Status: *Live*
Version: *2.4*

Threat and Vulnerability Management Standard




Table of Contents

1. Standards

1.1 Vulnerability Management

This standard provides requirements for the ongoing identification, prioritization, and remediation of vulnerabilities or information assets/systems within Diageo environment. All vulnerability management activities must align to the Common Vulnerability Scoring System version 3 (CVSS v3) & 2 (CVSS v2). There is a maximum annual time period allowed between scans.

Information assets/systems includes Hardware, Software, Mobile devices, Supply, Manufacturing & Operational Technology (OT) systems, recording media (e.g. external storage) and must include:

- Network devices and systems such as network switches, servers, NAS or SAN storage solutions
- Mobile devices such as tablets and smartphones (*Section 1.9 is only valid/relevant*)
- Servers and web applications, Enterprise Resource Planning (ERP) & Supply Chain Management (SCM) applications and cloud based applications
- Some client applications running on platforms such as desktop workstations, laptop computers and mobile devices
- Only applications installed as part of a Diageo standard build should be considered for vulnerability management.

System and software vulnerabilities associated with business applications, information systems and network devices must be managed by scanning for vulnerabilities. Patches and configuration changes must be applied as per defined patching and change management processes.

Findings shall be fed into configuration and hardening standards to ensure new system or application rollouts do not result in the same vulnerabilities when subsequently tested during regular scans or a project's task prior to going live.

Vulnerability scanning must be:

a) restricted to a limited number of authorised individuals (e.g. using a dedicated account that is only used for vulnerability scanning)
b) using approved and dedicated systems (e.g. using predetermined, static IP addresses)
c) monitored (e.g. to identify misuse by authorised individuals or help detect unauthorised scanning)

System and software vulnerabilities must be remediated using a patch management process, which:

a) specifies methods of validating patches (e.g. ensuring that the patch is from an authorised source)
b) assesses the business impact of implementing patches or not
c) ensures patches are tested prior to implementation
d) describes methods of deploying patches according to a regulated schedule (e.g. grouping multiple patches and using software distribution tools)
e) reports on the status of patch deployment across the organization

f) includes methods of dealing with the failed deployment of a patch (e.g. rollback and redeployment of the patch)
g) includes emergency patching criteria, approvals and steps in the event of an unforeseen event, incident or change introducing instability to the operating environment(s)

Other methods which can be used to remediate vulnerabilities include configuration changes, code fixes and design changes.

The system and software vulnerability management process requires performing vulnerability scans of critical and sensitive business applications, information systems and network devices to help:

a) identify system and software vulnerabilities that are present in business applications, information systems and network devices
b) determine and prevent business applications, information systems and network devices exposure to cyber threats, malware or accidental errors.
c) prioritise remediation of vulnerabilities (e.g. using the vendor's patch release schedule)
d) provide a high-level view of vulnerabilities across the organisation's technology (e.g. to compare and identify trends).

Other mitigating factors such as disabling services or removing software should also be used where appropriate.

In the rarest of cases, and dependent upon business stakeholder agreement, a system or application can be disconnected from the network until remediation can take place.

All third-party vendors conducting vulnerability management activities must have a documented process. This process is to be reviewed on an annual basis and signed off by Diageo (Global Operations & Engineering).

A proportionate view, based on risk, must be taken and the versions updated accordingly having regard to the state of the art of technological innovations available and the level of harm that may be suffered if a security beach were to occur. Special care should be applied to any information that may amount to Personally Identifiable information (PII) or Special PII (please see Diageo's Data Privacy Global Policy and Information Handling Standard, which should be read in conjunction with this Standard). This standard is applicable only for security patches but expected timelines can be found in Appendix II and with more details in Patching & Vulnerability Management Security Framework.

Functional patches are at the discretion of the business owner. Anti-malware/Anti-virus definitions must always be up to date, updated on a daily (as a minimum) basis.

