Security in Interactions with Third Parties

Version No	4.2
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	04/12/2024
Effective Date	16/12/2024
Next Review Date	31/07/2027

Table of Contents

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	4.2	04/12/2024	16/12/2024

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

1. INTRODUCTION AND SCOPE

The objective of this Information and Cyber Security ("ICS") Standard is to ensure protection of Group Information (Information and/or data owned by the Group) that is prone for ICS risk exposure in a Third Party ("TP") arrangement.

TPs typically form part of the Group's extended network and is therefore vital that the Group Information are equally or adequately protected by a TP which is allowed by the Group for possessing, otherwise stores, processes, transmits and/or manages the Group Information.

Through this ICS Standard, the Group sets out the direction and approach to be followed and adhered to in the life cycle management of TPs (includes Cloud Service Providers) who may be allowed for processing/managing the Group Information and/or the underlying Technology Assets within which the Group Information may be maintained.

This ICS Standard is important as TP compliance to our security controls reduces the risk of Security Incidents and helps ensure that the Group maintains the trust of its Customers/Clients and all relevant stakeholders. It also helps to identify areas where these TPs do not meet our requirements so that appropriate risk assessments can be carried out for a risk decision.

Note: This ICS Standard must be read and followed in conjunction with the Group Third Party Risk Management ["TPRM"] Policy framework and Group Contract Policy.

1.1. Risks

Failure to adopt and implement this ICS 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 ICS Standard must be read, and selection of relevant controls to be in conjunction with all other ICS Standards.

The term 'Third Party' follows the definition in Group TPRM and considers under same definition for any Group Information and/or Data processing/maintenance service that an external Third Party provides to the Group. This ICS Standard considers the Group's Third Party as a primary party responsible for the security of Group Information that the TP possess or otherwise store, process, or transmit on behalf of the Group, or to the extent that they could impact the security of the Group Information in the supply chain.

This Standard also to be applied in situation wherein there is a connectivity between a TP service provider and the Group end with no involvement of Group Information, but the Group may only receive or subscribe to its services for internal purposes. Such connectivity has potential for Cyber threat intrusions or attacks and hence subject to this Standard.

The ICS Standard is mandatory and applies to the Group Businesses, Functions, Countries, and/or 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.

2. ROLES & RESPONSIBILITIES

Information System Owner

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

Technology Infrastructure Owner

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

Application Owner

A named individual accountable for the protection of owned Applications and for compliance with applicable Control Statements within this ICS Standard.

Process Owner (PO)

A named individual accountable for the delivery and for compliance against applicable Control Statements within this ICS Standard.
TPSR – Third Party Security Risk ("TPSR")
Group Legal
SCM – Supply Chain Management ("SCM")

Contract/Service Owner

Contract Owner (Service Owner in Redux) must read this ICS Standard in conjunction with the Group TPRM Policy and its Standard and is responsible for ensuring that the ICS requirements are covered during the establishment, duration, and termination of the business relationship with the Third Party service provider. All other responsibilities shall refer to Group TPRM Policy & its Standard.

People Leaders

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

Group CISO

Group CISO must establish and maintain the Group's core ICS capabilities of threat intelligence, protection, security incident detection, response, recovery, assurance, and governance capabilities in relation to the management of Third Parties with TPSA Inherent Security Risk Rating ("ISRR") of Critical or High and/or those supporting SBIA-5 Information Systems.

CISO ICS Standards & Controls

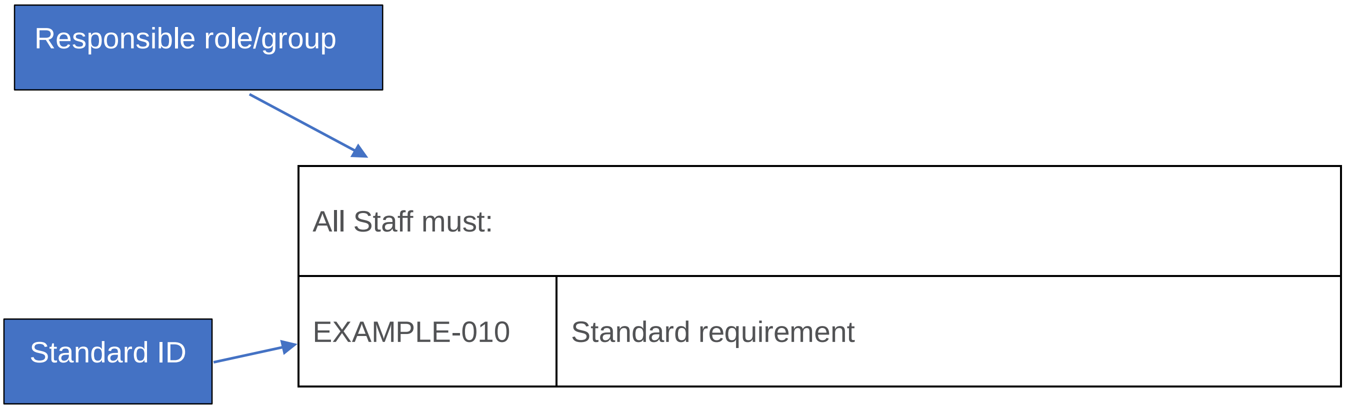
The CISO is the owner of this Information Security Standard and will ensure the document is updated to an agreed schedule.

