INFORMATION AND CYBER SECURITY RISK MANAGEMENT STANDARD

Version No	V3.0
Document Type	Standard
Parent Framework	Enterprise Risk Management Framework
Document Approver Name	Dominic Clarke
Document Approver Job Title	Global Head, OTCR
Document Owner Name	Margaret Norden
Document Owner Job Title	Global Head, OTCR, Framework & Stress Testing
Document Contact Name	Marek Kwas
Document Contact Job Title	Senior Manager ICS Risk
Business Scope	All Businesses
Function Role	All Functions
Geography Scope	Global

Refer to GovPoint for Effective Date, Approval Date and Review Dates.

Table of Contents

Version Control Table

Name	Changes made	Approved by	Version number
Leke Akanbi	New	Linda Olufawo	1.0
Leke Akanbi	2022 Refresh	Darren Argyle	2.0
Marek Kwas	2024 Interim Refresh	Margaret Norden	3.0

1. INTRODUCTION AND SCOPE

Information and Cyber Security (ICS) risk is an inherent part of the Group's business and is defined as "the risk to the Group's assets, operations and individuals due to the potential for unauthorised access, use, disclosure, disruption, modification, or destruction of information assets and/or information systems".
This ICS Risk Management Standard defines the approach and outlines the risk management components and key activities in managing ICS Risk systematically across the Group as depicted in Fig 1 below.

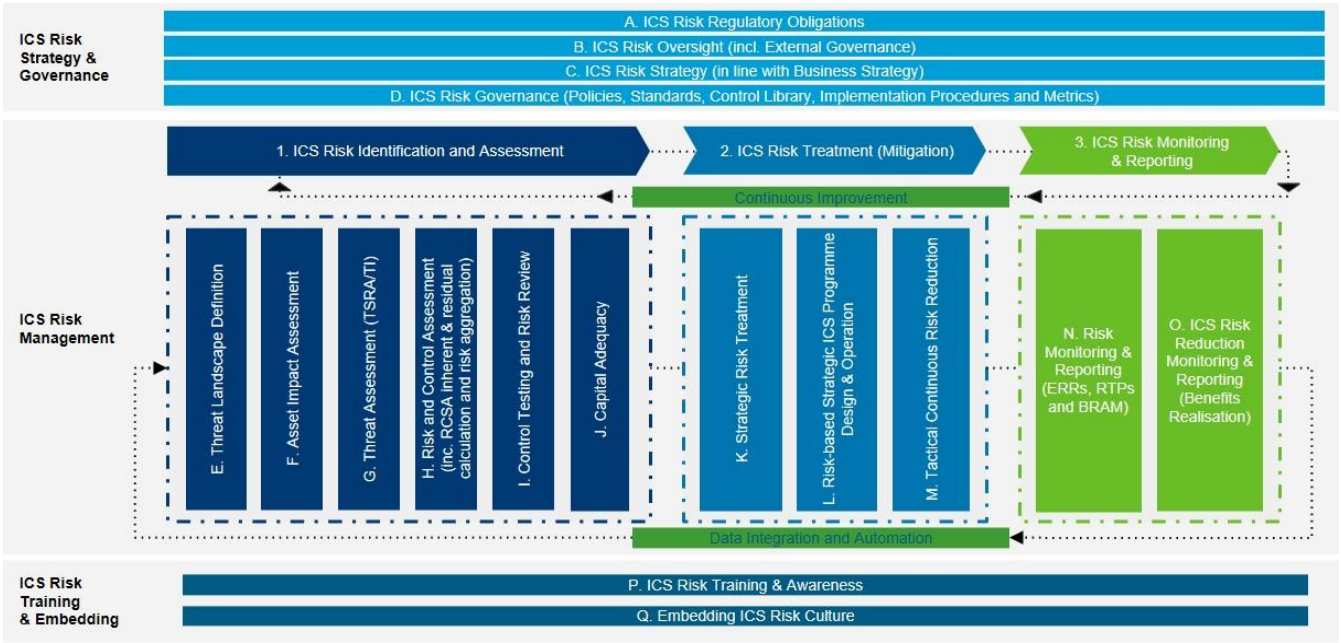
- An **Activity** refers to a collection of tasks executed to achieve an outcome/output as part of end-to-end ICS Risk Management and Governance.
- An **Activity Owner** is responsible for the performance or delivery of an activity.

Details of activities including how they are performed, and tooling used is out of scope of this document.

The Standard is mapped to the 3 Risk Sub-Type under Information and Cyber Security Risk Type Framework ("ICS RTF"):

- 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

Fig 1: **ICS E2E Risk Management & Governance (ICS RM&G) Model**



Note: Activities and sub-activities within the ICS E2E Risk Management & Governance model may relate to either Processes (as defined by the Process Universe) or to tasks that are performed by the Bank that are not formally defined as a Process.

1.1 Applicability

This standard must be implemented across the Group covering all businesses, functions, and countries. This standard is to be read in conjunction with the parent Information and Cyber Security Risk Type Framework (ICS RTF), Operational & Technology Risk Type Framework (O&T RTF), Group Operational Risk Standard and the related ICS Policies, Standards and Methodologies.
Applicability to different types of ventures with SC will be covered by the SC Ventures addendum to the ICS RTF.

1.2 Governance of ICS Risk Management Standard

The second line of defence (2LoD) has defined the following governance and oversight mechanisms to ensure risk management activities defined within the ICS E2E Risk Management & Governance model are consistently maintained and updated as key activities within the Group change over time:

- Activity* / Process owners maintain and update the ICS risk management activities within the ICS Risk Management Standard in the event that changes occur to existing activities or new sub-activities are created which help manage ICS risk.
- Activity* / Process owners will conduct light-touch (control metrics based) quarterly reviews, considering the accuracy, effectiveness, and status of gaps/deficiencies identified.
- Where these activities have been identified as processes and adopted into the Process Universe, the (evidence based) Enterprise Risk Management Effectiveness Review will apply as the fourth quarterly review.
- The results of these quarterly reviews and any ad-hoc changes/additions which occur will be reported to the 2LoD CISRO function for review and approval prior to the ICS E2E Risk Management & Governance model being amended.
- Trigger events[1] may invoke the need to update components of the risk management activities including changes to the threat landscape, assets and risk events that require the risk assessment to be reviewed or the risk and control taxonomies to be updated accordingly.

2. ICS END-TO-END RISK MANAGEMENT & GOVERNANCE OVERVIEW

2.1 End-to-End Risk Management & Governance (ICS RM&G) Model and Process Flow

Figure 1 (page 5) provides a visual representation of the ICS E2E Risk Management & Governance model, structured into 3 components (ICS Risk Strategy and Governance, ICS Risk Management and ICS Risk Training & Embedding), which defines the flow of components and activities that the Group performs to define its risk appetite, manage risk, and embed ICS risk management principles into the organisation's culture.
Underpinning the model are sub-activities that capture the logical operational tasks that are performed to manage ICS risk. These sub-activities are defined in more detail within Sections 3-5 of this document.