1.2 Server Scanning

All servers must be scanned regularly for known vulnerabilities. Scans must be non-intrusive and must run under a privileged (authenticated) account to allow full scanning. Every server must be scanned on *at least an annual basis*. High sensitivity/criticality for a server would result in an increased frequency of scanning. The scan frequency must be based on priority and risk of the asset. The remediation timetable should also be based on the following criteria:

- ***Data sensitive systems containing highly confidential information*** (as per Information Asset Inventory) and **systems hosting "Crown Jewel" applications** (according to FocalPoint) must be scanned *at least quarterly*.
- ***High risk systems*** under threat based on internal and external threat intelligence shall be scanned quarterly
- **All other systems** must be scanned *at least once per year*.
- All scan summary reports must be made available to IM&S on demand.

Scan-generated warnings (as opposed to actual known vulnerabilities) which detail configuration issues should be remediated.

1.2.1 Vulnerability Remediation

These recommended remediation targets are based on CVSS V3.0 and CVSS V2.0 and industry best practice (e.g. SANS, NIST).

Expected timelines per vulnerability (IAW severity rating per NIST NVD and First.org CVSS scores - both versions)			**NIST National Vulnerability Database**
Severity rating	**CVSS Score**	**DIAGEO SLA**	**Technology assets & applications benefit from a robust and timely patching schedule. By managing & reducing the risk exposure. Recommend you create action plans to fix vulnerabilities published or found during automated scanning activities. *PRIORITY TO PATCH OR FIX IS BASED ON SEVERITY RATING***
Low	0.1-3.9	Risk-based	
Medium *	4.0-6.9	60-180 days	
High	7.0-8.9	30 days	
Critical **	9.0-10.0	15 Days	

There are no exceptions for Critical and High severity ratings, regardless of the technology or operating system the vulnerability affects, e.g., MS, LINUX, UNIX, etc. This overrides the normal patching cycles (outlined in the Patching & Vulnerability Framework -see Appendix 2). Where the above requirements cannot apply, a special risk assessment shall be done by the IM&S team to ensure the right mitigation and plan steps are mobilized to reduce the risks where practicable - on a case by case basis and during the monthly JSEP (Diageo & TCS) call.

* AIX server patches are released by IBM every 6 months and cannot be patched more frequently – unless an "critical emergency" situation exists, e.g., a break & fix is necessary or when an attack, data breach or operational disruption is likely

** "Critical" Microsoft security updates and patches are to be managed within the "High" ratings above – unless an "critical emergency" situation exists, e.g., a break & fix is necessary or when an attack, data breach or operational disruption is likely

1.2.2 Patching

Patching expected timelines – See Appendix II for details

1.3 Critical Applications

Critical applications must be periodically scanned for application logic vulnerabilities.

Note: A critical application is any system which, if compromised, would have a significant impact on financial and business operations. Critical applications are denoted by a field in Focal point.

1.4 Non-Critical Applications

Applications (Adobe, Firefox etc.) which are not used for production services, should be scanned, and any vulnerabilities remediated as per process for OS and application remediation. Such vulnerabilities should be given identical priority to other discovered vulnerabilities.

1.5 Malware Awareness

User awareness activities should include appropriate awareness relating to threats, viruses and general malware. Through these training activities End Users must be informed about:

- prevalence of malware and associated risks (e.g. unauthorised access to critical business applications, corruption of critical business information, theft or unauthorized disclosure of sensitive information)
- ways in which malware can install itself on computing devices
- common symptoms of malware infection (e.g. poor system performance, unexpected application behaviour, sudden termination of an application).
- not installing software from untrusted sources, opening untrusted attachments or clicking on suspicious or unknown hyperlinks within emails or documents.

End users should be

- notified quickly of significant new malware-related risks (e.g. by email, freeware or suspicious websites)
- instructed to report suspected or actual malware to CSI@Diageo.com

1.6 Malware Protection

A defense-in-depth approach is applied to ensure anti-malware tools and training is given to protect data, information and other technology assets against infection and harmful events.