***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 ICS Standard. The requirements are set out in the following format:



Responsible role/group

All Staff must:

Standard ID

EXAMPLE-010

Standard requirement

3.1. Control Area: Third Party Security Risk

Process Owner [TPSR] **must**:	
STP-010	Establish a formal process for assessing the ICS risk and controls of TPs and ensure the process is communicated.
STP-015	Deploy the process that covers at minimum the following: a) To define an approach for assessing ICS risk and controls in a TP arrangement. The approach to include criteria for triggering TPSAs which includes onsite/offsite assessment and any other. b) To determine and document Scope of process applicability. c) To embed the process within the Group’s upstream TP arrangements for a preliminary ICS risk identification and risk assessment applicability. d) To define and document any ‘Out of Scope’ TPs along with rationale and in consultation with the CISO and OTCR. e) To review the process, scope of applicability and out of scope at least once in a year. f) To own, define and maintain minimum ICS requirements in consultation with OTCR and Group Legal. g) To have a mechanism that monitors performance of TPs in Scope against agreed ICS requirements and report any key risk identified to relevant stakeholders.
STP-016	Define minimum ICS requirements that supports protecting Confidentiality, Integrity and Availability of Group Information in a TP arrangement. The requirements to be maintained up to date and to include the following at the least: a) The ICS controls at TP end including their security Policy and/or Standard(s). b) ICS requirements, as applicable according to the process triggers, to be in alignment with the Group’s ICS Policy and Standards.

STP-030	Conduct assessment of ICS controls relevant to the TP arrangement. The assessment to cover: a) The life cycle handling (e.g., creation, processing, storage, transmission, and destruction) of Group information, Information Asset and Information System impacted by the arrangement. b) The Information flow in the supply chain (this includes identification of sub-contractors, other external parties and assessment of controls applied by the TP over the supply chain). c) Emerging ICS threats, where relevant. d) Documentation of ICS control gaps (post assessment), their impact/criticality rating (e.g., Low, Medium, High) and an agreed action plan along with action ownership.
STP-060	Inform relevant stakeholders on the outcome of TP ICS risk and controls assessment highlighting potential implications, if any to the Group.
STP-070	Ensure TPSR includes a review of all relevant regulatory requirements during the course of each assessment.

Contract/Service Owner **must**:	
STP-090	Ensure the ICS risk and controls are assessed on the TP arrangement (to cover sub party, if any, in the supply chain) for any or all of below conditions: a) Prior to TP's allowed accessing Group Information Assets, Information Systems and/or Technology Infrastructure. b) Whenever there is a change to current scope of services which has an impact on Group Information. c) Prior to renewal of TP arrangement. *[Reference STP-030]* *Note: Where an onsite assessment is recommended by the CISO TPSR, the same must be supported.*
STP-091	Ensure that identified control gaps from the TP ICS risk & controls assessment are remediated by the TP with a priority to high & medium control gaps. [Reference STP-060]. *Note: For any ICS dispensation related, example TPSA not performed, non-remediation of TP ICS control gaps and so on, to follow Section 4.2 of this Standard document. These to be fulfilled before allowing the TP accessing the Group Information.*
STP-095	Recertify annually all their TP engagements having ICS risk exposure. *Note: Where applicable, the annual recertification may trigger a more detailed ICS risk assessment on a TP which must be completed too.* *[Reference STP-030]*

STP-100	Re-assess the ICS risk of TP control environment for any or all below conditions: a) The processing site has changed. b) The TP has changed ownership. c) The rating of the Information Asset being processed by the TP has moved up to a '5' or a '4' as per the Information Asset register. d) A TP Security Incident has been reported (including sub party, if any). e) A change or proposed change impacting the Group's security posture in relation with the TP. f) A TP handling payment card data (requires annual compliance checks). g) Change in the data flow/architecture. *[Reference STP-030]*
STP-105	Ensure the following minimum details related to the Group Information Asset, Information System and/or Technology Infrastructure which are TP hosted/managed are maintained in an ICS TP register: a) TP Service Description b) Status of TP Service (ex. Active/Inactive) c) Contract/Service Owner d) Group Information/Data covered in TP Service along with Owner and if available, Delegate e) TP contact [useful during security incident co-ordinations]