2.2 ICS Risk Management Principles

The ICS Risk Management Principles listed below build upon those defined within the ICS RTF and set out the Group's approach for managing ICS Risk and the foundation for the key activities defined within the E2E ICS Risk Management Standard.

1. **Comprehensive** - ICS risk management should be comprehensive and consider the full spectrum of risk variables including assets and their value, threats and vulnerabilities, and relevant preventative, detective and corrective controls that mitigate risk within appetite.
2. **Consistent** - ICS risk management should be performed for all applicable risk sub-types (categories) and threats (based on the assessment scope and asset value), and at the appropriate level of abstraction[2] to support consistent application and aggregation of the Group ICS risk profile.
3. **Accurate** - ICS risk management should objectively define and measure the risk and risk reduction of preventative, detective and corrective controls to both threat likelihood and risk impact.

[1] As defined in the Operational & Technology Risk Management Standard

* Activities are being reviewed to identify those that will be converted to processes.

[2] E.g., assets logically grouped by process, such as Payment Systems. Specific scenario deviations can be defined where valuable due to a unique impact or threat exposure.

4. **Efficient** - ICS risk management activity should be efficient and manual processing should be automated where possible to improve accuracy and consistency and the productivity of people managing risk.
5. **Scalable** - ICS risk management activity should be scalable across the enterprise, and design decisions on aspects of its methodology and implementation thought through to make sure they do not produce undue strain on the business.
6. **Oversight** - ICS risk management activity should support board and senior manager oversight through simple business articulation of the threats and impacts to their operations, supported by relevant MI to the assets in scope of assessment.
7. **Sustainable** - ICS risk management should be sustainable in terms of the architecture of risk management, with processes and assets being implemented secure by design.

2.3 Roles and Responsibilities

All roles and responsibilities (across 1LoD and 2LoD) as they relate to each activity in this ICS Risk Management Standard can be found in the ICS E2E Risk Management & Governance Roles & Responsibilities document (see Appendix 6.6).

3. ICS RISK STRATEGY & GOVERNANCE

Component Overview
ICS Risk Strategy & Governance is the first component of the ICS E2E Risk Management & Governance model. It defines the Group's ICS risk strategy and risk appetite, incorporating applicable regulatory obligations, governance, and approach to managing ICS risk. It also establishes the oversight and governance performed over the activities within the risk management model to ensure ICS risk is being managed effectively on an ongoing basis.

3.1 A. ICS Risk Regulatory Obligations

ICS Risk Regulatory Obligations define the Group's regulatory obligations across all relevant markets/countries, and how these requirements translate to policies, standards and controls for the Group's businesses and countries to operate within and ensure compliance, covering the following key areas:

3.1.1 ICS Risk Regulatory Obligations

Identify, document, and maintain ICS regulatory requirements.
The ICS Legal Regulatory and Mandatory (LRM) Obligations Register and the ICS Policy / Standards Gap Analysis must be reviewed and updated on at least an annual basis, or upon the mandate of a new or modified LRM requirement applicable to the Bank and the relevant markets and countries it operates within.

3.1.2 ICS RTF Local Addendum

Identify, document, and approve local variation against the ICS RTF.
ICS RTF Local addendums must be reviewed and updated when material changes to the Group ICS RTF are made and at least once every two years, or upon the mandate of a new or modified LRM requirement applicable to the Bank and the entities it operates within. This includes ICS Policy and Standard addendums when needed.

3.1.3 ICS Risk Regulatory Attestations

ICS risk regulatory attestations must be formally declared, confirming the undertaking or completion of actions required by LRM bodies pursuant to a specific regulatory requirement. 2LOD must perform oversight role over all regulatory attestations.

3.2 B. ICS Risk Oversight

The ICS Risk Oversight activity sets and oversees the risk appetite, its continuous alignment with regulatory obligations and business risk strategy. This provides the Executive and Board insight into ICS risk to support their decision making.

3.2.1 Set Risk Appetite

Develop and maintain a methodology providing guidance, approach, and responsibilities on the setting of risk appetite for Group, Business and Regions and Country.

ICS Risk Appetite Statements must be agreed as the approved boundary for the risk that the Group is willing to undertake. It must be set within the Risk Capacity which is defined as the maximum level of risk the Group can assume, given its current capabilities and resources, before breaching constraints determined by capital and liquidity requirements, internal operational environment, or otherwise failing to meet the expectations of regulator and law enforcement agencies.

ICS Risk Appetite Statements (RAS), and their respective metrics with defined thresholds must be reviewed and updated on at least an annual basis with due consideration given to the external and internal threat landscape, and control effectiveness to mitigate relevant threats to the Group.

3.2.2 ICS Risk Oversight

CISRO teams, on behalf of the RFO, provide oversight and governance of key ICS Risk activities across the Group. This includes oversight of ICS Risk papers, ICS Risk profiles and Board Risk Appetite.

In addition, oversight is also performed by risk committees as defined by the ICS RTF and their respective Terms of Reference (ToR), including Board Risk Committee (BRC), Group Risk Committee (GRC), Group Non-Financial Risk Committee (GNFRC) and Non-Financial Risk Committees (NFRC).

3.2.3 Board Risk Appetite Metrics - Reporting Requirements

Definition of metrics that measure the Board ICS risk appetite and reporting requirements.

Board Risk Appetite Metrics (BRAMs) must be defined, as outlined in the ICS RTF, to reflect the risk appetite and measure the Banks ability to meet risk appetite. They must be reviewed and updated at least annually, and data used to support BRAM is considered a CRM and falls under the scope of BCBS239 (*Basel Committee on Banking Supervision - Principles for effective risk data aggregation and risk reporting*).

BRAM breaches will be treated in line with the requirements and guidelines in the ICS RTF and ERMF.

3.2.4 Partnerships (Internal & External)

Establishing collaboration and partnerships with key ICS stakeholders (internal and external), to share best practice, build thought leadership, and contribute to the wider cyber industry.

Partnerships with internal and external partners must be established. They should include: The Cyber Partnerships and Engagement Forum; The Cyber Security Regulatory Look Forward; ICS External Industry Forum Engagement; and Speaking Engagements and Regulatory Consultations. These forums will be used to highlight key regulatory developments and requirements, obtain valuable insights across the sector and distribute ICS regulatory updates.

3.2.5 Third Party Security Risk Oversight

CISRO, on behalf of the RFO will provide oversight and challenge of the management of Third-Party Security Risk (TPSR) – the ICS risk of sharing of data or provision of a service with/by a third party. This involves establishing baselines and policies to manage TPSR; guidance on what good looks like, and monitoring of activities to identify trends and cases where risk tolerances may be breached.