Malware protection software must be installed on systems e.g.,

(a) servers (e.g. servers that are at risk from malware, such as file and print servers, application servers, web servers and database servers)
(b) messaging gateways (e.g. email and web proxy servers that scan network traffic and electronic messages in real time) to minimize malware reaching computing devices
(c) computing devices (e.g. desktop computers and laptops)
(d) Information systems that support or enable the organisation's critical infrastructure (e.g. embedded systems and industrial control systems where the malware protection software is available [process control PCs, and programmable logic controllers: PLCs]).

Malware protection software should be distributed automatically. Updated frequently (daily if possible) to prevent the newest flavor of attack.

A patch management process/procedure must exist for each asset being protected, including those managed by third parties.

Malware protection software should be configured to scan:

- the master boot record (MBR) of hard disk drives (a popular target for boot sector-infecting viruses)
- targeted files (including executables, image files such as JPEG, document formats such as Adobe PDF and macro files in desktop software)
- protected files (e.g. compressed or password-protected files) where possible
- portable storage media (e.g. CDs, DVDs and USB storage devices) immediately upon loading or connection to computer equipment
- network folders immediately upon being mounted/shared
- network traffic entering the corporate network (including email and downloads from the Internet)
- network traffic leaving the corporate network (including email attachments and shared documents).
- Malware protection software should be configured to be active at all times (e.g. by scanning files as they are accessed to provide real-time protection, or by being configured to be active at all times and to restart if stopped)
- perform scheduled scanning at predetermined times
- provide a notification when suspected malware is identified (e.g. by producing an event log entry and providing an alert)
- disable and quarantine files suspected of containing malware (e.g. for further investigation)
- remove malware and any associated files immediately upon detection
- ensure that important settings cannot be disabled, or functionality altered.

1.7 Methods of Malware Detection to be used

(i) Signature-based anti-virus detection: This must be implemented by default.

(ii) Behavior-based malware detection: If available.

1.8 Mobile devices

Mobile devices must be enrolled in Diageo's MDM platform which will apply the following restrictions;

- Encryption – devices must be encrypted
- Rooted/Jailbroken devices must be blocked
- Remote wip
- Password – suitable strength password policies must be enforced. Microsoft Intune requires that at least 4 digit pin code must be used

See the Mobile Computing Standard for more information.

1.9 Security Event Logging

New systems deployed should be compatible with Logging Standard and existing SIEM technologies. Legacy systems which are incompatible with existing SIEM technologies should be replaced as part of refresh cycles.

1.10 System and Network Monitoring

System and network activity should be monitored for potentially suspicious activity based on criticality.

Systems and network devices should be scanned on a quarterly basis to remediate vulnerabilities and hardening configuration requirements.

Details relating to system/network monitoring should be retained to meet legal/regulatory requirements.

- System/network availability (i.e. response and up-time) should be measured from the perspective of business users by monitoring information system and network performance

Usage reports from service providers (e.g. service reports from Verizon) should be examined to discover any unusual activity on information systems and networks and investigated to repair/remove any future occurrence of unusual activities.

System/network monitoring activities should look for and identify:

(a) unauthorised scanning of business applications, information systems and networks
(b) successful and unsuccessful attempts to access restricted access resources (e.g. DNS servers, web portals and file shares)
(c) unauthorised changes to user accounts and access rights (to detect privilege escalation)

The results of monitoring activities should be reviewed by the owners of business applications, information systems and networks. Follow-up activities should fix the results where necessary.

1.11 Intrusion Detection

Network ingress/egress points must be monitored for malicious activity.

Network intrusion detection systems should be installed and configured in “stealth” mode so that they are difficult to detect or attack.

Intrusion detection alerts must be monitored and responded to as appropriate.

