Vulnerability and Security Patch Management Standard

Version No	5.2
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	Katarzyna Maria Wencka
Document Contact Job Title	Director, 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

Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Katarzyna Maria Wencka	Vulnerability and Security Patch Management Standard	Non-Material	Jamie Michael Cowan	5.2	04/12/2024	16/12/2024

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

1. INTRODUCTION AND PURPOSE

This Information and Cyber Security Standard defines the minimum set of requirements for the selection, application, and operation of Vulnerability Identification and Management controls in the bank. The Standard also covers mandatory requirements for the Security Patch Management, which strictly corresponds with the Vulnerability Identification and Management control area.

The key objectives of the Vulnerability Management are to ensure that:

1) Vulnerabilities are identified in line with predefined frequency considering acceptable 'window of exposure',
2) Only approved and agreed methods and tooling are used for vulnerabilities identification to make sure the results of such a security testing are reliable and deliver expected results,
3) Vulnerabilities are remediated in line with the predefined timelines and considering criteria for remediation (such as criticality of the Vulnerability or the Technology Asset impacted) and adequately risk managed,
4) Vulnerabilities are being tracked and reported through their lifecycle, i.e. from identification to remediation.

Security Patch Management is a control area, that strictly corresponds with the Vulnerability Identification and Management. Security patching is one of the methods of Vulnerability remediation, thus the effective alignment of Secure Patch Management with Vulnerability Management is a must.

Security Patches must be correctly identified, prioritised, acquired and validated to make sure they are deployed in timely manner and corresponding Vulnerabilities can be closed.

In addition to the above, Security Patch Management can also be considered as a proactive approach, being continuously delivered, so the affected Technology Assets can be patched even before the presence of the Vulnerability is identified via Vulnerability identification activities.

Both Vulnerability and Security Patch Management, when maintained and delivered effectively, reduce the risk of the ICS threats materialisation due to technology flaws or defects.

1.1. Risks

Ineffective management of the technology Vulnerabilities and Security Patches may lead to a breach to the confidentiality and availability of data and Group Technology Assets 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, especially with the ICS Secure Configuration Management Standard and Secure Asset Management Standard.

In addition to the above, this Standard corresponds with applicable controls of ENTERPRISE SYSTEM DELIVERY LIFECYCLE Standard and Enterprise IT Service Operations Management Standard, defining the requirements for technology changes authorisation and delivery.

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 or used by the Group's Information System [wherever the term 'Systems' or 'Information System' is used in a control statement it also refers to the applicable Information System components, such as Technology Infrastructure or Application].

The identification and management of incorrect configuration is conducted in line with the requirements as defined in the Secure Configuration Management Standard.

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

Note: *Target and factual scope of Vulnerability Management is defined in line with the Vulnerability Management Strategy and Process.*

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 with applicable ICS controls defined in ICS Standards.

2. ROLES & RESPONSIBILITIES

Information System/Application/Technology Infrastructure Owner

(*also referred as Technology Asset Owner*)

A named individual accountable for (1) the protection of owned Information System, Application or Technology Infrastructure (respectively) and (2) for compliance with applicable Control Statements defined in this Standard and (3) for maintaining the accuracy of Technology Asset Inventory (crucial for effective Vulnerability Management ("VM") and Security Patch Management ("SPM") delivery) in line with the requirements of the Secure Asset Management Standard.

Process Owner (PO)

POs (as defined by the Enterprise Risk Management Framework) are Business or Function managers responsible for the end-to-end business or function processes as identified within the Group's Process Universe.

They are responsible for identification and management of the end-to-end process as defined in the Group's Process Universe and associated risks, including ICS related activities as mandated by the Standard. In the context of this Standard, they are also accountable for defining the approach and strategy (i.e. the plan of actions designed to achieve the Standard objectives) for applicable ICS control areas.

The PO is responsible for ensuring the provision of quality, timely, and adequate 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 (as defined within the Process Owner accountabilities, in line with applicable ICS controls of this Standard) to support Information Asset/System/Technology Infrastructure Owners to deliver required objectives of the Standard.

Operation Technology Cyber Risk Coverage (OTCR Coverage)

The OTCR coverage, in the context of this Standard, provide independent challenge, guidance and oversight of the effectiveness of the ICS controls to support the successful execution of the Group wide Vulnerability and Patch management strategy.

Group Chief Information Security Office (Group CISO) Group CISO is responsible for:

- Complying with the control areas of this Information Security Standard which are applicable to them.
- 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 holder, the Group CISO will additionally perform effectiveness reviews to monitor first line compliance with this Information Security Standard.

CISO ICS Standards & Controls

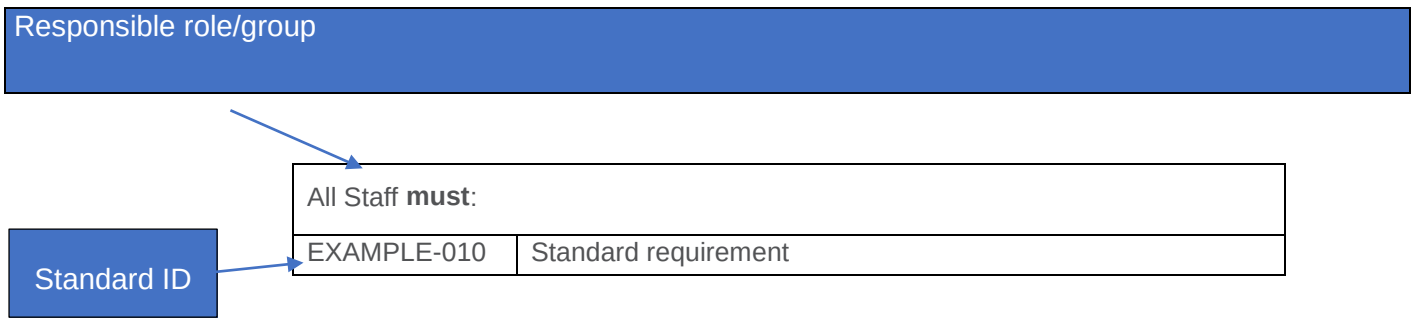
The CISO is the owner of this Information Security Standard and will ensure the document is updated to an agreed schedule.

***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:



3.1. Control Area - General Provisions

Group CISO **must**:	
VPM-010 *[new]*	Establish an operational definition to the approach to Vulnerability and Security Patch management by: 1) establishing process(es) for Vulnerability Management [VM] and Security Patch Management [SPM], 2) appointing Process(es) Owner(s), 3) defining a model for Process(es) effectiveness, oversight, and compliance validation. *[Reference: ERMF – Process Owner definition]* *[Objective: VM & SPM is delivered and executed in a defined, consistent and effective manner to ensure the likelihood of the CIA breach due to technical Vulnerabilities presence is mitigated.]*

Group Security Architecture function **must**:	
VPM-110 *[new]*	Support the delivery of a robust and effective VM and SPM operational approach and capabilities by: 1) reviewing, consulting and approving the VM and SPM Standard controls adoption, i.e. the accuracy and effectiveness of the Standard controls operationalisation [Ref.: VPM-100], 2) including, where applicable, VM and SPM requirements in the minimum security baseline control requirements, in accordance with SCM-030. *[Reference: Secure Configuration Management Standard, SCM-030, VPM-100]* *[Objective: VM & SPM is delivered and executed in a defined, consistent and effective manner to ensure the likelihood of the CIA breach due to technical Vulnerabilities presence is mitigated.]*

OTCR Coverage **must**:	
VPM-112 *[new]*	Support the delivery of the robust and effective VM and SPM operational approach and capabilities by: 1) providing applicable regulatory requirements to the VM and SPM Pos, 2) reviewing, consulting and approving the VM and SPM Standard controls adoption [Ref.: VPM-100], 3) ensuring the risks identified (if not resolved) are managed in line with formal Group processes for risk and issue management. *[Reference: VPM-100]* *[Objective; VM & SPM is delivered and executed in a defined, consistent and effective manner to ensure the likelihood of the CIA breach due to technical Vulnerabilities presence is mitigated.]*