3.3 C. ICS Risk Strategy

This activity defines and maintains the ICS risk strategy, in accordance with the risk appetite and ICS strategy, which outlines the key risks, threats and the strategic risk management plan including key ICS capabilities that will deliver risk mitigation.

3.3.1 Define Group ICS Risk Strategy (Overarching)

The Group ICS Strategy supports the delivery and realisation of the Group Strategy. This Strategy supports alignment of all ICS related activities, enabling a coherent and synergistic effort across the Group.

3.3.2 Define ICS Risk Strategy (CISRO)

The ICS Risk Strategy (CISRO) must define how the second line of defence (2LOD) for ICS (CISRO) will operate, engage, delegate, assure and oversee the Group's ICS implementation and strategy.

3.3.3 Define ICS Strategy (CISO)

The first line of defence (1LoD) ICS Strategy (CISO) must be defined and supported by the ICS Strategic Journey that outlines how long-term security outcomes are delivered including timelines for increasing security maturity.

3.4 D. ICS Risk Governance

This activity defines and sets the Risk Type Framework, policies, standards, methodologies, procedures, and metrics to identify, manage and monitor ICS risk.
The CISRO has developed an ICS Risk taxonomy to set out clear and consistent definitions for governing documentation types, which can be found in Appendix 6.3.

3.4.1 ICS Risk Type Framework

The Group Information and Cyber Security Risk Type Framework (ICS RTF) must document at a high-level risk management principle, risk sub-types, risk appetite (RA), second line processes for oversight and challenge, key first and second line roles and responsibilities, decision making authorises, delegation of authority, regulatory obligations and approach to risk assessment, identification, and monitoring against RA.
The Group ICS RTF must be reviewed with due consideration given to the LRM and ERMF requirements, Business and ICS strategy, industry best practice risk management frameworks, risk appetite, operational risks and other Principal Risk Types across the Bank.

3.4.2 ICS Policy

The ICS Policy defines the mandatory principle-based statements that are designed to control and mitigate ICS risk.
A policy must be designed to control and mitigate ICS risk through mandatory principle-based statements that are actionable through key control objectives or with expected outcomes. ICS policy statements support the guidance set out by the ICS RTF.
The Group ICS Policy must be reviewed according to the frequency set out by the ERMF, taking into account the guidance and requirements set out by the ICS RTF.

3.4.3 ICS Standards

The ICS Standards define the minimum control requirements for specific control disciplines or domains and support higher level statements in the ICS Policy.
A set of Standards must be created as operational documents to implement the requirements set out in the Framework or Policy.
The suite of ICS Standards must be reviewed according to the frequency set out by the ERMF, considering the guidance and requirements set out by the ICS RTF, or upon a significant change in the Groups operating environment with due consideration given to LRM requirements, industry standards and good practice.

3.4.4 ICS Methodologies

ICS Methodologies are a high-level description of 'how to principles' to support implementation of the Framework, Policy, or Standards.
The examples of methodologies governing ICS Risk Management are the Threat Scenario-Led Risk Assessment (TSRA) Methodology and the Asset Impact Assessment Methodology.

The ICS Methodologies must be reviewed according to the frequency set out by the ERMF, taking into account the guidance and requirements set out by the ICS RTF.

3.4.5 Technical Information Cyber Security Standards

Documentation describing the standards to maintain technical information security requirements.
The Technical Information Cyber Security Standards must be developed and reviewed at least annually, or upon update of the relevant security standard to ensure technical security requirements outlined in the ICS Policy and standards, are implemented for information systems and technology infrastructure.

The Technical Information Cyber Security Standards are the specific requirements for local implementation (not configurations) of a control on an information system and/or technology infrastructure asset and the associated activities and are the L4 technical ICS Actual Controls within the ICS Control Library.

Minimal security baseline requirements (MSBRs) for information systems and/or technology infrastructure as per SCM-030, reference the applicable L4 controls defined by the relevant Technical Information Cyber Security Standards.

3.4.6 Technical Information Procedures[3]

The Technical Information Procedures describe the granular steps required to implement requirements for Information Assets and Systems.
The Technical Information Procedures must be developed and reviewed at least annually, with due consideration given to the relevant ICS Standards; and Technical Information Security Standards.

****The Technical Information Procedures activity (description, ownership, and RACI) is currently under review****

3.4.7 ICS Security Architecture

The definition, review and guidance of Information Security capabilities is driven by the security architecture function which provides the strategic outline and recommends controls in line with business requirements with regards to protecting the confidentiality, integrity, and availability of organizational information and assets.

The security architecture function defines and approves the required cyber security architecture and designs principles which relevant control owners must consider for developing cyber security controls and applying cyber security requirements, information security architecture changes are reflected in the security plans both for ICS and Enterprise Technology as well as relevant Third Parties including JVs and acquisitions.
The security architecture function reviews the Bank's cyber security architecture and the cyber security capabilities against the changes in the ever-evolving threat landscape and business requirements, steering the organization towards compliance, and continuously improving the organization's security posture.

3.4.8 Control Library (including Metrics Definition)

The ICS Control Library describes the suite of ICS controls and their objectives, which are selected from ICS Standards and used to help the Group manage ICS risk. The library is comprised of multiple levels that have associated key terms and definitions (please see Appendix 6.4).

The controls and metrics maintained in the ICS Control Library must be reviewed on a regular basis, taking into account control statements detailed in the ICS Standards.

Metrics must be defined to measure coverage and performance of controls against risk appetite. Metrics definitions and thresholds must be reviewed on a regular basis.

[3] Activity under design / implementation

3.4.9 ICS Metrics Publishing (including development where applicable)

ICS Metrics required for the Threat Scenario Risk Assessment (TSRA) must be published on Sentinel as per the agreed metric frequency. The Board Risk Appetite Metrics (BRAM) must be published monthly on the BRAM dashboards within the Sentinel tool.
Where metrics are applicable to be developed and automated, this activity is done by the ICS R&G team.

3.4.10 RTF Effectiveness Review

RTF Effectiveness Reviews assess the effectiveness and quality of the operational implementation of the ICS RTF.
Effectiveness reviews must be performed in line with the requirements defined in the ERMF.
The RTF Effectiveness Review Plan, Schedule and Report must be established to ensure continuous improvement of ICS Activities and Processes and taking into account supporting documentation and evidence, control effectiveness evidence, audit and regulatory review findings.

