Cybersecurity Risk Management

IT product Risk Assessment

1 All IT products procured, produced, hosted, managed, or operated by or on behalf of WHO, or by WHO on behalf of a member state or other entity are subject to classification under the Cybersecurity Risk Assessment Guideline.

2 All such IT products must comply with the controls determined by that classification, by the hosting model, and technologies used in the product, as explained in the Cybersecurity Risk Assessment Guideline, or must seek a specific, time-bounded exception from CISO or from a combination of ADG BOS and their own ADG.

Cybersecurity Vulnerability Management

Vulnerability reporting and sources

3 Vulnerabilities come to the attention of the Cybersecurity team from several different sources, including but not limited to IT system infrastructure scanning, IT system penetration testing by team members or others, rules which cannot be fulfilled during the Cybersecurity Risk Assessment, and vulnerabilities reported by external ethical hacker researchers.

4 Vulnerability scanning is managed by the Cybersecurity team, and takes place at set intervals, normally no more than 2 weeks apart.

5 Penetration testing is done manually by members of the Cybersecurity team, or by external penetration testers hired by the IT product owner.

6 External security researchers report vulnerabilities via the mechanism of their choice. However, the preferred method is by email to vulnerability@who.int as described on the WHO public website.

7 Vulnerabilities reported by external researchers are triaged and validated by members of the Cybersecurity team before they are considered a reportable vulnerability.

8 External researchers who report vulnerabilities are eligible for recognition according to the rules described in the WHO public website.

Scoring and prioritization of vulnerabilities

9 Regardless of the source, vulnerabilities will be scored by members of the Cybersecurity team according to an internal version of the CVSS, and then assigned to a priority group, from priority 0 to 4 (P0 – P4). Priority 5 (P5) is purely informational only.

10 Out-of-support software or components will always be assigned to priority 0 unless the vendor has a post end-of-life support scheme to which the product owner subscribes, at the product sponsorship's expense.

Vulnerability remediation and mitigation

11 The responsibility for remediation of a given vulnerability falls upon the IT product owner of the system in which the vulnerability was found. The overarching rule is that responsibility for remediation and mitigation lies with the team which introduces the vulnerability into the WHO environment, and that they must not expect another part of the Organization, including the Cybersecurity team to pay to remediate the vulnerabilities they introduce.

12 Some vulnerabilities are due to the interactions between several systems. In this case, the primary responsibility is with the owner of the system which triggered the vulnerability; however, the underlying vulnerability in the older system must also be addressed. For this reason, the Cybersecurity team may choose to split a vulnerability into two separate vulnerabilities. However, in this case the risk assigned to the original vulnerability will be assigned to the two resulting vulnerabilities, even if they would normally have a lower risk individually.

13 Priority 0 (out-of-support by the vendor) vulnerabilities must be addressed with the utmost urgency upon their discovery. Continuing to operate a product with a priority 0 vulnerability requires that a formal risk exception be approved by the CISO, CIO, and by the officer with signatory authority for the department in the sponsoring chain of command. See paragraph 25 for a related document about timelines.

14 IT Products in the project phase must not go live in production with unaddressed vulnerabilities in priorities 0-2.

15 Existing products with priority 1 and 2 vulnerabilities may also require a formal exception process, at the CISO's discretion based on the product team's response when informed. For example, a vulnerability which the product team or their vendor expects to resolve within a few days would not require a formal exception process. However, if for some reason the product team or their vendors cannot address the issue in a timely manner, then a formal risk exception will be required. Acceptance of the risk will depend on any mitigating action proposed.

16 Vulnerabilities in priorities 3-4 must be addressed as soon as practical. Product owners must be aware that a lower risk and thus lower priority vulnerability might become more serious considering another vulnerability in the same product, or even one in a different product. The Cybersecurity team is responsible for communicating with that concept, but the product team is responsible for mitigating priorities 3 and 4 vulnerability priorities.

Vulnerability database, and responsibility assignment

17 The Cybersecurity team shall maintain an approved API integration between the vulnerability scanning platform and the WHO IT service management platform.

18 All vulnerabilities detected by Tenable shall be ingested automatically into The WHO IT service management platform without manual intervention.

19 Each ingested vulnerability will be created as a vulnerable item to enable centralized tracking, reporting, and governance.

20 Vulnerabilities must be prioritized according to the severity levels defined by the Cybersecurity team. For high-priority vulnerabilities (P0, P1, P2), remediation tasks will be created for the top five open items at any given time.

21 For medium- and low-priority vulnerabilities (P3, P4), remediation tasks will be created for the top two open items at any given time.

22 The remediation task queue must update automatically so that when a task is closed, the next outstanding vulnerability of the same priority is promoted into the queue.

23 Vulnerabilities identified through penetration tests or reported by external security researchers will be manually recorded in The WHO IT service management platform as vulnerable items. These entries must not generate automated remediation tasks. Instead, corresponding incidents must be raised and assigned to the technical owners responsible. Oversight of this process shall remain with the Cybersecurity Team.

24 All vulnerable items, remediation tasks, and related incidents will be assigned to the appropriate ownership groups. Ownership must be clearly defined, traceable, and enforceable. Automated notifications, reminders, and escalations must be issued to the relevant Cybersecurity Regional Focal Points and IT Regional Managers to support timely remediation in line with established service level expectations.

25 Assignees must accept or reject any vulnerabilities assigned to them within a reasonable delay, which will be enforced by The WHO IT service management platform.

26 Assignees must address vulnerabilities within a timeframe defined in the vulnerability management standard operating procedure document.

27 All vulnerabilities must be remediated within the timeframes defined by their assigned priority level in the related document Vulnerability Management Priority Definitions and Remediation Timeline.

28 The Timelines in that document should be reviewed and, if necessary, updated every six calendar months, with the agreement of the Global Cybersecurity Group.

Data Encryption

29 All sensitive data must be encrypted while in transit over untrusted networks, including but not limited to, the Public Internet and WHO end-user networks.

30 Cryptographic systems that have been proven to be weak must not be used to provide cryptographic services.

31 The control requirements outlined in this document must reflect a risk-based approach to identify the required level of protection taking into account the information to be protected.