Information System/Application/Technology Infrastructure Owners **must**:	
VPM-115 *[new]*	Comply with the VM and SPM Process requirements (as communicated by the Process Owners) and applicable controls of this Standard. *[Objective: VM & SPM is delivered and executed in a defined, consistent and effective manner to ensure the likelihood of the CIA breach due to technical Vulnerabilities presence is mitigated.]*

Process Owner [of the Vulnerability Management Process/Security Patch Management Process] **must**:	
VPM-090 *[new]*	Ensure that a model for Process effectiveness and compliance with the Standard is present by: 1) documenting the VM/SPM operational approach, 2) documenting and communicating operational procedures to impacted stakeholders, 3) defining Process effectiveness metrics, approach to issue identification and data quality checks, 4) determining escalation paths for issue management, 5) management Information ("MI") and reporting considering the applicable requirements of the Standard. *[Objective: VM & SPM is delivered and executed in a defined, consistent and effective manner to ensure the likelihood of the CIA breach due to technical Vulnerabilities presence is mitigated.]*
Process Owner [of the Vulnerability Management Process/Security Patch Management Process] **must**:	
VPM-100 *[new]*	Assess and continuously improve the VM/SPM operational approach and capabilities by: 1) consulting and agreeing the Standard adoption in the operational approach with Security Architecture, to ensure it fits into ICS strategic Cyber Security architecture [Ref. section 3.4.7 ICS Security Architecture of the Information and Information and Cyber Security Risk Management Standard], 2) consulting and agreeing the Standard adoption with 2LoD, to ensure it is aligned to the Bank's risk appetite, 3) periodically (at least annually) review and, if required, update the VM operational approach and capabilities to ensure it supports Standard's objectives delivery *[Reference: ICS controls of this Standard applicable to the VM/SPM Process Owner(s).]* *[Reference: Information and Cyber Security Risk Management Standard]* *[Reference: the Group Risk Appetite.]* *[Mandatory notice: In the case of difference in opinions regarding the ICS Standards control interpretation, CISRO ICS Policy must be contacted for the binding interpretation/clarification.* *The Standard adoption is stipulated as the definition of the ICS controls operationalisation, i.e. definition of the L4 controls (ICS Actual Controls) based on the L2 controls (L2 – SCB ICS Standard Statements) and the Objectives as defined in this Standard – reference: section 6.4 ICS Control Library definitions (aligned with ICS Risk Taxonomy) of the Information and Cyber Security Risk Management*

Process Owner [of the Vulnerability Management Process/Security Patch Management Process] **must**:	
	Standard.] *[Objective: VM & SPM is delivered and executed in a defined, consistent and effective manner to ensure the likelihood of the CIA breach due to technical Vulnerabilities presence is mitigated.]*

3.2. Control Area - Vulnerability Management

3.2.1 Operational approach and governance

Process Owner [of the Vulnerability Management Process] **must**:	
VPM-020a *[prev. VIAM-050]*	Define an operational approach to Vulnerability Management ("VM") by: 1) defining, maintaining and communicating (to the impacted stakeholders) operational process(es) and procedure(s), in line with the applicable requirements of the Standard, 2) identifying and documenting the key sources of Technology Asset related information (such as CMDB), 3) defining and documenting the scope of the VM activities in line with the applicable control requirements of the Standard, 4) ensuring the required protection of VM records is maintained *[Reference: the Group Risk Appetite.]* *[Objective:* *1) VM & SPM is delivered and executed in a defined, consistent and effective manner to ensure the risk of the CIA breach due to technical Vulnerabilities presence is kept within the Group's risk appetite (as defined in the Group Risk Appetite).* *2) The sources of information critical for effective VM delivery are identified and maintained to drive correct identification and mitigation of Vulnerabilities thus managing the risk of the CIA breach within the Group's risk appetite due to Vulnerabilities exploitation.]*

Process Owner [of the Vulnerability Management Process] **must**:	
VPM-020b *[prev. VIAM-050 VIAM-110 VIAM-120 VIAM-*	Define and document the scope and coverage of Vulnerability Identification in terms of: 1) the Technology Assets covered considering: a. technologies and products present in the Group and their exposure to Vulnerability exploitation, b. importance of the Technology Assets and associated subsystems (as defined by the S-BIA rating), c. architecture/placement of the Technology Assets on the network (e.g. internet facing, internal, cloud, etc),

Process Owner [of the Vulnerability Management Process] **must**:	
140 VIAM-240]	2) applicable country/regional prescriptive regulatory requirements for vulnerability identification (as provided by ISROs or impacted Technology Asset Owners). *[Note: Technology Assets, i.e. Information System, Technology Infrastructure or Application] Objective:* 1) *VM & SPM is delivered and executed in a defined, consistent and effective manner to ensure the likelihood of the CIA breach due to technical Vulnerabilities presence is mitigated.* 2) *The methods, scope and comprehensiveness of the Vulnerability identification activity ensures the results of such a security testing are reliable and allow identification of Vulnerabilities of the target technology so the corresponding risk to CIA breach can be managed.* 3) *Vulnerabilities are identified with frequency corresponding with acceptable 'window of exposure' applicable regulatory requirements and following industry best practices (for vulnerability identification scheduling).* 4) *Vulnerabilities (identified) are timely remediated to mitigate their risk of the exploitation, thus the breach of the CIA of the Asset exposed.* 5) *Vulnerabilities are centrally recorded, retained and tracked until their closure, to ensure the security posture of the Group Assets can be evaluated.]*
VPM-050 *[prev. VIAM-290]*	Define and document the monitoring and alerting of new vulnerabilities by: 1) monitoring reliable sources of technology vulnerability alerts (including their severity), such as internal/external threat intelligence, vulnerability alerts, advisories and directives (e.g. various vendors / OEMs, manufacturers, regulators, advisories issued by CERT and other similar agencies), 2) distributing (vulnerability) notifications to impacted Technology Asset Owners for assessment of the vulnerability impact (to the Group Technology Assets), 3) invoking the Group Incident Management and Response Process for new vulnerabilities assessed as of material severity to the Group, 4) Recording of subsequent action as reported by impacted Technology Asset Owners. *[Reference: VPM-020a, VPM-020b]* *[Objective: Vulnerability related information is timely and continuously acquired, distributed to impacted stakeholders and analysed to drive effective remediation.]*
VPM-060 *[prev. VIAM-050 VIAM-080 VIAM-070 VIAM-091 VIAM-099 VIAM-*	Define, document and use approved methods of vulnerabilities identification that: 1) allows the discovery of the vulnerabilities within the scope of identification (including potential resolution), 2) defines selection of the appropriate methodology and approach used (such as automated scans, penetration testing and code security reviews), 3) have an approved Scope of Work/Rules of Engagement in place where intrusive vulnerability identification is required (e.g. Penetration Testing), 4) if required, define the restrictions for methods used in terms of expected negative impact on technology or operations, 5) considers, where applicable, techniques and methods as defined in the [VPM-AP-020]. *[Reference: VPM-AP-020]* *[Objective: The methods, scope and comprehensiveness of the Vulnerability*