4 ICS RISK MANAGEMENT

Component Overview
ICS Risk Management is the second component of the ICS E2E Risk Management & Governance model. The purpose of this component is to manage the Group's exposure to risk through identification, assessment, treatment, monitoring, and reporting.
This component is split up into the following three sub-components:

1. ICS Risk Identification and Assessment;
2. ICS Risk Treatment (Mitigation); and
3. ICS Risk Monitoring & Reporting.

Activities described in this section are the required steps to perform the **TSRA/RCSA** process. Additional details on this process could be found in the TSRA Methodology.

ICS Risk Identification and Assessment Sub-component
ICS Risk Identification and Assessment is the first of three sub-components that make up the ICS Risk Management component. Its primary purpose is to identify ICS threats that are relevant to the Group's assets, assess their inherent risk (impact and likelihood), and how effective the Group's controls are at mitigating them (residual risk).

4.1 E. Threat Landscape

As an international organisation, the Group has a large attack surface that can be exploited or compromised by a number of internal and external Threat Actors. Therefore, understanding the Group's threat landscape is a vital component of the wider process of identifying Threat Scenarios, potential business impacts and mitigating controls.

This activity identifies and understands the threat landscape the Group operates in, recognises the ICS threats the Group is exposed to, including who can or would attack, and how they may do so. These can be driven by a variety of factors, including:

- The profile of the financial services as a whole; and
- The nature of Group business operations, assets held, systems used, geographic presence, political exposure, and business relationships.

4.1.1 Identify Threat Landscape

The threat landscape must be identified and monitored based on real world ICS threats on an ongoing basis as they continue to evolve - including the actors, their techniques and intent. The threat management process must be executed by qualified individuals with the purpose of organisational threat visibility, proactive and reactive response, and attribution of threat activity.

4.2 F. Asset Impact Assessment (TSRA)[4]

The Asset Impact Assessment activities support the Group's risk-based prioritisation of business risk management activities. Assets include the Group's Information Assets, and their supporting Information Systems and Technology Infrastructure. These assets are of value to the Group and require protection through controls to prevent the impact of a loss event.
These activities enable the Group to identify the criticality of its Information Assets, that represent the starting point for assessing risk. They are the object of value which could have its Confidentiality, Integrity, or Availability compromised leading to adverse business impacts.

4.2.1 Configuration Management

Accurate knowledge regarding the Assets that require protection is essential to ensure that ICS controls can be correctly identified and applied. Moreover, ICS risk management activities cannot be conducted accurately without proper impact identification and evaluation.

The inventory of Configuration Items (CIs) within the Configuration Management Database (CMDB) must be reviewed and updated on at least an annual basis, or upon a material change to assets in order to help facilitate effective decision making.
Ownerships of Information Assets, Information Systems and Technology Infrastructure must be assigned to ensure they are effectively maintained.

4.2.2 Information Asset & S-BIA

The Information Asset Impact Assessment and Security Business Impact Assessment (S-BIA) assesses the impact to the Group if the confidentiality, integrity, or availability (CIA) of an Information Asset or Information System is compromised respectively.
The Information Asset Inventory and Asset Impact Assessment ratings must be updated for Information Assets on an annual basis as a minimum, or upon material changes to assets, in accordance with the Information Asset Methodology.

Security Business Impact Assessments must be performed for Information Systems at least annually or upon material change to the system architecture, in accordance with the S-BIA Methodology. Technology Infrastructure, by default, inherits the impact rating from Information System(s) hosted. In the cases, where:

- Rating inheritance cannot be easily identified (usually for non-core Technology Infrastructure), or
- Technology Infrastructure should be rated independently (as the inheritance pattern may not provide reliable results or where particular Technology Infrastructure Components' impacts differ)

For more information regarding the detailed practices for the classification of assets, please refer to the Information Asset Impact Assessment & Security Business Impact Assessment Methodology documents.

4.2.3 Assess Third Party Risk Exposure[5]

Third party risk exposure must be assessed in order to understand and measure the inherent ICS risk of sharing data or outsourcing services to a third party, and the potential impact it may have on the Groups confidentiality, integrity and availability of its Information and Services.
The Inherent Security Risk Rating (ISRR) of a third party must be identified and a recertification and update performed on an annual basis, or upon material change to the scope of services being provided by a third party, taking the information in the Risk Identification Forms (RIF) and third party service provision details into consideration. The ISRR must be aligned to the GRAM rating.

---

[4] NOTE: This activity is related to the ICS Threat Scenario-Led Risk Assessment (TSRA). Any other TSRA activities will be referenced using "(TSRA)" in the activity titles.

[5] Activity under implementation

4.2.4 Report Attack Surface[6]

This activity reports on the change in size and complexity of the organisation by asset type (e.g. people, third parties, data, systems, connectivity).

****The Report Attack Surface activity (description, ownership, and RACI) is currently under review****

4.3 G. Threat Assessment (TSRA)

The Threat Assessment activity is a 'top-down' assessment of the key ICS Threat Scenarios that each global business, function and material geographic entity in the Group is exposed to. This activity identifies and assesses potential threats to the Group by defining Threat Scenarios and mapping key controls to mitigate these threats.
The TSRA Process describes how to:

- Identify threat vectors, threat actors and their intent and capabilities.
- Identify how threat actors may attack Bank's assets using defined threat scenarios with their kill chains;
- Associate threat scenarios with assets and risk subtypes to assess the inherent risk; and
- Assess controls that may prevent threat scenario from materialisation.

For more information regarding the detailed practices followed in the Risk and Control Assessment, please refer to the TSRA Methodology document.

4.3.1 Define Threat Scenarios

Threat Scenarios are a key component of the Threat Assessment, as they enable the identification of a discrete set of mitigating controls to be mapped and assessed. A Threat Scenario is a series of steps conducted by a Threat Actor with a particular intent, using one or more Threat Vectors that result in an impact to the business[7]. Threat Scenarios are reflective of the cyber threat landscape in which the Group operates and how the threat materialises will evolve in line with changes that occur across that cyber threat landscape.

Threat Actors and Threat Scenarios (including the Threat Scenario Library) must be reviewed and updated on at least an annual basis, with due consideration given to the threat landscape and Business context.

4.3.2 Assess Inherent Risk

The inherent risk (impact and likelihood) of each Threat Scenario must be assessed based on the impact assessment of relevant assets and analysis of real-world incidents (likelihood) in terms of proximity, prevalence and sophistication.
The inherent impact and likelihood of Threat Scenarios must be assessed at least on an annual basis.

4.3.3 Report Threat Exposure4

Threat exposure provides an understanding of the threats the Group faces. This includes the number of incidents of different types (e.g., near misses), learnings from external and internal incidents and developments in the threat landscape through the use of data visualisation and dashboards.
Threat exposure reports and country dashboards must be produced on a regular basis.