Intrusion detection software should be:

a) updated automatically and within defined timescales, e.g. delivery of distribution attack signature files to intrusion detection sensors via a central management console

b) configured to send an alert when suspicious activity is detected
c) Handled as a security incident

Suspected intrusions should be analyzed, assessed for business impact and include:

(a) confirm whether an attack is actually occurring (e.g. by eliminating false positives)
(b) determine the type of attack (e.g. worms, buffer overflows or denial of service)
(c) identify original point of attack
(d) quantify the impact of an attack.

The status of an attack should be assessed in terms of both scale and time elapsed from when notification begins.

All attacks should be reported to **CSI@Diageo.com**.

2. Measurements

2.1 Critical Success Factors

- Correct configuration of key servers for logging
- Identification and correct location of intrusion detection systems

2.2 KPI Measures

The following KPIs are recommended to confirm effectiveness of vulnerability management, security and AV patching operations.

Control	KPI
Vulnerability Scan Schedule	Ensure the vulnerability scan cycles on track (Critical systems - Quarterly and Non-Critical – Annually)
Patch Management	Detailed SLA for patching is in Appendix II and in Patching & Vulnerability Management Security Framework.
Antivirus Signature update	Maintain >90% antivirus signature updates on workstation and server level
Detection of virus / malware infection	Timely detection on virus / malware infections (keep trend low from actuals)
Respond on virus / malware infection and vulnerabilities (ie: open ports, etc)	Timely respond clean / quarantine on infections and vulnerabilities (keep trend low from actuals)

The appendix provides further recommendations for vulnerability management program report requirements.

3. Deliverables and Reports

Reports will be produced identifying compliance to the ongoing security activities defined in this standard and to outline detected security exceptions and incidents.

4. Glossary, Acronyms and References

Term	Definition
KPI	Key Performance Indicator
IDS	Intrusion Detection System
IPS	Intrusion Protection System
Zero-Day Vulnerability	An attack on a software flaw that occurs before the software's developers have had time to develop a patch for the flaw is often known as a zero-day exploit. The term "zero-day" denotes that developers have had zero days to fix the vulnerability.

5. Audience

- Technical staff (e.g. Global Operations & Engineering, Enterprise Architecture, TCS and other vendors) should review and adhere to this standard when developing and maintaining vulnerability management solutions for Diageo. Any areas a vendor cannot comply with should be referred to IM&S for advice.
- The BRM community to ensure that any local market systems are up-to-date with available patches.
- The Supply Management community to ensure that any manufacturing systems and supporting infrastructure are up-to-date with available patches.
- Corporate Security – IM&S and Corporate Security work together to ensure a seamless approach to threat response.
- Diageo's 3rd parties, suppliers and vendors are to ensure their threat identification and response products are fit-for-purpose and comply with principles similar to this standard in nature.

6. Scope

Failure to address threats in the right way will lead to operational disruption, theft/loss of proprietary assets which negatively affects business performance, customer sentiment, market share and reputational damage. Cyber-threats are continually evolving (complex, sophisticated, persistent and potentially destructive) and evolving each year. New and emerging threats are always appearing, and

some threats are no longer relevant. Diageo must actively determine its own threat profile and this will be based on factors such as our business sector (regulatory), geographical presence, line of business (alcohol and online retaining/digital marketing), changes in overall threat landscape and plan effective measures against the most likely new threats and the most prevalent current ones. We are informed about our current and future risk landscape by internal security data, external threat input along with breach and incident data. We regularly review and revise the threat profile based on changing variables such as IT trends.

This standard aligns to the timelines, frequencies and guidance in the "Patching & Vulnerability Management Security Framework."

The scope includes:

- Our approach, processes and tools for identifying and countering known cyber threats & discovering new emerging threats and finding ways to identify these
- Protection from known threats to the Diageo environment
- The remediation of known and identified vulnerabilities within the Diageo and 3rd party provided environments

All processes and procedures referred to in this document are defined as Global in nature and therefore must be adhered to globally.

