

Procedure for Vulnerability Management

Policy Statement

World Bank is committed to a proactive and systematic Vulnerability Management Program designed to identify, assess, prioritize, remediate, and report on security vulnerabilities across all its Information Technology (IT) assets. This program aims to minimize the risk of exploitation, protect the Bank's data and systems, ensure operational resilience, and maintain compliance with regulatory requirements.

Scope

This procedure applies to all IT assets owned, managed, or utilized by World Bank, including but not limited to networks, servers (physical and virtual), workstations, applications (both internally developed and third-party), databases, mobile devices, Internet of Things (IoT) devices, and cloud services. It encompasses vulnerabilities in operating systems, software applications, firmware, and configurations.

Roles and Responsibilities

Effective vulnerability management is a collaborative effort involving multiple teams :

- **Chief Information Security Officer (CISO) / Security Manager:** Owns the Vulnerability Management Program, defines and approves the policy and procedures, ensures adequate resources are allocated, oversees the risk management process related to vulnerabilities, and makes final decisions on risk acceptance.
- **Security Operations Center (SOC) / Cybersecurity Team:** Responsible for the operational execution of the vulnerability management lifecycle. This includes configuring and running vulnerability scans, analyzing scan results, validating findings, assisting in the prioritization of vulnerabilities, tracking remediation efforts, managing vulnerability disclosure processes, and generating vulnerability management reports.
- **IT Operations (IT Ops):** Accountable for the remediation of vulnerabilities related to infrastructure components, such as operating systems, network devices, and servers. This primarily involves patch deployment and secure configuration management.
- **Application Owners / Development Teams:** Responsible for remediating vulnerabilities specific to the applications they own or develop. This includes applying vendor patches for COTS software or developing and deploying code fixes for in-house applications.
- **Asset Owners:** Individuals or departments accountable for specific IT assets. They are responsible for ensuring that vulnerabilities identified on their assets are addressed in accordance with this procedure and within defined Service Level Agreements (SLAs).

- **Risk Management Team:** Collaborates with the Cybersecurity Team to assess the business impact of vulnerabilities and to review risk acceptance requests.

Vulnerability Management Lifecycle

World Bank adheres to a structured, multi-phase lifecycle for managing vulnerabilities, ensuring a consistent and effective approach :

1. Discovery / Identification:

The objective of this phase is to comprehensively identify vulnerabilities across all in-scope World Bank assets.

- **Comprehensive Asset Inventory:** Maintain an accurate and up-to-date inventory of all IT assets, as detailed in the Asset Lifecycle Document. This inventory is crucial for ensuring complete scan coverage.
- **Regular Vulnerability Scanning:** Conduct automated vulnerability scans of all in-scope assets at predefined frequencies. This includes:
 - Network-based scans (internal and external) to identify network service vulnerabilities.
 - Host-based scans (authenticated/credentialed scans) to identify vulnerabilities in operating systems and installed software on servers and workstations.
 - Web application scans (DAST) to identify vulnerabilities in web applications (e.g., OWASP Top 10).
 - Database vulnerability scans.
 - Cloud configuration posture management (CSPM) scans for cloud assets.
- **Penetration Testing:** Perform regular penetration tests (both internal and external) on critical systems, applications (especially financial transaction systems), and network perimeters. These tests are conducted by independent internal teams or qualified external third parties.
- **Threat Intelligence and Advisory Monitoring:** Continuously monitor vendor security advisories, public vulnerability databases (e.g., CVE, NVD), security mailing lists, and commercial threat intelligence feeds to proactively identify newly disclosed vulnerabilities relevant to World Bank's technology stack.
- **Vulnerability Disclosure Program (VDP):** Maintain a VDP that allows external security researchers to responsibly report potential vulnerabilities discovered in

World Bank's public-facing systems. All submissions are triaged and validated by the Cybersecurity Team.

- **Software Composition Analysis (SCA):** Integrate SCA tools into the SDLC to identify vulnerabilities in third-party and open-source software components.
- *Security Manager's Perspective:* At World Bank, our discovery strategy employs a defense-in-depth approach. We utilize a suite of leading commercial vulnerability scanning tools, augmented by specialized financial application security testing services. For our core banking platforms and international payment systems, continuous monitoring and more frequent, targeted scanning are implemented due to their criticality and high-risk profile.

2. Analysis & Assessment

Once potential vulnerabilities are identified, they must be analyzed and assessed to understand their true risk to World Bank.