4.3.4 Map Controls to Threat Scenarios

[6] Activity under design / implementation

[7] There are a number of business-specific Threat Scenarios that can be developed for the Group. These are detailed descriptions of how a threat would materialise for a particular party of the Group. For more details regarding Threat Scenarios and their use within the ICS risk assessment process, please refer to the TSRA Methodology document.

Controls must be mapped to Threat Scenarios to help prevent, detect or correct relevant threat scenarios/vectors across the stages of the cyber-attack kill chain and impacts, defining the key controls that mitigate the Groups ICS risk.
Threat Scenarios and Vectors (which have been aligned with mitigating key controls and underlying metrics and effectiveness requirements) must be reviewed and updated on an annual basis.

4.4 H. Risk & Control Assessment (TSRA)

The Risk & Control Assessment is used to assess risks and controls by analysing threat exposure and controls effectiveness.

Assessing risk requires the careful analysis of threat, vulnerabilities in Information Systems and Technology Infrastructure, and control information to determine the extent to which incidents could adversely impact the Confidentiality, Integrity and Availability of Information Assets and Systems of the Group, and the likelihood that such circumstances or events will occur.

Any ICS risk identified must be assessed using the Group's Risk Assessment Matrix. The ICS risk assessment must determine the inherent risk rating, assess mitigating controls, and determine the residual risk rating. The residual risk rating will be calculated using the residual impact and likelihood ratings in alignment with the O&T RTF document. Similarly, the control assessment analysis is used to review effectiveness of existing controls for identified risks and implement new or enhanced controls as necessary.
The threat scenarios, their inherent risk ratings, and the identified mitigating controls, as derived from the Threat Assessment 'G' activity, must be used as part of the Risk & Control Assessment 'H' activity.

4.4.1 Risk & Control Assessment

The Risk & Control Assessment is performed to calculate the inherent and residual risk profile of the organisation (Business / Function / Country).

Any ICS risk identified must be assessed using the Group's Risk Assessment Matrix. Information security risk assessment must determine the Inherent Risk Rating, assess mitigating controls, and determine the Residual Risk rating. The residual risk will consider the risk reduction afforded by key controls to protect, detect, respond, and recover from the threat.
The inherent risk rating must be established at minimum once a year. Residual risk ratings, risk aggregation and prioritisation and ICS risk profiles must be established at minimum twice a year.

4.4.2 Horizon-scanning, Emerging and Thematic ICS Risk Assessment

Horizon-scanning is regularly conducted at a thematic level for Bank and industry developments in topical and emerging trends/technologies that may affect the likelihood and/or impact of ICS risk at the Bank in the next 1-5 years. This process produces a report to help the Bank proactively identify, track and prioritise topical and emerging ICS risk.

Emerging Risk Assessment is conducted on a trigger basis – either at management request or through prioritisation resultant of horizon-scanning activity. The activity is more in-depth than horizon-scanning activity and involves analysis of where ICS control gaps may exist for the topical or emerging ICS risk.

Thematic Risk Assessment is also conducted on a trigger basis at an in-depth level, to assess existing ICS risk themes and issues holistically across the Group. Such triggers may include management request or a material development internally (e.g. GIA finding) or externally (e.g. rapid acceleration of remote working during COVID-19 pandemic).

Any recommended actions emergent from the above processes should be formally tracked and managed via the established issue management process.

4.5 I. Control Testing & Risk Review

The Control Testing & Risk Review activity validates the effectiveness of controls based on:

- Design check (for ensuring the compliance of operational design with the ICS Standards control statement); and
- Operational effectiveness requirements (whether the control is deployed in line with the design/is executed effectively).
- Tiered levels of verification
- Key controls will be under formal controls testing.
- Other controls will be subject to periodic assurance reviews, red/purple team testing, vulnerability management etc.

Weaknesses must be communicated, with Treatment Plans (TP) and may be used to correct RR assessments.

4.5.1 ICS Control Testing

The ICS Control Testing process is an independent testing that is performed by ICS Control Testing team, which aimed to assess the design adequacy and operating effectiveness of Information Cyber Security (ICS) key controls as defined in the Risk Type Framework (RTF) for Information and Cyber Security (ICS). The ICS Control Testing process lifecycle comprises of phases of annual and sprint planning, testing execution, conclusions, quality checking and reporting. Identified control weaknesses /issues and risks behind them must be communicated and logged in the risk management tool (iTrack) and appropriate risk treatments agreed in accordance with the defined residual risk level. For more information regarding the detailed practices followed regarding the testing of controls, please refer to the ICS Control Testing Strategy and Approach document.

4.5.2 Third Party Security Assessments (TPSA)

TPSAs are ICS risk and control assessments of Third Parties which (a) access, process, store or transmit SCB data, and/or (b) access SCB systems/networks. TPSAs are performed throughout the lifecycle of the Third-Party relationship. Their purpose is to assess Third Party's ability to meet a set of minimum-security requirements as set out in the Third-Party Security Control Library.

For new-to-Bank Third Parties, for which ICS risk is identified as applicable by Supply Chain Management (SCM), TPSA must be conducted as part of the onboarding process.

For existing onboarded Third Parties the active Risk Identification Form (RIF) must be recertified annually. TPSA reassessments must be conducted with a frequency commensurate to Inherent Security Risk Ratings (ISRRs). If a material change in service provision (as described in the ICS Security in Interaction with Third Parties Standard) is identified during RIF recertification, TPSA reassessment must be conducted sooner, out-of-cycle.

The ISRR, TPSA Control Library and various forms of supporting material including Third-Party Independent Assurance Reports (e.g., SOC2) must be taken into consideration in TPSA.

4.5.3 ICS Assurance

Risk-focused, evidence-based independent assessments must be conducted by the 2LoD to validate and benchmark the effectiveness of key controls against industry peers and regulatory expectations.

Key controls, the control effectiveness principles (relevancy, accuracy, timeliness and coverage), 1LoD controls testing outcomes and the Risk-driven Second Line Assurance Plan must be used to produce workpapers, issues, reports and other relevant artefacts as required under the Assurance One Methodology. Control effectiveness reviews must be conducted on at least and annual basis.

For more information regarding the detailed practices followed regarding the testing of controls, please refer to the Second Line Assurance Methodology document.

4.5.4 Red Teaming

Red Team Operations are risk based, intelligence led, scenario driven assessments that simulate the actions of real-world cyber adversaries targeting the organisation. The goal is to assess the capability of the Bank to prevent, detect and respond to a cyber-attack targeting important business services and critical functions through compromise of key systems, data, and people.
For more information regarding the detailed practices followed please refer to the Red Team Operations Standard Operating Procedure.

4.5.5 Purple Teaming

The Purple Team conducts offensive testing exercises to validate control effectiveness and enhance the Group's cyber defence capabilities on detection, prevention, response controls and/or a particular scope/set of assets. Those tests are conducted ad-hoc, and are triggered by regulatory issues, response controls testing requests, business and technology changes or stress test issue validation.
The Purple Team activity is also referenced in Section 4.9.1. will also contribute ICS Assurance.