7. Objectives

The objective is to ensure a consistent, repeatable and auditable approach for conducting threat and vulnerability management within the Diageo environment. This should be achieved regardless of the source of threat or the platform in which a vulnerability is located.

8. Exceptions

Exceptions to this document can only be granted in accordance with the Diageo IM&S Policy Framework. Applications for exceptions are requested through the ServiceNow via the Diageo Information Security Exception Approval Process.

9. Incident Reporting

Any failure to comply with this document or security incident that materialises relating to the requirements within this document must be reported to the Diageo Computer Security Incident (CSI) team by email at CSI@Diageo.com.

Document Location

The current document will be held online in the Diageo Mosaic repository:

Site: Mosaic IM&S Document Library

Directory/File: Standards Folder

This file will also be available for Diageo Employees in the IM&S Codes & Policies public site on Mosaic.

Printed copies are valid only on the day of printing. It is the responsibility of users of this document to ensure they are using the most recent version. If the online location is not reachable, a copy of this document can be obtained from the Global IM&S team.

Revision History

This document is subject to Change Control and as such any amendments must be carried out through the Document Change Management process and all Approvers must agree the amendments.

Date of this revision	27th Mar 2018	Date of next review	8th Nov 2018

Version Number	Revision Date	Change History	Changes Marked	Updated By
2.4	20/3/2018	Interim change: Patching & remediation timelines and frequencies aligned according to the new " Patching & Vulnerability Management Security Framework"	Yes	Tamas Sziller & Jane Smith
2.3	06/11/2017	Minor readability and grammar corrections were made to the whole Standard and related content has been also added to bring in line with requirements of ITGC Framework. Specific KPIs for vulnerability management, security and AV were added.	Yes	Jane Smith, Thiagarajan Sundaravadanam, Thiagarajan, Tamas Sziller
2.2	25/04/2017	Reviewed and updated as per annual cycle, key changes were made to the security patching requirements (section 1.1) which has been changed from a general (at least version n-2) rule to a more realistic 'risk-based' standard. Server scanning section has been extended with High-risk systems (section 1.2), also section 1.12 about IP is new and recommended KPIs for the *Vulnerability Management program* report in Appendix were added as well.	N/A	Paul Galbraith

2.1	24/06/2016	Amended as part of IM&S PSG Update process.	N/A	Steven Markey
2	30/3/2016	Updated sections 1.1 to 1.10 (with ISF SoGP Controls) and added section 1.4 (Methods of Malware detection). Put standards at start of doc.	Y	John Haren
1.2	15/12/2015	Added builds in section 5.1, amended table 1.1 entry to read “section 9.2”	Y	Paul Galbraith
1.1	5/12/2014	Added new related documentation (section 9.6). Added section 4 (Target Audience & Incident Reporting)	Y	John Haren
1.0	19/12/2013	Updated document after review by team. Originally started as a process but it was agreed this should be a standard document. Live version	N/A	John Haren

Reviewers

This document requires to be reviewed by the following reviewers.

Name	Title	Approved Date
John Haren	IM&S Head of Governance, Risk & Compliance	Mar 2018
Jane Smith	Information Security Risk Specialist	Mar 2018
John Merritt	Global Information Security Director	Nov 2017
Thiagarajan Sundaravadanam	Regional Information Protection Specialist	Nov 2017
Arvind S	Cyber Threat and Intelligence Lead	Nov 2017
Malcolm Ellis	Director of Network Infrastructure, (EA)	Jan 2017
Stuart D Holmes	Global Security Engineering and Ops Lead	Nov 2017

Approvals – Document Signoff (acceptance)

This document requires following approvals.

Name	Title	Approved Date
John Haren	IM&S Head of Governance, Risk & Compliance	28 Mar2018

Distribution List

Once complete, this document will be distributed to:

Title (including company)
Above Approver List
Enterprise Architecture Team
Global Operations & Engineering
TCS
BRM Community

Related Documentation

The following documentation can be found on the **ITIL Process site** on Mosaic;

Diageo Information Security Risk Management Process
Information Security Exception Approval Process

The following document can be found on the Global Policies site.