Process Owner [of the Vulnerability Management Process] **must**:	
120]	*identification activity ensures the results of such a security testing are reliable and deliver expected outcomes AND allows for Vulnerabilities identification so the corresponding risk to CIA can be managed.]*
Process Owner [of the Vulnerability Management Process] **must**:	
VPM-070 *[prev. VIAM-330]*	Define and document the classification and handling of identified vulnerabilities (for remediation) in terms of: 1) vulnerabilities classes based on : a. vulnerability severity, b. impacted Asset criticality (impact rating), c. AND, if a penetration test is the source of the Vulnerability information, also ”exploitability” and factual Vulnerability exposure, 2) standard remediation timelines for respective vulnerability classes that commensurate with the potential ICS risk posed by respective vulnerability classes/categories and the impact tolerance defined for respective services, considering the acceptable vulnerable period, i.e. the max period for which the vulnerability can be present (before it is remediated, or risk managed). AND Define a scope and requirements for logging identified vulnerabilities to ensure they are registered with required level of details, available to authorised stakeholders and tracked to remediation. *[Reference VPM-020b]* *[Objectives:* *1) Vulnerabilities remediation work is prioritised in order to ensure the most critical ICS risks are remediated first.* *2) Vulnerabilities are recorded and tracked till their remediation, to ensure the security posture of the Group Assets can be evaluated.]*
VPM-080 *[prev. VIAM-050]*	Deliver operational capability to ensure VM accountabilities of the Information System / Technology Infrastructure / Application Owners can be fulfilled by: 1) deploying and maintaining the VM Process defined activities required to ensure consistent and compliant Process is present, 2) identifying, deploying, and maintaining resources required to support Process objectives (such as tooling, operational procedures, etc), 3) defining and communicating vulnerability identification requirements, 4) maintaining a vulnerability repository. *[Objective: VM & SPM is delivered and executed in a defined, consistent and effective manner to ensure the likelihood of the CIA breach due to technical Vulnerabilities presence is mitigated.]*

Process Owner [of the Vulnerability Management Process] **must**:	
VPM-120 *[prev. VIAM-*	Define and document the frequency of Vulnerabilities identification that is commensurate with: 1) the ICS risk exposure of respective technologies and architecture; and

Process Owner [of the Vulnerability Management Process] **must**:	
280]	2) Technology Asset criticality; and 3) acceptable 'window of exposure' and 4) applicable regulatory requirements; and 5) security impactful change (of the Technology Assets or ICS threat landscape). *[Objective: Vulnerabilities are identified with frequency corresponding with acceptable 'window of exposure', industry best practises and applicable regulatory requirements.]* *[Note: Security impactful change is any change to the Technology Asset that may directly impact this Asset security state due to, for example: material configuration changes, significant architecture changes or change in its security footprint as defined by changes to its threat model.* *The catalogue of changes considered as the security impactful changes must be determined by the VM Process Owner to ensure consistent and comprehensive approach to Vulnerabilities identification frequency and triggers.]*

3.2.2 Vulnerability Identification

3.2.2.1 Plan & Schedule

Process Owner [of the Vulnerability Management Process] **must**:	
VPM-130 *[prev. VIAM-100 VIAM-280]*	Schedule vulnerability identification activities in line with: 1) predefined VM scope, coverage, frequency and approach [reference VPM-020b, VPM060, VPM-120], 2) timelines/schedule appropriate to ensure that disruption to business operations is minimised, 3) valid requests from Technology Asset Owners, as defined in VPM-200. *[Reference:VPM-200,VPM-020b, VPM-060, VPM-120]]* *[Objective:* *1) Vulnerabilities are identified with frequency corresponding with acceptable 'window of exposure', industry best practises and applicable regulatory requirements.* *2) The target environment (where Vulnerability identification is conducted) is selected considering applicable regulatory requirements, level of intrusion thus disturbance caused to ensure the correct identification of the Vulnerabilities and availability and stability of the environment tested.]*
VPM-140 *[prev. VIAM-130]*	When planning vulnerability identification activities, consider: 1) limitations as reported by Technology Asset Owners; 2) applicable regulatory requirements, as provided by ISRO. to determine the factual approach to those activities and target environment to test (i.e. production or non-production). *[Objective:* *1) Vulnerabilities are identified with frequency corresponding with acceptable 'window of exposure', industry best practises and applicable regulatory requirements.*

Process Owner [of the Vulnerability Management Process] **must**:	
	2) *The target environment (where Vulnerability identification is conducted) is selected considering applicable regulatory requirements, level of intrusion thus disturbance caused to ensure the correct identification of the Vulnerabilities and availability and stability of the environment tested.]*
VPM-150 *[prev. VIAM-131 VIAM-132]*	Ensure that when Vulnerability identification is conducted on: 1) the Production environment proper safeguards must be implemented in order to minimize the likelihood of: a. Operational disruption (for constrains as provided by Information System Owner); b. ICS risk events due to e.g. accidental data manipulation or configuration changes. 2) on Non-Production environment (when considered as representation of the target, production environment), in order to provide reliable reference of the testing outcomes, ensure that: a. test scope, methods and approach reflect the testing requirements for the Production environment; b. any differences between the target and Production environment, as communicated by the Asset Owner, are documented [Ref.: VPM-180]. *[Objective:* 1) *Operational disruption and increase of the ICS risk exposure due to Vulnerabilities identification activities (due to, for example, accidental or planned configuration changes) is mitigated adequately.* 2) *The adequacy and reliability of the Vulnerability identification must be ensured, when such activities are conducted on substitute environments (instead of the factual environment).]*
Process Owner [of the Vulnerability Management Process] **must**:	
VPM-160 *[new]*	Communicate the vulnerability identification schedule, plan and approach to the impacted Asset Owners. *[Note: Impacted Asset Owners must be informed about:* 1) *the scope of the tests, scans and assessment,* 2) *dates and times for the Vulnerability identification,* 3) *potential impact to normal operations,* 4) *required configuration changes/amendments to allow for successful vulnerability identification.]* *[Objective:* 1) *Vulnerabilities are identified with frequency corresponding with acceptable 'window of exposure', industry best practises and applicable regulatory requirements.* 2) *Operational disruption and increase of the ICS risk exposure due to Vulnerabilities identification activities (due to, for example, accidental or planned configuration changes) is mitigated adequately.* 3) *Vulnerability identification is executed in a planned and controlled manner, to minimise the negative impact of the testing and increase the effectiveness of*

Process Owner [of the Vulnerability Management Process] **must**:	
	the identification.]
VPM-170 *[new]*	Document and, if applicable, plan for resolution, any deviations from the planned schedule for the Vulnerability identification activities. *[Reference: the Group Risk Appetite.]* *[Objective:* 1) *Vulnerability identification is executed in a planned and controlled manner, to minimise the negative impact of the testing and increase the effectiveness of the identification.* 2) *Any deviations or limitation to the planned Vulnerability identification scope and approach are adequately managed to ensure that risk of the technical Vulnerability presence is managed within the Group risk appetite.]*

Information System/Application/Technology Infrastructure Owners **must**:	
VPM-175 *[new]*	Document and, in coordination with the Process Owner, plan for resolution any deviations from the Vulnerability identification plan or schedule. *[Note: Unresolved issues must be risk managed]* *[Reference: the Group Risk Appetite.]* *[Objective:* 1) *Vulnerability identification is executed in a planned and controlled manner, to minimise the negative impact of the testing and increase the effectiveness of the identification.* 2) *Any deviations or limitation to the planned Vulnerability identification scope and approach are adequately managed to ensure that risk of the technical Vulnerability presence is managed within the Group risk appetite.]*
Information System/Application/Technology Infrastructure Owners **must**:	
VPM-180 *[prev. VIAM-020 VIAM-040 VIAM-132 VIAM-125]*	Ensure that (owned) Technology Assets: 1) are available for periodic Vulnerability Identification in line with the schedule and plan communicated by the Process Owner and their records in the respective asset inventories are up to date – reference: SAM-120, SAM-130, 2) have the configuration required (as communicated by the PO) for effective Vulnerability identification, including any temporary security controls amendments required for successful Vulnerability identification, 3) in the case when non-production environment is scoped as a production environment image/representation: a. the non-production environment represents the same level of security controls, technology and configuration (to ensure the Vulnerability identification results can be considered as the reliable representation of the target environment), b. any differences between target and Production environment, as communicated to the PO, are documented and applicable corresponding risks identified and managed. *[Reference: Secure Asset Management Standard, Group Risk*