4.6 J. Capital Adequacy

This activity identifies the Group’s capital adequacy requirements as they relate to ICS risk i.e., the threat scenarios that should be modelled to support capital adequacy planning.

4.6.1 Capital Adequacy

At a Group level, the Pillar 2 assessment for ICS risk must be produced by Operational Risk with SME input from the Group CISRO function. This will be cascaded to Solo and Countries. Where Local Regulators have an approach that varies slightly to the above, local regulations should be followed. The Group CISRO can determine if any additional Pillar 2A add-on or reduction is required based on any material residual risk net of the inherent risk and the control effectiveness.

Adequacy must be measured annually to evaluate how much capital is available to the Bank. This understanding will help in determining how effectively the Bank can sustain the risk of financial insolvency.

ICS Risk Treatment (Mitigation) Sub-component

ICS Risk Treatment is the second sub-component within ICS Risk Management.
Risk treatment aims to reduce identified risks back within the Group’s appetite through the application of strategic, tactical, and operational measures. Risks can be modified through reduction, acceptance, avoidance, or transference.

4.7 K. Strategic Risk Treatment

The Strategic Risk Treatment activity defines risk treatment plans to bring residual risks within the desired risk tolerance level, through avoidance/termination, acceptance/tolerance, transfer/sharing or reduction.
ICS risk must be treated in alignment with the guidance provided within the O&T RTF, thus considering the following when determining how to treat an identified ICS risk:

- Risk Reduction (e.g., improve existing controls, process re-engineering, etc.)
- Risk Prevention (e.g., implement new controls, curtail business, etc.)
- Risk Transfer (e.g., insurance)
- Risk Acceptance (e.g., accept the risk where no action plan can be implemented)

4.7.1 Define Risk Treatment Plans

Risk Treatment Plans are strategic plans of activities which must be defined to help reduce elevated residual risks, so they are within the risk appetite of the organisation, taking organisational and budgetary constraints into consideration.

Treatment plans must define clear ownership and a target completion date. Where a treatment plan cannot be completed within the expected 'Target Completion Date', a justification must be provided to the appropriate approval Risk Committees for review.

Action Owners are responsible for the agreed remediation actions. This includes assigning and dedicating resources to complete the agreed actions within the designated timeframe, as well as to provide regular, at minimum monthly, progress updates to the Process Owners
Treatment Plans for their respective Elevated Residual Risks must be defined and reviewed according to the guidance and requirements set out by the Group Operational Risk Standard.

4.7.2 ICS Dispensations[8]

ICS dispensations must be raised if any requirements of Group Information and Cybersecurity Policy and related ICS Standards cannot be met, and if the residual risk of the non-compliance is assessed as 'Medium or above' in GRAM rating. This is aligned with the Group Operational Risk Standard.

4.7.3 TPSA Dispensations & Conditional Acceptances

TPSA Dispensation process is established to handle exceptions to the TPSA process for the following:

- Delay TPSA completion
- Signing of a third-party contract to be expedited prior to the completion of the TPSA or remediation of any known observations.
- Non-performance of TPSA
- TPSA observations:
    - Extend observation closure timeline.
    - Non remediation of TPSA Observations

4.8 L. Risk-based Cyber ICS Initiative Design & Operation

This activity defines and manages the ICS initiatives, that deliver on the risk treatment plans, in line with the Group's ICS risk and control strategy.
Approved ICS initiatives work must be determined on an annual basis (as a minimum) and on an ongoing basis as per New Ways of Working Investment Management Standard.

4.8.1 Investment Prioritisation

Financial and non-financial benefits from ICS investments must be defined and submitted for budget approval to prioritize investments.
Approved ICS investments and project work must be determined on an annual basis with monthly refinements (as a minimum).

4.8.2 Strategic Portfolio Governance

Strategic portfolio governance systematically remediates and addresses gaps, regulatory requirements, and audit issues through the portfolio of initiatives which are driven by risk reduction targets and treatment plans.

The 90-day backlog must be reviewed at the QPR, with due consideration given to the following:

- Backlog refinement planning
- RAID
- SDF artefacts and
- Initiative closure and remaining activities

[8] The description of ICS Dispensations activity is currently under review and will be aligned to the updated definitions proposed by ERM and overall guidance to be proposed for ICS issue management process in ICS RTF / Risk Management standard.

4.9 M. Tactical Continuous Risk Reduction

This activity performs continuous assessment of control effectiveness, including control owner self-assessment, and through attack simulations that cut across risks, controls and their treatment plans, and measure the Group's ability to prevent, detect and respond from real-life threat scenarios. This includes agile and continuous tuning of controls in a tactical manner (i.e. do not require a strategic programme or project to deliver the risk reduction).

4.9.1 Purple Teaming

The Purple Team conducts offensive testing exercises to validate control effectiveness and enhance the Group's cyber defence capabilities on particular detection, prevention, response controls and/or a particular scope/set of assets. Those tests are conducted ad-hoc, and are triggered by regulatory issues, response controls testing requests, business and technology changes or stress test issue validation.
The Purple Team activity as previously referenced in Section 4.5.5 will also contribute to tactical continuous risk reduction.

ICS Risk Monitoring & Reporting Sub-component
ICS Risk Monitoring & Reporting is the third sub-component of ICS Risk Management. Its purpose is to continuously monitor ICS risks against appetite and risk objectives, and to report the Group's current ICS risk posture, and the benefits delivered through improvement activities.

4.10 N. Risk Monitoring & Reporting

This activity continuously monitors and demonstrates that residual risk is managed in line within the business risk objectives and appetite, supporting the right prioritisation of initiatives and investment to improve the key controls, as well as reporting on control effectiveness, the organisation's risk profile and risk posture.

ICS Risk must be monitored and reported in adherence with the Group's Risk Data Aggregation Standards, Risk Reporting Standards and Data Quality Management Policy (and underlying standards) to meet the Group's risk reporting requirements.

4.10.1 Risk Monitoring

2LOD must perform oversight and challenge of the 1LOD risk management activities. Risk-focused and evidenced-based monitoring reviews must be carried out to provide confidence to the Senior Management and the Board that 2LOD validate and review the effectiveness of the internal controls in a methodical manner.
ICS risk monitoring must be performed on an on-going basis to inform operational, strategic, and tactical risk decisions, with due consideration given to the ICS risk appetite, risk profiles, Risk Treatment Plans (RTPs), ICS metrics, risk fora and dispensations.

