

World Bank Vendor Risk Assessment (VRA) Procedure

Preamble

At World Bank, engaging third-party vendors is a strategic necessity that enables innovation and operational efficiency. However, such engagements inherently introduce a spectrum of risks to our institution. This Vendor Risk Assessment (VRA) Procedure is the cornerstone of World Bank's comprehensive Third-Party Risk Management (TPRM) program. It details the systematic and consistent process we follow to identify, analyze, evaluate, treat, and monitor risks associated with our vendors. This procedure ensures that all vendors, particularly those accessing sensitive data or providing critical services, meet World Bank's stringent security, operational, and compliance standards before and throughout their engagement with us. The formalization of VRA into a documented procedure elevates its importance, ensures consistency in application, and signals to all stakeholders that vendor-introduced risk is managed with the utmost seriousness.

Section 1: Purpose and Policy Statement

The purpose of this VRA Procedure is to establish a consistent, risk-based, and comprehensive process for evaluating the risks introduced by engaging third-party vendors. This procedure aims to protect World Bank's information assets, customer data, reputation, and operational stability from potential adverse impacts arising from vendor relationships.

It is World Bank policy that all third-party vendors, suppliers, and service providers, especially those that will access, store, process, or transmit World Bank sensitive data, or those providing services deemed critical to bank operations, must undergo a VRA as defined herein prior to contract execution and periodically thereafter throughout the lifecycle of the relationship. This aligns with regulatory expectations and industry best practices for managing third-party risks.

Section 2: Vendor Risk Management Lifecycle Overview

The VRA procedure is an integral part of World Bank's overall Vendor Risk Management (VRM) lifecycle, which encompasses several distinct stages. Understanding this lifecycle is crucial as it contextualizes the VRA within a broader framework of ongoing vendor governance. The stages include:

1. **Planning:** Identifying the business need for a third-party service and defining initial requirements.
2. **Due Diligence and Selection:** Conducting thorough assessments of potential vendors to evaluate their capabilities, financial stability, security posture, and compliance. This stage is a primary focus of this VRA procedure.

3. **Contracting:** Negotiating and finalizing contractual agreements that include appropriate security, compliance, and service level requirements (as detailed in World Bank's Policy on Vendor Contract and SLA Security Requirements).
4. **Onboarding:** Integrating the selected vendor into World Bank's operational environment, including system access provisioning and initial training, if applicable.
5. **Ongoing Monitoring:** Continuously overseeing vendor performance, security posture, and compliance with contractual obligations. This is another key focus of the VRA procedure.
6. **Termination/Offboarding:** Securely ending the vendor relationship, ensuring data return or destruction, access revocation, and final settlement.

Viewing VRA as part of this lifecycle, rather than a one-time event at onboarding, is critical for managing the dynamic nature of vendor risks. A vendor's risk profile can evolve due to new cyber threats, changes in their service offerings, or deterioration in their internal controls. This lifecycle approach ensures that risk management activities are performed at appropriate junctures, aligning with regulatory expectations for continuous vendor oversight.

Section 3: Vendor Identification and Tiering

A fundamental step in the VRA process is the identification and subsequent risk-based tiering of all vendors. This allows World Bank to allocate its VRA resources efficiently, focusing the most intensive scrutiny on vendors that pose the highest potential risk. This risk-based approach is a hallmark of mature risk management, preventing a one-size-fits-all methodology that could be overly burdensome for low-risk vendors or insufficient for high-risk ones.

Vendor Identification: All potential and existing third-party relationships must be centrally inventoried in the World Bank Register of Suppliers (see Document 4).

Vendor Tiering Criteria: Vendors are classified into tiers based on an initial risk assessment conducted by the business unit proposing the engagement, with oversight from the Vendor Management Office (VMO) and Cybersecurity. The tiering is determined by factors including:

1. **Data Access and Sensitivity:** The type and volume of World Bank data (e.g., customer Personally Identifiable Information (PII), financial records, strategic plans, intellectual property) that the vendor will access, process, store, or transmit.
2. **Service Criticality:** The potential impact on World Bank's critical business operations, customer services, or reputation if the vendor's service is disrupted or fails.
3. **System Connectivity and Integration:** The extent and method of the vendor's connection to World Bank's internal networks, systems, or cloud environments.

4. **Regulatory Scope:** Whether the vendor's services or data handling fall under specific regulatory mandates (e.g., GDPR, PCI DSS, GLBA, DORA) that impose obligations on World Bank.
5. **Financial Impact:** The potential direct or indirect financial loss to World Bank resulting from a vendor failure, data breach, or non-compliance.
6. **Geographic Location:** The geopolitical stability and legal/regulatory environment of the vendor's operating locations, especially if data is processed or stored offshore.