- **Validation:** All identified vulnerabilities must be validated by the Cybersecurity Team to confirm their existence and applicability, thereby eliminating false positives.
- **Severity Scoring:** Assign a severity score to each validated vulnerability using the Common Vulnerability Scoring System (CVSS). The current version of CVSS is used, and both base, temporal, and environmental scores are considered where applicable.
- **Business Impact Analysis:** Evaluate the potential business impact if a vulnerability is exploited. This considers:
 - The criticality of the affected asset(s) (e.g., systems supporting critical financial operations).
 - The sensitivity of the data potentially exposed or compromised (e.g., customer PII, confidential financial data, strategic bank information).
 - Potential operational disruption, financial loss, reputational damage, and legal/regulatory consequences.
- **Exploitability Assessment:** Determine the likelihood of a vulnerability being exploited. This includes considering the availability of public exploit code, the complexity of the attack, required attacker privileges, and user interaction needed. Information from threat intelligence feeds on active exploitation in the wild is a key factor.
- **Contextualization:** Analyze vulnerabilities within the context of World Bank's specific environment, including existing compensating controls (e.g., web

application firewalls, network segmentation, intrusion prevention systems) that might reduce the effective risk.

3. Prioritization

Not all vulnerabilities can be remediated simultaneously. Prioritization ensures that resources are focused on addressing the most significant risks first.

- **Risk-Based Prioritization:** Vulnerabilities are prioritized for remediation based on a holistic risk assessment that combines the CVSS severity score, business impact, asset criticality, exploitability, and current threat intelligence (e.g., vulnerabilities known to be actively exploited).
- **Focus on Critical Risks:** Highest priority is given to vulnerabilities that, if exploited, could lead to significant financial loss, compromise of sensitive World Bank or customer data, major operational disruptions, or severe reputational damage.
- *Use Case (Vulnerability Prioritization at World Bank):* A newly discovered vulnerability with a CVSS base score of 9.8 (Critical) is found on an internal development server that contains no production data and is isolated from the main network. Concurrently, a vulnerability with a CVSS score of 7.5 (High) is identified on an internet-facing production server that processes international fund transfers, and threat intelligence indicates active exploits are available for this vulnerability. The High-severity vulnerability on the production server is assigned a higher remediation priority due to its greater business impact and exploitability, despite the development server vulnerability having a higher raw CVSS score.

4. Remediation / Mitigation

This phase involves taking action to address prioritized vulnerabilities.

- **Patching:** Applying vendor-supplied patches is the primary method for remediating known software vulnerabilities. This must be done in accordance with the World Bank Patch Management Policy.
- **Configuration Changes:** Modifying system or application configurations to eliminate vulnerabilities (e.g., disabling insecure protocols, strengthening encryption ciphers, correcting permission settings).
- **Code Fixes:** For vulnerabilities in internally developed applications, development teams are responsible for creating and deploying secure code fixes.
- **Compensating Controls:** If a patch or direct fix is not immediately available or cannot be deployed without unacceptable operational impact, temporary

compensating controls may be implemented to reduce the likelihood or impact of exploitation. Examples include deploying specific Web Application Firewall (WAF) rules, enhancing monitoring around the vulnerable asset, restricting network access, or disabling specific functionalities. Compensating controls are documented and regularly reviewed.

- **Remediation Service Level Agreements (SLAs):** World Bank enforces strict SLAs for vulnerability remediation, based on the assigned priority/severity level. These SLAs define the maximum allowable time to remediate a vulnerability once it has been confirmed and prioritized.
 - *World Bank Vulnerability Remediation SLAs:*
 - **Critical Severity:** Remediation within 7 calendar days. For vulnerabilities with known active exploits targeting financial institutions, remediation or effective mitigation is required within 48 hours.
 - **High Severity:** Remediation within 30 calendar days.
 - **Medium Severity:** Remediation within 90 calendar days.
 - **Low Severity:** Remediation within 180 calendar days, or risk acceptance with justification.
- *Security Manager's Perspective:* Our remediation SLAs are rigorously enforced. For any critical or high-severity vulnerability on an internet-facing system or a system processing financial transactions, the clock starts immediately upon validation. The Cybersecurity team works closely with IT Operations and Application Development teams to ensure these aggressive timelines are met. Any deviation requires formal risk acceptance signed off at the CISO level. This reflects the FFIEC's expectation for timely remediation of significant vulnerabilities.

5. Verification

After remediation actions have been taken, it is essential to verify their effectiveness.

- **Rescanning:** Conduct follow-up vulnerability scans on the affected assets to confirm that the vulnerability has been successfully remediated and no longer appears in scan reports.
- **Targeted Testing:** For critical vulnerabilities or complex fixes, targeted testing (e.g., mini-penetration test, specific exploit attempt in a controlled manner) may be performed to validate the remediation.

- **Documentation:** All remediation actions, verification results, and dates must be meticulously documented in the vulnerability management system or ticketing system.

6. Reporting & Continuous Monitoring

Ongoing reporting and monitoring are crucial for program oversight and continuous improvement.

- **Regular Reporting:** Generate and distribute regular vulnerability management reports to relevant stakeholders, including IT management, business unit leaders, and senior executives. Reports should include metrics such as the number of open vulnerabilities by severity, remediation SLA compliance rates, aging of vulnerabilities, and trends over time.
- **Continuous Monitoring:** Continuously monitor the IT environment for new assets (which must be brought into the VM program scope) and newly emerging vulnerabilities.
- **Program Review and Improvement:** Periodically review and update the vulnerability management program, policies, procedures, and tools based on lessons learned from incidents, changes in the threat landscape, new technologies, and evolving business requirements.