Information System/Application/Technology Infrastructure Owners **must**:	
	Appetite.] *[Objective:* *1) Vulnerability identification is executed in a planned and controlled manner, to minimise the negative impact of the testing and increase the effectiveness of the identification.* *2) Any deviations or limitation to the planned Vulnerability identification scope and approach are adequately managed to ensure that risk of the technical Vulnerability presence is managed within the Group risk appetite.* *3) Operational disruption and increase of the ICS risk exposure due to Vulnerabilities identification activities (due to, for example, accidental or planned configuration changes) is mitigated adequately.* *4) The adequacy and reliability of the Vulnerability identification must be ensured, when such activities are conducted on substitute environments (instead of the factual environment).]*
VPM-190 *[prev. VIAM-125]*	Report to the PO any issues or limitations for planned Vulnerability identification activities, including information needed to implement proper safeguards and define test scope, methods, and approach for Vulnerability identification. *[Objective:* *1) Operational disruption and increase of the ICS risk exposure due to Vulnerabilities identification activities (due to, for example, accidental or planned configuration changes) is mitigated adequately.* *2) Any deviations or limitation to the planned Vulnerability identification scope and approach are adequately managed to ensure that risk of the technical Vulnerability presence is managed within the Group risk appetite.]*
VPM-200 *[prev. VIAM-270]*	Request any additional Vulnerability identification activities (i.e. other than those defined and communicated by the PO) if: 1) such scans or assessments are regulatory driven, 2) there is a trigger for such assessments/scans, such as Major Release to the owned Asset(s). *[Note: Such requests must follow the formal requirements as communicated defined within the VM Process and communicated by the PO.]* *[Reference: ENTERPRISE SYSTEM DELIVERY LIFECYCLE Standard.]* *[Objective: Vulnerabilities are identified with frequency corresponding with acceptable 'window of exposure', industry best practises and applicable regulatory requirements.]*

3.2.2.2 Scan & Assess

Process Owner [of the Vulnerability Management Process] **must**:	
VPM-210 *[prev.*	Execute the Vulnerability scanning and assessment, in line with the predefined plan and schedule.

Process Owner [of the Vulnerability Management Process] **must**:	
VIAM-250 SPM-010]	*[Reference: VPM section 3.2.2.1 "Plan & Schedule"] [Objective:* *1) Vulnerabilities are identified with frequency corresponding with acceptable 'window of exposure', industry best practises and applicable regulatory requirements.* *2) Vulnerability identification is executed in a planned and controlled manner, to minimise the negative impact of the testing and increase the effectiveness of the identification.* *3) The adequacy and reliability of the Vulnerability identification must be ensured, when such activities are conducted on substitute environments (instead of the factual environment).]*
VPM-220 *[new]*	Log (in line with the VM process requirements): 1) identified Vulnerabilities, 2) operational impact, such as stability, performance or any other issues with the identification tasks execution (as identified or reported by the Assets Owners or Technology functions). *[Objective:* *1) Operational disruption and increase of the ICS risk exposure due to Vulnerabilities identification activities (due to, for example, accidental or planned configuration changes) is mitigated adequately.* *2) Vulnerabilities are centrally recorded, retained and tracked until their closure, to ensure the security posture of the Group Assets can be evaluated.]*
VPM-225 *[prev. VIAM-080]*	Ensure failed vulnerability identification activities impacting expected results are: 1) considered for re-scanning or assessment, and, 2) **if required**, alternative methods of Vulnerability identification are considered. *[Objective: Any deviations or limitation to the planned Vulnerability identification scope and approach are adequately managed to ensure that risk of the technical Vulnerability presence is managed within the Group risk appetite.]*

Information System/Application/Technology Infrastructure Owners **must**:	
VPM-230 *[new]*	Monitor Technology Asset stability and performance and immediately report issues to the PO. *[Objective: Operational disruption and increase of the ICS risk exposure due to Vulnerabilities identification activities (due to, for example, accidental or planned configuration changes) is mitigated adequately.]*

3.2.3 Vulnerability Remediation

3.2.3.1 Plan the response

Process Owner [of the Vulnerability Management Process] **must**:	
VPM-240 *[prev. VIAM-330]*	Analyse identified Vulnerabilities to: 1) determine their relevance (for manual methods of Vulnerability identification), 2) categorise and prioritise them in line with vulnerabilities classes/categories [Reference: VPM-070], 3) recommend potential remediation [reference: VPM-AP-010] AND update the vulnerabilities repository with relevant information. *[Objectives:* *1) Vulnerabilities remediation work is prioritised in order to ensure the most critical ICS risks are remediated first.* *2) Vulnerabilities are recorded and tracked till their remediation, to ensure the security posture of the Group Assets can be evaluated.]*
VPM-250 *[new]*	Share the outcomes of the vulnerability identification and analysis with impacted stakeholders, including the expected remediation timelines and priority. *[Objectives:* *1) Information regarding identified Vulnerabilities is timely and continuously delivered to the impacted stakeholders, so those can be planned and scheduled for mitigation, in line with the Group's risk appetite.* *2) Vulnerabilities remediation work is prioritised in order to ensure the most critical ICS risks are remediated first.]*
VPM-260 *[new]*	Where a workaround is used to mitigate a zero-day CVE with no patch available, report the thematic solution(s) to SACA, so the remediation can be considered in the minimum security baseline control requirements, as defined in the SCM-030. *[Reference: ICS Secure Configuration Management Standard]* *[Objective:* *1) Zero-day vulnerabilities are mitigated in a consistent, repeatable and controlled manner across Group Technology Assets, so the effectiveness and continuous maintenance of such a mitigation can be ensured.* *2) Known Vulnerabilities are mitigated by embedding required controls in the default configuration or settings.]*

Information System/Application/Technology Infrastructure Owners **must**:	
VPM-270 *[prev. VIAM-370]*	1) Analyse identified vulnerabilities (considering analysis and remediation recommendation received from the PO and applicable Technology functions), 2) plan, define and document remediation activities. *[Objective:* *1) Vulnerabilities (identified) are timely remediated to mitigate their risk of the exploitation, thus the breach of the CIA of the Asset exposed.* *2) Vulnerabilities remediation work is prioritised in order to ensure the most critical ICS risks are remediated first.*

Information System/Application/Technology Infrastructure Owners **must**:	
	3) *Vulnerabilities are recorded and tracked till their remediation, to ensure the security posture of the Group Assets can be evaluated.* 4) *Vulnerabilities remediations plan is documented to ensure accountabilities (for the remediation) and the timelines are known and can be tracked and evaluated.]*
Information System/Application/Technology Infrastructure Owners **must**:	
VPM-280 *[prev. VIAM-350]*	Ensure that vulnerabilities that cannot be remediated or cannot be remediated within given predefined timelines are: 1) risk managed, 2) reported to the PO (with details of managed risk). *[Objective: the ICS risk of the presence of technical Vulnerabilities is adequately managed in line with the Group's risk appetite.]*