IM&S Global Policy

The following documentation can be found on the **IM&S Document site** on Mosaic.

Acceptable Use Policy

Diageo Vulnerability Management Program (Available from TCS)

The Accountable Party for this Standard coordinates and insures that the document is completed. This individual as well as others in the IT areas may also contribute in a collaborative fashion as is often necessary.

APPENDIX I.

Reporting Criteria: A TVM program must generate stats on a regular basis. The following are the recommended KPIs for a vulnerability management program report.

- **Vulnerability Title**
- **QID, CVE ID wherever reported**
- **Threat Description**
- **Solution Description**
- **List of assets affected by the vulnerability**
- **Category of assets affected by the vulnerability**
- **Vulnerability age (No. of days since identified during scan)**
- **Platform Used By Affected Assets (Operating System / Application / Software)**
- **Vulnerability Remediation Action**
- **Target date for completion**
- **Action owner**
- **Vulnerability remediation status (Red / Amber / Green)**
- **Risk acceptance description**
- **Risk ID**
- **Risk acceptance date**
- **Risk accepted by**

APPENDIX II.

NOTE: Technology assets include, e.g., Firmware updates, Server patches, Vulnerability fixes & patches, Database, add-ons, plug-ins, etc. This is not a comprehensive list.

Patching expected timelines			
PATCH MANAGEMENT FREQUENCY - For exceptions Vulnerability Scan/Pen Test results, emergency, security and CVE notifications			
UNIX (Non-SAP)	30 days	Unmanaged / legacy devices and apps	Depends on severity level
Windows	30 days	Workstations (incl. Diageo Anywhere)	30 days
VMware	30 days	Mobile devices	Service provider / user responsibility to download and install
SQL Database	30 days	CVE notification	Depends on severity level
Oracle Database (non-SAP)	30 days	Vulnerability scan	Depends on severity level
SAP OS (AIX)	6 months	Penetration test	Depends on severity level
SAP DB (Oracle)	6 months	Patch & vulnerability tracking	Update ASAP
SAP Kernel patching	6 Months	KPI & dashboard reporting	Monthly / Quarterly
Applications	30 days	Feed fixes into hardening standards	Update ASAP
Firmware updates	30 days - 6 months	Exception approval & processing	Update ASAP
Network infrastructure & devices	30 days - 6 months	All other technology	Update ASAP

SPECIAL CONSIDERATIONS:
1. Applications & Manufacturing patching or remediation may need testing or more time because of infrequent planned downtimes.
2. Vulnerability and patching severity levels are rarely "downgraded" unless a risk assessment is done. An exception must be approved.
3. Configuration or other remediation fixes that can be done without downtime shall be done as soon as possible.
4. Internet facing technology at Data Centres is always a higher priority to patch and remediate than internal technology. Both must be done within SLA.
5. All technology assets should be patched and remediated including those scheduled for de-commissioning.
6. Vulnerability patching and remediation fixes should be done on all assets with the same OS or configuration based on severity ratings.
7. ALL scans, re-scans or checks resulting in new Critical or High vulnerability(ies) are managed routinely
8. Recommendation: Develop a RASCI to support your functional or local patch and vulnerability management processes

APPENDIX III.

Suitable KPIs for Dashboard or Reporting		
SLA (within)	**KPI 1 - EXAMPLE Percentage done on time < 90%=Red Between 90-94.9%=Amber**	**KPI 2 - EXAMPLE Percentage overdue >10%=Red >5%=Amber)**
180 days	Microsoft servers	Microsoft servers
60 days	Microsoft servers	Microsoft servers
30 days	Microsoft servers	Microsoft servers
15 Days	Microsoft servers	Microsoft servers

Note: CARM Controls (C1235 Patching & C1274 Vulnerability Management) illustrate that all teams adhere to the above & exception processing requirements

End of Document