Risk Acceptance

In instances where a vulnerability cannot be remediated within the defined SLA (e.g., due to lack of a vendor patch, significant operational impact of the fix, or prohibitive cost), a formal risk acceptance process must be followed.

- **Documentation:** The risk acceptance request must include a detailed description of the vulnerability, the affected assets, the assessed risk, the reasons why remediation is not feasible, and any implemented or proposed compensating controls.
- **Approval:** Risk acceptance must be approved by the Asset Owner, the CISO, and, for high-impact risks, potentially by a higher-level risk committee or senior management.
- **Duration and Review:** Accepted risks are granted for a limited time period (e.g., 6-12 months) and must be regularly reviewed to determine if remediation has become feasible or if the risk level has changed.

Framework Alignment

This Vulnerability Management Procedure is aligned with leading industry standards and frameworks, including:

- **ISO 27001/ISO 27002:** Specifically, control A.12.6.1 (Management of technical vulnerabilities) from ISO 27001:2013 (mapping to A.8.8 in ISO 27001:2022 - Management of technical vulnerabilities).

- **NIST Cybersecurity Framework (CSF):** Elements of Identify (ID.AM, ID.RA), Protect (PR.IP), Detect (DE.CM), and Respond (RS.AN, RS.MI).
- **NIST Special Publication 800-40 Revision 4 (Guide to Enterprise Patch Management Planning):** While focused on patching, its principles of risk assessment, prioritization, and verification are integral to vulnerability remediation.
- **NIST Special Publication 800-53:** Relevant controls from families such as RA (Risk Assessment) and SI (System and Information Integrity).
- **SANS Vulnerability Management Process (e.g., PIACT - Prepare, Identify, Analyze/Assess, Communicate, Treat):** The lifecycle described aligns with the core phases advocated by SANS.
- **FFIEC Guidelines:** Financial industry regulators like the FFIEC mandate robust vulnerability management programs, including timely patching and risk assessment.

Real-World Example: Vulnerability in a Third-Party Financial Data Aggregation Service

World Bank utilizes a third-party cloud service for aggregating certain market data feeds.

- **Discovery:** A vulnerability alert from a threat intelligence service indicates a new critical remote code execution (RCE) vulnerability (CVE-202X-YYYYY) in the software version used by this third-party service.
- **Analysis:** The World Bank Cybersecurity Team confirms with the vendor that their instance is affected. CVSS score is 9.8. Business impact is assessed as High, as compromise could lead to inaccurate market data influencing Bank decisions or exposure of sensitive data feed credentials.
- **Prioritization:** The vulnerability is flagged as Critical due to its severity, potential impact, and the external-facing nature of the service (though access is restricted).
- **Remediation (Vendor-Side):** The vendor is immediately contacted and informed of the vulnerability. World Bank requests an urgent timeline for patching from the vendor, referencing contractual SLA clauses for critical vulnerability remediation. The vendor commits to patching within 24 hours.
- **Mitigation (World Bank-Side):** While awaiting vendor patching, World Bank's SOC implements enhanced monitoring on traffic to and from the vendor service. Access to the service from internal Bank systems is temporarily restricted to only absolutely essential functions, with heightened scrutiny.
- **Verification:** Once the vendor confirms patching, World Bank requests evidence (e.g., scan report from vendor, attestation). The Cybersecurity Team performs its own

targeted checks (if feasible and permitted by contract) to verify the patch has been applied and is effective.

- **Reporting:** The incident, vendor response, and verification are documented in the vulnerability management system and reported to relevant risk committees. The vendor's performance against the SLA is noted for future vendor risk assessments.

Table: Vulnerability Severity and Remediation SLAs

Severity Level	CVSS Score Range (v3.1)	Remediation SLA (from validation)	Escalation Path if SLA Missed
Critical	9.0 - 10.0	7 calendar days (48 hours if actively exploited & high impact)	Immediate to CISO, IT Ops Head, relevant Business Unit Head
High	7.0 - 8.9	30 calendar days	To Security Manager & IT Ops Manager after 15 days; CISO after 30 days
Medium	4.0 - 6.9	90 calendar days	To Security Manager after 60 days
Low	0.1 - 3.9	180 calendar days / Risk Acceptance	Monitored by Security Team; risk acceptance reviewed annually

- **Value of Table:** This table is fundamental to operationalizing the Vulnerability Management Procedure at World Bank. It provides unambiguous, measurable targets for remediation efforts, ensuring that vulnerabilities are addressed in a timeframe commensurate with their risk level. For a financial institution like World Bank, adherence to such SLAs is not just a best practice but a critical component of its regulatory compliance (e.g., FFIEC expectations for timely patching) and its ability to defend against sophisticated cyber threats. The defined escalation paths ensure accountability and prompt attention if remediation efforts falter, thereby maintaining a consistently strong security posture.