3.2.3.2 Execute the response

Information System/Application/Technology Infrastructure Owners **must**:	
VPM-290 *[prev. VIAM-370 VIAM-390]*	Remediate identified vulnerabilities by implementing (or requesting the implementation) of corrective actions as defined in the remediation plan and in line with the Group Change Management Process. *[Objective:* 1) *Vulnerabilities (identified) are timely remediated to mitigate their risk of the exploitation, thus the breach of the CIA of the Asset exposed.* 2) *Vulnerabilities remediation work is prioritised in order to ensure the most critical ICS risks are remediated first.* 3) *Vulnerabilities remediation plan is documented to ensure accountabilities (for the remediation) and the timelines are known and can be tracked and evaluated.]*
VPM-300 *[prev. VIAM-410]*	For unsuccessful implementation of the remediating actions: 1) discuss and agree the alternatives with applicable Technology functions, 2) document the remediation plan change, 3) raise and manage corresponding risks or issues in line with the Group processes and report the exception the PO, 4) implement alternative corrective actions. *[Objective:* 1) *the ICS risk of the presence of technical Vulnerabilities is adequately managed in line with the Group's risk appetite.* 2) *Vulnerabilities remediation plan is documented to ensure accountabilities (for the remediation) and the timelines are known and can be tracked and evaluated.]*
VPM-310 *[prev. VIAM-370 VIAM-380*	Document and track to resolution the remediating actions by: 1) verifying the effectiveness of remediation actions for vulnerabilities (including requesting retest for non-automated identification methods), 2) reporting the status of the remediation plan delivery to the PO (in line with the

Information System/Application/Technology Infrastructure Owners **must**:	
VIAM-410]	communicated requirements) 3) ensuring that any breach to remediation delivery timelines or scope (as defined in the plan) is risk managed, 4) updating information in the Vulnerabilities repository. *[Objective:* *1) the ICS risk of the presence of technical Vulnerabilities is adequately managed in line with the Group's risk appetite.* *2) Vulnerabilities remediation plan is documented to ensure accountabilities (for the remediation) and the timelines are known and can be tracked and evaluated.* *3) Vulnerabilities are recorded and tracked till their remediation, to ensure the security posture of the Group Assets can be evaluated.* *4) Vulnerabilities remediation must be evaluated for effectiveness, to ensure that the risk their exploitation is adequately mitigated.]*
Information System/Application/Technology Infrastructure Owners **must**:	
VPM-320 *[prev. VIAM-360 VIAM-361]*	Ensure that any incidents or security events identified during the Vulnerability management activities are handled in line with the Group Incident Management process. *[For example: unauthorised services or devices, unauthorised changes to Asset configuration or state, etc.]* *[Objective: Considering the increased likelihood of operational disruption (from Vulnerabilities management activities), any identified security evens or incidents must be timely and appropriately handled to avoid ICS risk materialisation beyond the acceptable risk appetite.]*

Process Owner [of the Vulnerability Management Process] **must**:	
VPM-330 *[new]*	Track and record remediation status (as informed by Information System/Application/Technology Infrastructure Owners) and, if required: 1) update information in the vulnerability repository 2) Report/escalate material issues in line with the VM Process requirements [Reference: VPM-090] *[Reference: VPM-090]* *[Objective:* *1) the ICS risk of the presence of technical Vulnerabilities is adequately managed in line with the Group's risk appetite.* *2) Vulnerabilities are recorded and tracked till their remediation, to ensure the security posture of the Group Assets can be evaluated.]*

3.2.4 Verification and Monitoring of the Vulnerability Remediation

Process Owner [of the Vulnerability Management Process] **must**:	
VPM-340	After remediation completion (as confirmed by the respective Asset Owners), validate

Process Owner [of the Vulnerability Management Process] **must**:	
[prev. VIAM-400 SPM-010]	the effectiveness of the vulnerability remediation. *[Note: Validation considers re-verification of the Vulnerability presence and corresponds with the method used for the initial identification AND, respectively, may consider:* • *Re-assessment or re-scans of the vulnerability,* • *Re-attempting to exploit the Vulnerability, Asset state checks (for decommissioned or replaced Assets).]* *[Objective: Vulnerabilities remediation must be evaluated for effectiveness, to ensure that the risk their exploitation is adequately mitigated.]*
Process Owner [of the Vulnerability Management Process] **must**:	
VPM-345 *[prev. VIAM-310]*	After the verification: 1) provide the feedback and report outcomes to respective Asset Owners, 2) update the Vulnerability record in the Vulnerability repository with the results and finding of the evaluation, 3) re-open the Vulnerability in the case of unsuccessful mitigation (for Vulnerabilities planned for remediation). *[Objective:* *1) Vulnerabilities remediation must be evaluated for effectiveness, to ensure that the risk their exploitation is adequately mitigated.* *2) the ICS risk of the presence of technical Vulnerabilities is adequately managed in line with the Group's risk appetite.* *3) Vulnerabilities are recorded and tracked till their remediation, to ensure the security posture of the Group Assets can be evaluated.]*
VPM-350 *[new]*	Periodically conduct thematic analysis to identify potential configuration setting updates to mitigate vulnerabilities by reporting applicable minimum security baseline changes to SACA. *[Reference: Secure Configuration Management Standard, VPM-250] [Objective:* *1) Technical Vulnerabilities are mitigated in a consistent, repeatable and controlled manner across Group Technology Assets, so the effectiveness and continuous maintenance of such a mitigation can be ensured.* *2) Known Vulnerabilities are mitigated by embedding required controls in the default configuration or settings.]*

3.2.5 Supplementary Provisions

3.2.5.1 Vulnerability Reporting

Process Owner [of the Vulnerability Management Process] **must**:	
VPM-360 *[prev. VIAM-300]*	Generate and distribute internal vulnerability alerts, advisories, and directives as deemed necessary to the intended Technology Asset Owners. *[Objective: Vulnerability related information is timely and continuously acquired, distributed to impacted stakeholders and analysed to drive effective remediation.]*

Process Owner [of the Vulnerability Management Process] **must**:	
VPM-370 *[new]*	Ensure that vulnerability assessment reports together with remediation status is made available to authorised stakeholders. *[Objective:* *1) Information regarding identified Vulnerabilities is timely and continuously delivered to the impacted stakeholders, so those can be planned and scheduled for mitigation, in line with the Group's risk appetite.* *2) the ICS risk of the presence of technical Vulnerabilities is adequately managed in line with the Group's risk appetite.]*
Process Owner [of the Vulnerability Management Process] **must**:	
VPM-380 *[new]*	Generate and distribute management information that: 1) provides an overview of the vulnerability remediation status, 2) outlines material concerns in the context of unresolved vulnerabilities, misconfiguration and code defects present in Group Technology Assets. *[Objective:* *1) the ICS risk of the presence of technical Vulnerabilities is adequately managed in line with the Group's risk appetite.* *2) Vulnerabilities are recorded and tracked till their remediation, to ensure the security posture of the Group Assets can be evaluated.]*

3.2.5.2 Code Security Reviews & Application-Level Assessments

Process Owner [of the Vulnerability Management Process] **must**:	
VPM-390 *[new]*	Ensure that the VM strategy for Applications Vulnerability identification considers: 1) static application security testing (SAST) to analyse the source code to identify security findings arising due to coding defects, as predefined in the scope and approach of the VM [Ref.: VPM-020a & VPM-020b], 2) dynamic application security testing (DAST) to scan the behaviour of the applications, 3) penetration testing under different scenarios (e.g. bypassing authorisation and authentication, token injection, cross-site scripting), 4) leveraging applicable industry best practises. *[Reference: VPM-060]* *[Objective: Application-level Vulnerabilities are identified effectively, with methods and approach selected adequately, so the ICS risk that such Vulnerabilities can pose, is managed withing the Group's risk appetite.]*
VPM-400 *[prev.*	Define, maintain and deliver the Code Security Review self-service / self-attests guidance for Application Teams.