People Leader **must**:	
STP-110	Ensure that Staff who engage with a TP adhere to the TPSR process. *[Reference STP-010]*

3.2. Control Area: ICS Requirements and Legal Protection

Process Owner [Group Legal] **must**:	
STP-120	Where relevant, include appropriate legal language in a TP arrangement addressing applicable (w.r.t ICS Clauses in the Regulatory Schedule and ICS Schedule) ICS requirements (including for any cross-border sharing risk). *[Reference STP-016]*
STP-130	Where relevant, include appropriate legal language addressing Country specific ICS Legal, Regulatory and Mandatory ("LRM") requirements.
STP-235	Where relevant, include appropriate legal language in a TP arrangement, including termination rights and a right to the return of Group Information & related properties (e.g.., physical access token, Group IT Assets and where applicable) whenever a security incident breaches the Group's ICS risk appetite/threshold.

3.3. Control Area: ICS Requirements in TP On-boarding

Process Owner [Group SCM] **must**:	
STP-135	Support integration of ICS TPSR Process into the Vendor on-boarding process before a Vendor starts processing/provides maintenance services of Group classified Internal/Confidential/Restricted Information and/or for system interface or connectivity between the Vendor and Group system. *[Reference STP-015]*

Contract/Service Owner **must**:	
STP-140	Ensure the ICS requirements are included at the on-boarding stage of a TP arrangement that involves processing/maintenance service of Group Information (e.g., Request for Proposal [“RFP”]).
STP-080	Ensure before any disclosure of or grant of access to Group Information to a TP, appropriate legal agreement is put in place. [Reference STP-120] *Note: This includes for any one time sharing such as for Proof of Concept (“POC”). Such sharing to follow the Group’s Information Classification and Information Handling protection requirements.*
STP-150	Ensure TPs formally agree to: a) manage and maintain securely the Group Information and/or Group Information processing systems. b) permit audit/assurance checks by the Group and/or its authorised representatives throughout the TP arrangement period.
STP-170	Ensure any changes [including any emergency and/or exceptional changes] impacting the Group Information are notified by the TP in advance and are formally reviewed and approved by Group / Country ICS, Legal, Compliance teams.
STP-180	Ensure TP-owned laptops and Mobile Devices are not connected to the Group’s network when TP Staff are working within the Group’s premises. *Note: When required to access Group Information Systems, the TP Staff must be issued with Group approved laptops and/or desktops, and on-boarded as Non-Employed Workers [NEWs].*
STP-185	Ensure Roles and Responsibilities between the Group and the TP (e.g., Cloud hosting, record management arrangements) are defined, documented and maintained.
STP-210	Ensure that the TP have a security incident reporting process (to cover their sub parties/supply chain, as applicable) to a standard and design acceptable to the Group and that any incidents involving Group Information Assets, Information Systems or Technology Infrastructure and/or Group Information processing facilities must be immediately reported to the Group. *[Reference: ICS Standard Security Incident Response and Management]*
STP-220	Ensure that the TP takes appropriate steps to immediately address security incidents, and will cooperate with the Group’s authorised representative, with respect to the investigation of such incident(s). *[Reference STP-105]*

STP-230	Ensure that the TP share with the Group of any concern/observation/feedback from any regulators that the Group need to be aware of.

3.4. Control Area: On-going Monitoring

Contract/Service Owner **must**:	
STP-240	Ensure that TPs follow Group communications, advisories concerning the security of Group Information Assets, Information Systems and Technology Infrastructure.
STP-250	Ensure that the TP does not make or permit any statement concerning any Security Breach/Incident impacted the Group Information without the authorisation of Group Legal and Group Compliance. *Note: The exception would be to law enforcement agencies as required by law and regulators.*
STP-260	Ensure that the ICS control requirements as agreed by the TP are validated to determine the adherence, adequacy and for effectiveness. Any key risk outcomes to be reported via regular ICS governance channels.
STP-265	Perform regular (6 month) reviews of ICS controls as part of service review meeting with vendors with TPSA risk rating of Critical / High or those supporting Crown Jewel Information Systems (to cover the period in between TPSAs).