4.10.2 Risk Reporting (key risks, capabilities, metrics)

Regular risk profiles must be produced for Group, Business, Functions, Regions, and Countries, using the ICS Risk Category profile format. ICS risks must be reported in a central repository, such as a risk register (where they can be reviewed, monitored over a period of time and compared with other risks and related treatment decisions).
Risk reporting must be conducted regularly in line with frequency defined by the ERMF and ICS RTF, and with due consideration given to risk profiles, RTPs and ICS metrics.

4.10.3 Board Risk Appetite Metrics - Reporting Preparation & Distribution

Production and distribution of the BRAMs and breach notifications to the Board.
The reporting preparation and distribution for the ICS BRAMs must be conducted in line with frequency defined by the ERMF.

4.10.4 ICS Risk Reporting to Risk Committees

Regular updates regarding the Group ICS Risk Profile and BRAMs must be made to the relevant Group Risk Committees and the Board. This includes the delivery of ICS Governance Committee submissions and determining the priority reports and critical risk measures required to identify, monitor, and report on the Group's material risks.
Management Information (MI) and Group Risk Committees and Board submission must be established in accordance with committee timetables.

4.11 O. ICS Risk Reduction Monitoring & Reporting (Benefits Realisation)

This activity reports on the risk reduction benefits delivered by strategic and tactical improvement activities on an ongoing basis as and when they are delivered. Such reporting occurs on a more frequent and dynamic basis than those defined in the Risk Monitoring and Reporting activity (N), and at a more granular level of detail not suitable for risk committee consumption.

4.11.1 Validate Risk Reduction

ICS 2LoD provides an oversight to ensure that 1LoD risk reduction activity undertaken as part of agreed ICS ERR Treatment plans results in effective Group risk-buydown to keep the Group ICS residual risk within the appetite.

4.11.2 ICS Value Management

The Value Management activity is the process through which value (financial and non-financial) is identified, owned, approved, maintained, measured, realised, and signed off.

ICS must define the Scorecard, which shows the financial and non-financial targets to be achieved over the next 1 and 3 years and Refinement Forums must be responsible for prioritising initiatives which deliver business value aligned to these scorecards. The financial benefits RAG and benefits reporting to TTO RF and MT must be established on a quarterly basis, with due consideration given to the target state and current baseline.

4.11.3 Group ICS Risk Profiling and Reporting

This activity must be undertaken to understand what the organisation's residual risks is and produce ICS Group Risk Profiles and Group Risk Reduction timelines based on the agreed Group ICS Aggregation Methodology. This includes the provision of executive summary reports for GNFRC and reports to GRC as required (via Group Enterprise Risk Management Team).

5 ICS RISK TRAINING & EMBEDDING ICS RISK CULTURE

Component Overview

The ICS Risk Training & Embedding of ICS Risk Culture component raises awareness of ICS risks, threats, as well as staff responsibilities in line with requirements defined in ICS RTF, ICS Policy and Standards. It also establishes and maintains an ICS risk culture which improves staff behaviours and aids appropriate risk decisions. This is supported by a structured training and awareness programme, that demonstrates what is employee role in protecting the bank, how to act as a human firewall or what good risk culture means.

5.1 P. ICS Risk Training & Awareness

The ICS Risk Training & Awareness activity provides training to employees to educate them on the ICS risks and threats they and the Group face, and their obligations as defined in the ICS policies and standards. This complements the broader ICS Training and Awareness undertaken across the organisation.

5.1.1 ICS RTF (ICS RM&G) Training and Awareness

This activity is undertaken to reduce the risk of a breach of CIA of information assets due to a lack of ICS risk training and awareness. it provides awareness of the end-to-end activities undertaken to manage ICS risks in line with the ICS RTF.

The Group ICS Training & Awareness Standard (*stored on the GovPoint portal*) also lays out the requirements of how training and awareness is conducted in the Bank for all employees including Non-Employed Workers and Third Parties in order to minimize risk exposure to the Bank.

5.1.2 ICS SME Training (ICS Risk Practitioner Learning)

This includes focused subject matter expert (SME) training aimed at 1LoD and 2LoD colleagues that undertake key tasks in the downstream processes e.g., TSRA, executed for the management of ICS risk. Such SMEs include 1LoD ISROs and 2LoD ISROs.
This activity also ensures ICS Risk Practitioners are aware of their obligations and conversant with the Bank's risk management and governance approach set out in the ICS RTF, policies, and standards in order to discharge their risk management responsibilities.

5.2 Q. Embedding ICS Risk Culture

This activity defines and measures the ICS risk culture of the Bank and develops interventions that improve behaviours of all staff and particularly key risk management personnel.

5.2.1 Define & Implement Risk Culture (as applied to ICS)

This sub-activity defines risk culture as applied to ICS and outlines the expected desired behaviours that uphold a healthy risk culture. This enables the Bank to build trust and drive sustainable value for our stakeholders. Embedding of risk culture as applied to ICS will include:

- Ensuring clarity of roles and responsibilities in ICS risk management processes
- Uplifting ICS risk management knowledge to perform these roles and responsibilities
- Provisioning of behavioural guidance to enable employees to do the right thing
- Ensuring continuous discussion on ICS in business and governance forums
- Employing Bank-wide platforms to recognise employees who demonstrate positive risk culture behaviours as well as managing those who show indifference or wilful disregard for risk culture expectations

Risk culture as applied to ICS must have metrics to measure performance against expectations, including indicators to track ICS risk management behaviours, risk practitioners' knowledge levels and employee cyber hygiene behaviours. Risk culture appetite thresholds should be set and reported to Board and Group MT. At country risk forums, relevant risk culture performance metrics should be discussed at least twice a year.

6 APPENDICES

6.1 Risk Sub-Types (Categories)

Risk Sub-Type	Description
Financial Loss by External Attacker and/or Trusted Insider	Cyber-attack causing direct financial loss to the Group, caused by either trusted insider or external attacker and targeted on the banks' IT environment using access abuse, hacking, malware and/or social engineering. Primary impact: Integrity Secondary impact: Availability
Disclosure of Sensitive Information by External Attacker and/or Trusted Insider	Leakage of the Group's sensitive information caused by either trusted insider or external attacker and targeted on the banks' IT environment using access abuse, hacking, malware and/or social engineering. Primary impact: Confidentiality