Process Owner [of the Vulnerability Management Process] **must**:	
VIAM-246]	*[Objective: Application-level Vulnerabilities are identified effectively, with methods and approach selected adequately, so the ICS risk that such Vulnerabilities can pose, is managed withing the Group's risk appetite.]*
VPM-405 *[prev. VIAM-247]*	Ensure for Commercial off the Shelf Software [COTS] Applications are assessed in line with the VM operational approach. *[Objective: Application-level Vulnerabilities are identified effectively, with methods and approach selected adequately, so the ICS risk that such Vulnerabilities can pose, is managed withing the Group's risk appetite.]*
VPM-410 *[prev. VIAM-170]*	Ensure that applications vulnerability identification, at minimum, covers applicable OWASP Top 10 vulnerability classes. *[Reference: OWASP Top Ten | OWASP Foundation]* *[Objective: Application-level Vulnerabilities are identified effectively, with methods and approach selected adequately, so the ICS risk that such Vulnerabilities can pose, is managed withing the Group's risk appetite.]*

Information System/Application/Technology Infrastructure Owners **must**:	
VPM-405a	Ensure, that for all software/applications (for which the source code is not available, such as Commercial off the Shelf Software [COTS] applications) contractual agreements with vendors include provision for vendors to provide SAST (and, if not available, DAST or penetration testing) reports when requested by the Bank. *[Reference: Security in Interactions with Third Parties Standard]* *[Objective: Application-level Vulnerabilities are identified effectively, with methods and approach selected adequately, so the ICS risk that such Vulnerabilities can pose, is managed withing the Group's risk appetite.]*

3.2.5.3 Independent Security Assessors

Group CISO/Group CISRO/Process Owner [of the Vulnerability Management Process] **must**:	
VPM-420 *[new]*	Define, maintain and follow the criteria for Security Assessors involvement in the Vulnerability identification to ensure that, where and when required (for example – mandated by applicable regulatory requirements or driven by elevated ICS risk exposure), an independent Vulnerability assessment is delivered. *[Objective:* 1) *Vulnerabilities identification efficiency can be elevated, when an independent assessor is involved so 'fresh' perspective on the asset security is provided. Also, independents assessor's involvement may be required due to internal functions capacity limitations or applicable regulatory requirements.* 2) *The procedure, approach and criteria for Security Assessors involvement must be predefined and then followed to ensure the consistent and repeatable approach is present.]*

Group CISO/Group CISRO/Process Owner [of the Vulnerability Management Process] **must**:	
VPM-430 *[prev. VIAM-140 VIAM-150 VIAM-190 VIAM-200]*	(If any Vulnerability identification activity is expected to be conducted by Security Assessors): 1) perform Security Assessor Assessment in line with respective process definition (i.e. VM and Red Team operations), 2) if required and effective, rotate Security Assessors to avoid complacency of the vendors and blind spots, 3) ensure that the knowledge and practical skills of the Security Assessors is supported by industry recognised relevant certification obtained by the key delivery resources. *[Reference: Security in Interactions with Third Parties Standard]* *[Objective: Vulnerabilities identification must be conducted in line with the industry best practices and by skilled professionals, so the results can be considered effective and the testing does not pose any additional risk or cause operational disruption to the Group.]*
VPM-440 *[new]*	Ensure that that all vulnerability identification activities performed by Security Assessors are conducted with oversight of the authorised Group personnel to ascertain that the activities are within the intended scope and do not disrupt Group operations. *[Note: Oversight could be considered as:* • *verification and approval of the testing methodology and approach,* • *specific contractual clauses,* • *precise scope and plan of the work, etc.]* *[Objective: Vulnerabilities identification must be conducted in line with the industry best practices and by skilled professionals, so the results can be considered effective and the testing does not pose any additional risk or cause operational disruption to the Group.]*

3.2.6 Red Teaming

Group CISRO **must**:	
VPM-450 *[prev. VIAM-180]*	Establish, maintain and deliver a documented process for Red Team operations including: 1) scope of work and rules of engagement, 2) scoping, Reconnaissance, Threat Intelligence, Scenario definition, Execution, Reporting and Risk Management (for risks corresponding with the Red Team operations). *[Objective: Red Teaming operations are conducted to identify security gaps that can be exploited, so those can be managed thus mitigate the resulting ICS risk effectively.]*
VPM-455 *[new]*	Plan the Read Team exercises in line with: 1) applicable regulatory requirements,

Group CISRO **must**:	
	2) other applicable factors, such as material increase of the ICS risk exposure. 3) the requirements from the approved CISRO Assurance plan. *[Objective: Red Teaming exercises are conducted to identify security gaps that can be exploited, so those can be managed thus mitigate the resulting ICS risk effectively.]*
VPM-460 *[prev. VIAM-185]*	Ensure, that for every Red Teaming exercise the below is defined and documented: 1) Scope of Work/Rules of Engagement 2) Exercise scenarios, including the goals/flags planned to achieve/capture. *[Objective: Red Teaming exercises are conducted to identify security gaps that can be exploited, so those can be managed thus mitigate the resulting ICS risk effectively.]*
VPM-470 *[prev. VIAM-220]*	Execute the Red Team exercises in line with the process definition and plan. *[Objective: Red Teaming exercises are conducted to identify security gaps that can be exploited, so those can be managed thus mitigate the resulting ICS risk effectively.]*
VPM-475 *[new]*	Document and report the outcomes (of the executed Red Team exercises); AND Ensure that identified security weaknesses and vulnerabilities are either tracked to closure or handed over to applicable Group processes. *[Objective: Red Teaming exercises are conducted to identify security gaps that can be exploited, so those can be managed thus mitigate the resulting ICS risk effectively* *AND* *The findings identifies and actions against those findings are tracked as part of issue management, so the ICS risk pose by them can be kept within the Group's risk appetite.]*

3.2.7 Responsible Disclosure Policy ("RDP")

Group CISO **must**:	
VPM-480 *[prev. VIAM-420]*	Develop and publish a Responsible Disclosure Policy [RDP] which must include: 1) Information Systems and types of vulnerabilities which are in scope; 2) types of testing that are allowed (or specifically not authorized); 3) a statement prohibiting the disclosure of any Personal Data [PD] discovered to any Third Party [TP]; 4) a comprehensive description of how to submit vulnerability reports including quality requirements; 5) a statement that sets expectations regarding acknowledgement of reported vulnerabilities, including timing and financials; 6) laws and regulations which are binding for researchers; 7) a document version number and version history.

Group CISO **must**:	
	[Reference: ISO 29147 – Vulnerability Disclosure; ISO 30111 – Vulnerability Handling Process; OWASP Vulnerability Disclosure Cheat Sheet; The CERT Guide to Coordinated Vulnerability Disclosure; Cybersecurity and Infrastructure Security Agency Binding Operational Directive 20-01] *[Objective: Ensure that security Vulnerabilities can be safely and formally reported to the Group, so those can be managed in line with the Group's risk appetite (before they can be exploited).]*
VPM-490 *[prev. VIAM-430]*	Develop RDP procedures which must describe how: 1) vulnerability reports are tracked to resolution; 2) remediation activities are coordinated internally; 3) disclosed vulnerabilities are evaluated for potential impact and prioritized for action; 4) reports for systems and services that are out of scope are handled; 5) communication with the reporter and other stakeholders occurs; 6) current or past impact of the reported vulnerabilities was assessed and if it was treated as an incident or breach (as applicable); 7) defined target timelines are tracked; 8) defined Key Metrics are reported. *[Objective: Ensure that security Vulnerabilities can be safely and formally reported to the Group, so those can be managed in line with the Group's risk appetite (before they can be exploited).]*

3.3. Control Area - Security Patch Management

3.3.1 Planning, scoping and governance

Process Owner [of the Security Patch Management Process] **must**:	
VPM-500 *[prev. SPM-010]*	Define operational approach to Security Patch Management ("SPM") by: 1) defining, maintaining and communicating (to the impacted stakeholders) operational process and procedures, in line with the applicable requirements of the Standard, 2) defining approach for security patches identification, 3) defining the criteria for routine and emergency patching, 4) integrating the SPM with applicable elements of the VM Process, i.e.: a. prioritisation approach to Security Patches (so it is aligned with the Vulnerability prioritisation) b. standard remediation timelines for Vulnerabilities (so the Security Patches, if applicable, can be deployed withing the predefined timelines), c. coverage and scoping.

