the identification, collection, and preservation of evidence in accordance with different types of media, devices and status of devices.
SIR-100	Facilitate in the provision of data to the requestor, in response to investigative and litigation support requests.
SIR-120	Ensure that the evidence collection is in accordance with applicable laws and regulations and is carried out in consultation with the forensic team, legal team and appropriate law enforcement agencies so that any evidence retains its evidentiary value and can be admissible in court.
SIR-130	Ensure that the evidence is accounted for at all times whenever evidence is transferred from person to person. Chain of custody forms should detail the transfer and include each party's signature.

3.1.3 Containment, Eradication and Recovery

Information System / Technology Infrastructure / Process Owner **must**:	
SIR-140	Co-ordinate with the CISOs, and the key stakeholders as per the Cyber Security Incident Response process for remedial actions where a breach of Information security is suspected or confirmed. *[Reference: Table: Remedial Actions]*
SIR-150	Engage with external providers when support is needed with investigation and containment of incident.

3.1.4 Post Incident Activity

Information System / Technology Infrastructure / Process Owner **must**:	
SIR-160	Co-ordinate post incident reviews for all high and critically rated incidents.
SIR-170	Ensure the post incident review includes the following: a) The root causes are accurately identified; b) The response process followed the established process; c) The incident evidence has been maintained appropriately in line with legal and group retention requirements; d) The incident was resolved in a timely and efficient manner; e) Appropriate preventive or corrective steps were taken; f) Advise on approach to detect similar incidents in the future is documented and communicated and g) Lessons learnt are communicated and incorporated to prevent future incidents. *Note: Consult Legal regarding the terms of reference of review as well as the format and distribution of security incident report which are rated high and critical.*
SIR-180	Ensure all closed incidents and associated evidences are retained for at least a period of 3 months. This excludes considerations for retention related to business, legal and regulatory requirements which need to be established separately in consultations with relevant parties. *[Reference: Group Data Conduct Policy and Group Record Keeping Standard]*

OTCR Coverage **must**:	
SIR-190	Provide 2nd Line of Defense [LoD] review and challenge of risk ratings for ICS related incidents (external/internal).
SIR-200	Contribute to and review the Root Cause Analysis [RCA] for ICS Incident that result in Material Risk Events. *Note: Material Risk Events are defined in the Group Operational Risk Standard: Where the Financial and/or Non-Financial Impact exceeds the Materiality threshold in the Group Operational Risk Standard, the risk event is classified as a Material Risk Event.*

3.2. Control Area - Coordination and Information Sharing

Process Owner **must**:	
SIR-210	Implement a coordinated and structured communication plan to be followed during an incident for notifying relevant stakeholders.
SIR-220	Implement a process to report the Information and Cyber Security incidents to the relevant internal parties and regulators as per their defined notification period.

OTCR **must**:	
SIR-230	Be consulted to review any decisions taken relating to the reporting to Regulators of ICS incidents leading to Material Risk Events in any part of the Group. *Note: Reporting of incidents must meet Regulatory requirements in force in the affected area.*

4. INFORMATION AND SUPPORT

4.1. General Information and Support

For queries relating to this Security Standard please contact the ICS Standards Policy 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. Remedial Actions

S. No	Actions
1	Assessment of scope, effects and prioritisation of the incident or breach.
2	Ensure all evidence required for further incident investigation is preserved properly
3	Minimise the business impact from an identified Information security incident in a way which does not interfere with the investigation of the incident or destroy required evidences.
4	Cleansing of Information Systems and Technology Infrastructure configuration
5	Restoration of Information Systems, Information Assets and services
6	Validate the Information System restoration to confirm that the Information System has resumed normal business service.
7	Preventive and corrective actions to prevent recurrence of the incident
8	Collection of evidence for further investigation

7.2. Process References

a) Cyber Security Incident Response Process –

Link - https://standardcharteredbank.sharepoint.com/:b:/r/sites/ttotpuregistry/L2%20Processes/(Detection%20%26%20Response)%20Cyber%20Security%20Incident%20Response%20Process.pdf?csf=1&web=1&e=P6G3pc

b) Major Incident Management Process –

Link - https://standardcharteredbank.sharepoint.com/sites/ttotpuregistry/L2%20Processes/Forms/AllItems.aspx?id=%2Fsites%2Fttotpuregistry%2FL2%20Processes%2F%28L2%2DPRO%2ETMT%2EIM%29%20INCIDENT%20MANAGEMENT%20PROCESS%2Epdf&parent=%2Fsites%2Fttotpuregistry%2FL2%20Processes

7.3. Appendix A - Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISRO Policy	Annual review includes: 1. Migrated existing standard to ERM standard template. 2. The existing Security Incident Response and Management Standard document has been uplifted into this standard. 3. Consultation feedback, corrections incorporated.	-	Liz Banbury, Head, ICS Policy	1.0	20-Dec-19	24-Dec-19
CISRO Policy	Annual Review – Alignment of Scope, Risks, Roles & Responsibilities with correct functions: Amended statements: **Administrative, Editorial**: SIR-060, SIR-230 **Administrative, Removed**: SIR-070, SIR-080, SIR-110, SIR-200	-	Liz Banbury, Head, ICS Policy	1.1	20-May-21	25-May-21
CISRO ICS Policy	1.Template updated to ERM Standard template v5.6 2.Changes made w.r.t ICS Policy Change Requests – ICSCR-26Feb23-1 – Added SIR-200 & modified SIR-140, SIR-190 & SIR-230.	-	Paul Hoare Head, ICS Policy and Best Practice	1.2	17-July-23	22-July-23
CISRO ICS Policy	Amendment w.r.t ICS Policy Change Requests – 1. ICSCR-10Apr23-2 – Added SIR-020 b). 2. ICSCR-18Feb2022-1 –	-	Paul Hoare, Head, ICS Policy and Best Practice	1.3	13-Nov-23	18-Nov-23

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	Removed SIR-060 as covered in AUS Standard. 3. People Manager to People Leader					

8. 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	1.4	04-Dec-24	16-Dec-24