3.5. Control Area: Exit / Termination of TP arrangement

Contract/Service Owner **must**:	
STP-270	Follow Group defined process to securely handle the exit/termination of TPs and ensure: a) Revocation of TP access to Group's Information and Group Information processing systems, as per the Group Information and Cyber Security Policy and Standards or as agreed. b) Return or transfer of Group's Information and Group Information processing systems (including backup copies) or Secure Dispose in line with the Group's Information and Cyber Security requirements and obtain a certificate of destruction signed by a valid authority. *Note: Valid authority is a named person holding authority to sign destruction certificate for the TP. [Reference: Secure Decommissioning and Destruction Standard]*

3.6. Control Area: Third Party and Technology Assets Information Systems Applications and Technology Infrastructure

Information System Owner **must**:	
STP-290	Ensure that TP owned, supplied, or developed Technology Assets and/or Services are security assessed (including for security architecture) before technology on-boarding in the Group. This assessment preferably to happen alongside ICS risk and controls assessment of a TP (ref. STP-030) for addressing together. *[Reference: Applications Security Standard & Secure Configuration Management Standard]*
STP-300	Ensure that the TP provides security assurance before production roll out and annually on an Application supplied to the Group through demonstration of secure development practices, Application vulnerability tests and at a minimum demonstrated compliance against OWASP top 10 vulnerabilities and SANS 25 programming errors. *[Reference: Application Security Standard]*
STP-310	Ensure TP controlled environments used for Application or software development for the Group are compliant with Information security best practices and must have documented independent audits or established compliance roadmaps in alignment with Industry Standard Certifications for Information Security (for example: SSAE18 SOC 2 reports, ISO27001/2, NIST Cyber Security Framework, FIPS 140-2 etc.). *[Reference: Application Security Standard]*

4. INFORMATION & SUPPORT

4.1. General Information and Support

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

4.2. Reporting Non-Compliance

As a general guideline, any non-compliance against the Applications and underlying Technology Infrastructure in CMDB should follow the ICS Non-Compliance Register (ICS NCR) process. Further assessment of these non-compliance should follow the issue management process, i.e. iTrack for issues with remediation plan or ICS Dispensation when there is an explicit decision not to remediate the issue.

4.3. Breach of this Standard

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

5. GLOSSARY

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

6. REGULATORY / INDUSTRY REFERENCES

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

7. Version Control Table

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISO Policy	Annual review includes: 1. Migrated existing standard to ERM standard template. 2. The existing Security in Interactions with Third Parties Standard document has been uplifted into this standard. 3. Consultation feedback, corrections incorporated	-	Liz Banbury	1.0	21-Dec19	21-Dec-19
CISRO Policy	New control for Contract Managers (STP265). Updates to R&R section to better reflect 1LOD and 2LOD activities	Non-material	Liz Banbury	1.1	30-Mar21	30-Mar-21
CISRO Policy	Updated (after additional stakeholder feedback) control for Contract Managers (STP265) and R&R section to better reflect 1LOD and 2LOD activities	Non-material	Liz Banbury	1.2	28-Apr21	28-Apr-21

CISRO Policy	Annual Review: Updated risks & paragraph 4. Cloud Services Standard merged. New – STP-105 & STP-235 Modified – STP-010, STP-030, STP-040, STP-050, STP-080, STP-090, STP-120, STP-150, STP-170, STP270, STP-300. Removed – STP020, STP-160 & STP-190	Material	Liz Banbury	2.0	08-Jun21	08-Jun-21
CISRO ICS Policy	Template update to ERM Standard template v5.6 Included the first 2 ICS risk subtypes in line with the ICS RTF v5.0 Changes made w.r.t ICS Policy Change Requests – ICSCR-12Apr2022-1 – Out of Scope removed, STP-010, STP-100 & Replaced Appendix 7.1 with New STP-095. ICSCR-14Jul2022-3 - Enhancing Third Party Assessment with Security Architecture & Engineering – STP-100 & STP290.	Material	Paul Hoare Head, ICS Policy and Best Practice	3.0	08-Mar23	08-Mar-23

CISRO ICS Policy	Uplift of Standard addressing R&R of the ICS LoDs - ICSCR14Oct2022-1 & the control statements are rearranged, consolidated where possible and strengthened where necessary to enhance the current understanding, coverage of ICS Third Party ("TP") risk.	Material	Paul Hoare Head, ICS Policy and Best Practice	4.0	03-Jan24	03-Jan-24
Arti Singh [ICS Standards]	Administrative changes introduced to update document template, references, roles and ownership.	Non-material	Jamie Cowan Head, ICS Risk Framework & Governance	4.1	04-Dec24	16-Dec-24