Process Owner [of the Security Patch Management Process] **must**:	
	5) identifying and documenting the key sources of Technology Asset related information (such as CMDB). *[References: Release Management Standard, Technology Change Management Standard]* *[Objective: Security Patches must be correctly identified, prioritised, acquired and validated to make sure they are deployed in timely manner and corresponding Vulnerabilities can be closed.]*
VPM-510 *[prev. SPM-010]*	Define and document the scope and coverage of the Security Patch Management in terms of: 1) the Technology Assets covered considering: a. technologies and products present in the Group and their exposure to Vulnerability exploitation, b. importance of the Technology Assets and associated subsystems (as defined by the S-BIA rating), c. architecture/placement of the Technology Assets on the network (e.g. internet facing, internal, cloud, etc), 2) applicable country/regional prescriptive regulatory requirements for patching security vulnerabilities (as provided by ISROs or impacted Technology Asset Owners), 3) Security Patch prioritisation and expected deployment timelines (for respective priority classes/categories [Reference VPM-520]. *[Reference: VPM-520]* *[Note: Technology Assets, i.e. Information System, Technology Infrastructure or Application] [Objective:* *1) Security Patches must be correctly identified, prioritised, acquired and validated to make sure they are deployed in timely manner and corresponding Vulnerabilities can be closed.* *2) Patching efforts can be prioritised, so the most critical ICS risks are addressed first.* *3) Patching scope and frequency corresponds with the Group's ICS risk appetite and applicable regulatory requirements.]*
Process Owner [of the Security Patch Management Process] **must**:	
VPM-520 *[prev. SPM-010 SPM-110]*	Define and document prioritisation of the Security Patches, considering: 1) Security Patches classes/categories based on : a. impacted Asset criticality (impact rating), b. corresponding Vulnerability severity, 2) standard/expected deployment timelines for respective Security Patch classes/categories that commensurate with the potential ICS risk posed by lack of respective Security Patch class/category and the impact tolerance defined for respective services, considering the acceptable vulnerable period, i.e. the max period for which the Asset can remain unpatched. *[Reference: VPM-510]* *[Objective:*

Process Owner [of the Security Patch Management Process] **must**:	
	1) *Patching efforts can be prioritised, so the most critical ICS risks are addressed first.* 2) *Patching scope and frequency corresponds with the Group's ICS risk appetite and applicable regulatory requirements.]*
VPM-530 *[new]*	Deliver operational capability to ensure SPM accountabilities (as defined in the SPM Process) of the Information System/ Technology Infrastructure / Application Owners can be fulfilled by: 1) delivering and maintaining the SPM Process defined activities required to ensure consistent and compliant Process is present, 2) identifying, deploying and maintaining resources required to support Process objectives (such as tooling, operational procedures, etc), 3) integrating applicable operational activities with the Group Change Management Process and Technology Release Management Processes. *[References: ENTERPRISE SYSTEM DELIVERY LIFECYCLE Standard, Enterprise IT Service Operations Management Standard.] [Objective:* 1) *Security Patches must be correctly identified, prioritised, acquired and validated to make sure they are deployed in timely manner and corresponding Vulnerabilities can be closed.* 2) *Security patching is delivered in a planned and controlled manner, increasing effectiveness of technical Vulnerabilities maintenance and closure.]*

3.3.2 Security Patch Identification and Prioritisation

Process Owner [of the Security Patch Management Process] **must**:	
VPM-560 *[prev. SPM-010 SPM-100 SPM-110 SPM-130]*	If a Security Patch is identified (in line with the activities defined in the VPM-050) ensure that: 1) the Security Patch is prioritised [reference: VPM-520] 2) notification regarding the Security Patch is disseminated (together with the patch priority and expected deployment timeline) to impacted Technology Asset Owners and Technology Functions (routine patching), 3) For emergency Security Patch, Group Incident Management and Response Process is invoked (as mandated in VPM-050), 4) Record the outcomes of the Security Patch assessment (as conducted by the impacted Assets Owners) and, if applicable, re-assess and update the Security Patch priority. *[Reference: VPM-520, VPM-050, VPM-570]*

Process Owner [of the Security Patch Management Process] **must**:	
	[Objective: *1) Security Patches must be correctly identified, prioritised, acquired and validated to make sure they are deployed in timely manner and corresponding Vulnerabilities can be closed.* *2) Patching efforts can be prioritised, so the most critical ICS risks are addressed first.* *3) Information regarding available Security Patches is timely and continuously acquired, distributed to impacted stakeholders and analysed to drive effective remediation.]*

3.3.3 Security Patch Assessment, Acquisition, Validation, Testing & Deployment

Information System/Application/Technology Infrastructure Owners **must**:	
VPM-570 *[prev. SPM-010 SPM-110 SPM-130]*	Based on the notification delivered by the SPM PO: 1) assess the applicability and pre-assigned priority of the Security Patch, 2) identify Technology Assets impacted, 3) report back the outcomes to the assessment and identification to the SPM PO. *[Reference: VPM-560]* *[Keynote: during the patch assessment, impact of both deploying and not deploying the patch should be evaluated.] [Objective:* *1) Security Patches must be correctly identified, prioritised, acquired and validated to make sure they are deployed in timely manner and corresponding Vulnerabilities can be closed.* *2) Patching efforts can be prioritised, so the most critical ICS risks are addressed first.]*
VPM-580 *[prev. SPM-010 SPM-130 SPM-220]*	Based on the assessed and agreed Security patch Priority (referenceVPM-560), plan and schedule the Security patch deployment in line with: 1) (revalidated) Security Patch priority, as assigned and notified by the SPM PO, 2) Applicable requirements of the Group Change Management and Technology Release Management Processes. *[Objective:* *1) Security Patches must be correctly identified, prioritised, acquired and validated to make sure they are deployed in timely manner and corresponding Vulnerabilities can be closed.* *2) Patching efforts can be prioritised, so the most critical ICS risks are addressed first.* *3) Security Patch deployment is conducted in a governed and controlled manner to ensure effective closure of corresponding Vulnerabilities.]*
VPM-590 *[prev. SPM-010 SPM-105]*	Acquire the applicable Security Patch(es) only from authorised sources, such as vendor's/OEM's repositories, internal Group repositories, etc.

Information System/Application/Technology Infrastructure Owners **must**:	
Information System/Application/Technology Infrastructure Owners **must**:	
	[Objective: Only valid Security Patches are deployed to ensure that corresponding technical Vulnerability is effectively mitigated AND the impacted Technology Assets are not exposed to additional ICS risks (due to invalid or malicious component installation).]
VPM-600 *[prev. SPM-010 SPM-130 SPM-190 SPM-170 SPM-150 SPM-120 SPM-180 SPM-200 SPM-210 SPM-160 SPM-211 SPM-220 SPM-232]*	Ensure the Security Patch is validated, tested and deployed in line with the Group Change Management and Technology Release Management Processes on all instances of the impacted Technology Assets; OR In the case of the unsuccessful Security Patch deployment: 1) Report the to the SPM PO, 2) Assess the case and either: a. plan and schedule re-deployment OR b. ensure the exception is risk managed in line with the Group processes (such as CRISP) and (if applicable) roll back the change. *[Keynote: Security Patch must be evaluated before rolled out to production environments. The validation must consider:* • *applicable regression testing,* • *verification if the Security Patch effectively closes corresponding Vulnerability,* • *testing of the roll back procedures.] [Objective:* 1) *Security Patch deployment is conducted in a governed and controlled manner to ensure effective closure of corresponding Vulnerabilities.* 2) *Only valid Security Patches are deployed to ensure that corresponding technical Vulnerability is effectively mitigated AND the impacted Technology Assets are not exposed to additional ICS risks (due to invalid or malicious component installation).]*
VPM-610 *[prev. SPM-010 SPM-230 SPM-231 SPM-232]*	Post deployment, conduct rigorous verification, to ensure that: 1) Technology Asset is operational (as per its specification) and 2) the Security Patch effectively closed corresponding vulnerability. AND Report the Security Path deployment status back to the SPM PO. *[Objective: Security Patches deployment effectiveness and security is validated, to ensure the expected result is achieved.]*