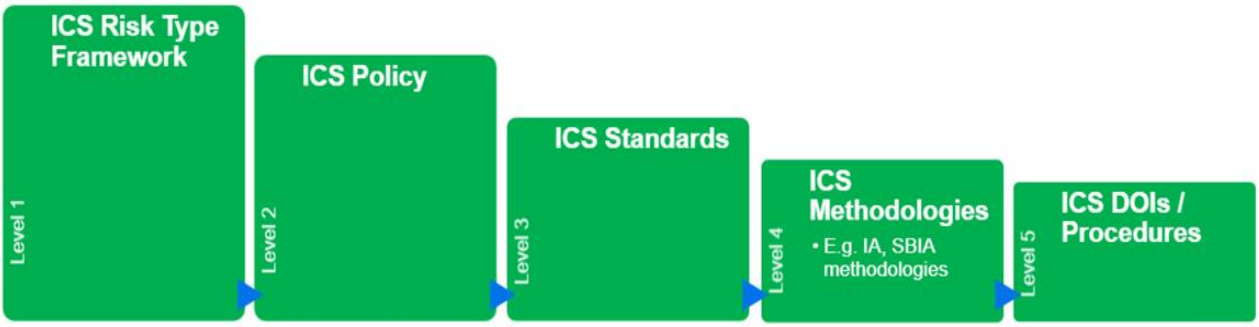
Disruption of Business Operations by External Attacker and/or Trusted Insider	Disruption of the Bank's operations caused by either trusted insider or external attacker and targeted on the banks' IT environment using access abuse, hacking, malware and/or social engineering. Primary impact: Availability Secondary impact: Integrity

6.2 Threat Vectors

Threat Vector	Description
Malware	An attack that uses malicious software, specifically designed to harm a computer, a system, or data, to compromise an organisation's Information System/Technology Infrastructure. It usually appears to perform a useful function, but instead executes other malicious logic. Examples of malware include: trojans, virus, spyware, worms, ransomware, keyloggers, etc.
Web-based attacks	An attack that leverages web-based systems and services to compromise an organisation's Information System/Technology Infrastructure. The outcome of such attacks includes attacking web infrastructure, infection of browsers / web activity, stealing of web tokens, and the theft of personal information within web application databases.
Denial-of-Service	An attack that seeks to make a machine or network resource unavailable to its intended user. This attack could originate from internal or client-facing systems owned by the organisation or external systems owned by third parties.
Privilege Misuse	An attack that uses authorised privileged credentials to compromise an organisation's Information System/Technology Infrastructure. These credentials could be obtained by an insider, who is an employee (existing or offboarded), contractor, vendor; or an external party to the organisation
Phishing and Social Engineering	Phishing refers to the use of electronic means (e.g., fax, email, forums) or phone calls, that appear to originate from a trusted source, to trick a victim(s) into, among other things, clicking on a malicious link or documents, permitting access to secured areas or divulging confidential information. Social engineering refers to the use of psychological manipulation (e.g., lies, impersonation, blackmail, bribes) to trick a victim(s) into, among other things, clicking on a malicious link or documents, permitting access to secured areas, or divulging confidential information.
Compromised Credentials	The use of compromised of credentials (including weak credentials) to gain the initial access to corporate networks is still very predominant in the current threat landscape and one of the most common types of initial access. Threat actors compromise victim credentials through phishing, insides, malware, brute-force or often can buy dumped credentials in the dark-net from a previous compromise.
Misconfiguration	Misconfiguration is mostly a human-led modification of system configurations that weakness the system configuration and/or gives too many privileges making the information/system vulnerable to unauthorized access. A default

	password can be considered a very common misconfiguration. This is one of predominant type of breaches in cloud environments, as the configuration can be easily made available to the internet.
Supply Chain Compromise	An attack that exploits vulnerabilities in the 3rd Party hardware, software, operating systems, peripherals, or services used by an organisation, to compromise the organisation's Information System/Technology Infrastructure.
Vulnerability Exploitation	An attack that exploits the inherent weaknesses or misconfigurations in an information system to compromise an organisation's Information System/Technology Infrastructure.
Lateral Movement	An attack in which the access to one asset is used to explore and subsequently move through a network. It may involve pivoting across several Information Systems to reach the eventual target.

6.3 ICS Risk Taxonomy



Terminology	Definition
Framework (RTF)	Documents at a high-level risk management principles, risk subtypes, risk appetite (RA), second line processes for oversight and challenge, key first and second line roles and responsibilities, decision making authorises, delegation of authority, regulatory obligations and approach to risk assessment, identification, and monitoring against RA.
Policy	A policy is designed to control and mitigate a distinct set of critical risks through mandatory policy statements. Policy statements must be principle based statements that are actionable, through key control requirements or with expected outcomes.
Standard	Standards are operational documents to implement the requirements set out in this Frameworks or Policies.
Methodology	High-level description of 'how to principles' to support implementation of a Framework, Policies or Standard.
Department Operating Instructions (DOI) / Procedures	Define how Policies and Standards should be executed within their department.

6.4 ICS Control Library definitions (aligned with ICS Risk Taxonomy)

Control Level	Definition
L1 – SCB ICS Policy	A reference to the ICS Policy and the requirement(s) that the Control is aiming to implement.
L2 – SCB ICS Standard Statements	A reference to the relevant standard statements that the Control is aiming to achieve compliance against.

L3 – ICS Control Objectives	A Control objective outlines the outcome intended by one or a suite of Controls in the context of the risk and threat being managed.
L4 – ICS Actual Controls	The specific local implementation / occurrence of a Control on an asset or process, and the associated activities.

NOTE: Control definitions must have globally consistent definitions of design effectiveness. Their implementation (i.e., level 4) may be both centrally provisioned and consumed by asset owners or federated to individual asset owners in their entirety.

6.5 Cyber Attack Kill-chain

The elements of the cyber-attack chain include:

- Pre-Attack: the first stage in which targets are identified and reconnaissance is performed.
- Weaponisation: development of tools that will be used in an attack, such as malware.
- Delivery: the 'transmission' phase in which the 'weapon' is delivered to the target through, for example, spear phishing or an attack in Internet facing services.
- Exploitation: the attacker starts to execute malicious code and exploit weaknesses or vulnerabilities, such as performing an external denial of service attack or an insider abusing their privileges to gain unauthorised access to an asset.
- Installation: the attacker can begin to install malicious files or malware on the target's systems, this could include elements of the supply chain such as Group application software.
- Command and Control: a channel is connected from the target system to attacker- controlled infrastructure.
- Action on Objectives: the final phase in which the attacker is able to remotely start achieving its ultimate goal such as extracting sensitive data.

6.6 Roles & Responsibilities (RACI)

Accountabilities and responsibilities for the activities described in the ICS Risk Management Standard are reflected in the ICS Roles & Responsibilities (RACI) document.
The RACI is maintained as a 'live document' with periodic updates applied to reflect changes in values (accountable, responsible, consulted and/or informed). The RACI is also mandatorily updated in parallel with the standard.

This document is available in the supporting materials section of the ICS Risk Management One Stop Shop Portal via the following link:
https://standardcharteredbank.sharepoint.com/sites/onestopshop/SitePages/Supporting_Materials.aspx

6.7 Glossary

ICS Glossary of terms is available via the following link:

Governance Libraries - Glossary of Terms - Glossary of Terms (sharepoint.com)