3.3.4 Security Patch Tracking & Monitoring

Process Owner [of the Security Patch Management Process] **must**:	
VPM-650 *[prev. SPM-*	1) Monitor: a. proactively – in line with the VM Process identification capabilities OR b. based on the status reports from the impacted Technology Asset

Process Owner [of the Security Patch Management Process] **must**:	
010]	Owners) the status and the effect of the Security Patch deployment, 2) Ensure that issues identified are reported, escalated and: a. tracked to completion OR b. registered and risk managed (by the respective Asset Owners), in line with the Group processes (such as CRISP) *[Reference: VPM-600]* *[Objective:* *1) Security Patches deployment effectiveness and security is validated, to ensure the expected result is achieved.* *2) Failed Security Patches are adequately handled, to ensure that ICS risk posed by the corresponding Vulnerabilities can kept with the Group's risk appetite.]*

3.3.5 Supplementary provisions

Process Owner [Enterprise Technology End User Services] **must**:	
VPM-700 *[prev. SPM-233]*	Ensure that any Group IT Equipment that will remain unpatched (in breach with defined timeline) must be disallowed from accessing Group network or Information. *[Objective: IT Equipment accessing the Group network or Information must be compliant with relevant security requirements, to ensure it will not be used as an attack vector (due to present technical Vulnerabilities).]*
VPM-710 *[prev. SPM-234]*	Ensure that re-enrolment of any Group IT Equipment access to Group Information is only allowed after deployment of required Security Patches. *[Objective: IT Equipment accessing the Group network or Information must be compliant with relevant security requirements, to ensure it will not be used as an attack vector (due to present technical Vulnerabilities).]*
VPM-720 *[prev. SPM-090]*	Communicate to Staff by when Security Patches need to be deployed on Group IT Equipment assigned to them. *[Objective: IT Equipment accessing the Group network or Information must be compliant with relevant security requirements, to ensure it will not be used as an attack vector (due to present technical Vulnerabilities).]*

4. INFORMATION & SUPPORT

4.1. General Information and Support

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

4.2. Reporting Non-Compliance

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

4.3. Breach of this Standard

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

5. GLOSSARY

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

6. REGULATORY - INDUSTRY REFERENCES

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

7. APPENDIX

7.1. [VPM-AP-010] Table 1 – Responding to identified Vulnerabilities

#	Response	Additional notes
1	Patching	Removing vulnerability with patch installation or software upgrade, as defined in the section 3.3 Control Area: Security Patch Management
2	Reconfiguration	Closing the vulnerability with configuration changes, such as disabling vulnerable services.
3	Adding controls	Mitigating the vulnerability with additional security controls to either early detect the vulnerability exploitation or prevent its exploits.
4	Changing asset state	Replacement or decommissioning of the impacted asset.
5	(Other) mitigating measures recommended by Vendors	A single or combination of methods (defined) above which are defined by Vendors as effective Vulnerability closure or remediation with no or acceptable impact to solution stability and operations.

7.2. [VPM-AP-020] Mandatory minimum baseline for Vulnerability identification

#	Vulnerability identification aspect	Baseline approach to be considered for selection	Examples and notes
A1	A. Techniques of Vulnerabilities identification	Automated scans	Depending on the scope and test cases of the vulnerability identification and the approach, both authenticated and unauthenticated scans should be considered
A2		Manual assessment	Manual assessments, such as penetration testing, should be considered when: 1) there is a regulatory requirement explicitly requesting such assessment is in place 2) detailed, hands-on examination is required.
A3		Code security reviews	For example: SAST
A4		Application level scans	For example: DAST
A5		Internal and external network scanning	Identification of unauthorised services/ports (against the list of predefined authorised services and corresponding ports)
A6		Security Assessors	3rd party involvement should be considered when: 1) there is a specific regulatory requirement, 2) the Asset threat/risk profile may require independent assessment is performed, 3) resource shortage may impact the VM approach and plan.
A7		Adequate tooling and testing technique	The methods and toolset need to be identified and selected in line with: 1) Technology/asset category that needs to be tested (such as cloud environments, specific architecture such as containers, etc), 2) the nature/category of the Vulnerability to be identified.
B1	B. Levels/types of vulnerabilities identification	Discovery/confirmation of known vulnerabilities.	Confirmation of presence of reported Vulnerabilities or software flaws.

#	Vulnerability identification aspect	Baseline approach to be considered for selection	Examples and notes
B2		Weak security configurations	Open network ports, nonstandardised services or configuration, lack of security controls or applicable Security Patches.
B3		Discovery of unanticipated vulnerabilities	Identification of both known and unknown vulnerabilities, verification against most common vulnerabilities for respective application technology type/category.
B4		Application and infrastructure level vulnerabilities identification	Identification conducted on both application and technology infrastructure layer.

7.3. Appendix A – 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 Compliance & Vulnerability Management Standard document has been uplifted into this standard. 3) Consultation feedback, corrections incorporated	Material	Gareth Carrigan	1.0	04-Jun19	04-Jun-19
CISRO ICS Policy	Based on ICS Change request	Non-material	Liz Banbury	1.1	17-Dec19	17-Dec-19

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	forum, security configuration validation for systems S-BIA rated 1-3 has been changed to quarterly [Table 1]					
CISRO ICS Policy	Based on ICS Change request forum definition of unauthorized network services added to glossary [ICSCR-17Dec2019-1 - Extend glossary of VIAM Standard]	Non-material	Liz Banbury	1.2	27-Jan20	27-Jan-20
CISRO ICS Policy	Annual Review	Material	Liz Banbury	2.0	02-Oct20	02-Oct-20
CISRO ICS Policy	Annual review:	Material	Samantha Finan,	3.0	10-Dec21	01-Jan-22
	Risks, Roles and Responsibilities aligned to RTF. Introduction of changes from ICSCR-4Mar2021-1, ICSCR-30Jun2021-1, ICSCR-21Jan2021-1 **Controls updated:** VIAM040, VIAM-130, VIAM-310, VIAM400 **New controls:** VIAM-131, VIAM132, VIAM-420, VIAM-430 **Controls removed:**		Global Head, ICS Policy, Standards and Reporting			

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	VIAM030 **Updated Table 1** (Vulnerability Identification Frequency)					
CISRO ICS Policy	Based on Change Requests and additional standard review: **New:** VIAM-125, VIAM-245, VIAM-246, VIAM-247 **Updated:** VIAM-250, VIAM-390, VIAM-410, Table 7.1 **Administrative:** VIAM-091, VIAM090 **Removed:** VIAM-230, VIAM-260, Table 7.4	Material	Samantha Finan, Global Head, ICS Policy, Standards and Reporting	4.0	22-Jun22	01-Jul-22
CISRO ICS Policy	Annual review:	Material	Paul Hoare	5.0	18-Dec23	24-Jun-24
	1. Document template updated in line with the Template for Group Standards V5.6 2. ICS controls from the Security Patch Management Standard embedded in the VIAM Standard 3. The Standard name changed to ICS Vulnerability and Security Patch		Head, ICS Policy and Best Practice			

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	Management Standard The Standard structure and approach aligned with the ICS Standards simplification Strategy					
Katarzyna Wencka **[ICS Standards]**	Administrative changes introduced to update document template, references, roles and ownership.	Non-material	Jamie Cowan Head, ICS Risk Framework & Governance	5.1	04-Dec24	16-Dec-24

8. Version Control Table

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Katarzyna Wencka **[ICS Standards]**	Administrative changes introduced to update document template, references, roles and ownership.	Non-material	Jamie Cowan Head, ICS Risk Framework & Governance	5.1	04-Dec24	16-Dec-24