Risk Tiers and Assessment Depth: Based on these criteria, vendors are assigned to one of the following tiers, which dictates the scope and rigor of the VRA:

Table 4: World Bank Vendor Risk Tiering Criteria

Tier	Description	Data Access Implication Examples	Assessment Frequency	Key Due Diligence Activities Examples
Tier 1: Critical	Vendor provides essential services where failure would cause significant disruption to World Bank operations or customers; extensive access to highly sensitive data; high regulatory impact.	Full access to core banking systems, large volumes of customer PII/financials, payment processing.	Annual Full VRA + Continuous Monitoring (e.g., security ratings, threat intel). Trigger-based re-assessments.	On-site/Virtual Assessment, SIG Full Questionnaire, SOC 2 Type II Review, Penetration Test Result Review, Financial Viability Check, BCDR Plan Deep Dive, Fourth-Party Risk Assessment.
Tier 2: High	Vendor provides important services or has access to sensitive data, where failure or breach could cause moderate disruption or impact.	Access to significant amounts of PII, sensitive internal data; integration with key business applications.	Annual Full VRA.	SIG Core Questionnaire, SOC 2 Type II (or equivalent) Review, Vulnerability Assessment Review, Financial Review, BCDR Plan Review.
Tier 3: Medium	Vendor provides services with limited access to sensitive data, or where failure would cause minor, localized disruption.	Access to limited PII or operational data; standalone applications with limited integration.	VRA at Onboarding and Contract Renewal (typically every 2-3 years).	SIG Lite Questionnaire, Review of basic security policies, ISO 27001 (if applicable).
Tier 4: Low	Vendor provides non-critical services with no access to sensitive World Bank data or systems.	No access to sensitive data; commodity goods/services.	Minimal VRA at Onboarding (e.g., basic questionnaire, public information check).	Confirmation of no sensitive data access; review of standard contract terms.

Section 4: Due Diligence Process

The due diligence process involves a thorough examination of the vendor's controls and practices. The activities performed are scaled according to the vendor's assigned risk tier. This shift from trust-based to evidence-based vendor assurance is critical for robust risk management.

Key due diligence activities include:

1. **Information Gathering:** Distribution of standardized security questionnaires (e.g., Standardized Information Gathering (SIG) Lite for Tier 3, SIG Core or Full for Tiers 1-2, or Cloud Security Alliance CAIQ for CSPs). Collection of vendor-provided documentation such as information security policies, data privacy policies, network diagrams, and incident response plans.
2. **Documentation Review:** Detailed analysis of critical documents including:
 - **Independent Audit Reports:** SOC 2 Type II reports (evaluating security, availability, processing integrity, confidentiality, privacy controls over a period), ISO 27001 certificates and Statement of Applicability.
 - **Security Assessment Reports:** Results and remediation plans from recent penetration tests and vulnerability assessments.
 - **Financial Stability:** Public financial statements or third-party financial health reports.
 - **Business Continuity and Disaster Recovery (BCDR) Plans:** Review of plans and test results.
 - **Insurance Certificates:** Evidence of relevant coverage, such as Cyber Liability, Errors & Omissions.
3. **Security Posture Assessment:** Evaluation of the vendor's implemented security controls, covering technical (e.g., encryption methods, network security, endpoint protection), administrative (e.g., security awareness training, personnel security), and physical security measures. Assessment of their vulnerability management program (scanning, patching cadence), identity and access management (IAM) practices (MFA, least privilege), and data encryption standards.
4. **Compliance Evaluation:** Verification of the vendor's adherence to applicable laws, regulations (e.g., GDPR, CCPA, PCI DSS, GLBA, DORA), and industry standards relevant to the services provided and data handled. This includes reviewing their data handling procedures and privacy policies.
5. **Contract Review:** Ensuring that World Bank's standard security clauses and SLA requirements (as per Document 1) are incorporated into the contract and are appropriate for the vendor's risk tier and services.
6. **Reference Checks:** For Tier 1 and Tier 2 vendors, contacting other clients (with vendor permission) to gather feedback on their security practices, reliability, and responsiveness to issues.
7. **On-site or Virtual Assessments:** For Tier 1 vendors (and potentially Tier 2 based on risk), conducting direct assessments (physical or virtual) of their facilities, controls, and processes to gain deeper insights and verify documented claims.

8. **Fourth-Party Risk Inquiry:** For critical vendors, understanding their reliance on their own key suppliers (fourth parties) and how they manage those risks, especially if those fourth parties will handle or impact World Bank data or services.

Section 5: Risk Assessment and Analysis

Following due diligence, the collected information is analyzed to identify vulnerabilities, control gaps, and potential risks. The use of both qualitative and quantitative methods, along with specific risk categories, allows for a more nuanced and comprehensive understanding of vendor risk, moving beyond a simple "pass/fail" to a detailed risk profile that can inform specific mitigation strategies.

1. **Methodology:** World Bank employs a hybrid approach, combining:
 - **Qualitative Analysis:** Using risk matrices to assess the likelihood and impact of identified threats/vulnerabilities (e.g., High/Medium/Low for both likelihood and impact). Expert judgment from Cybersecurity, Legal, and business SMEs is incorporated.
 - **Quantitative Analysis (where applicable):** Utilizing security rating services for an objective measure of a vendor's external security posture, analyzing financial health scores, or using specific metrics from audit reports (e.g., number of high-risk findings in a pen test).
2. **Risk Scoring and Rating:** Identified risks are scored based on their assessed likelihood and potential impact. These individual risk scores are then aggregated (often weighted by criticality) to produce an overall vendor risk rating (e.g., Critical, High, Medium, Low), which may differ from the initial tiering if significant issues are found.
3. **Identification of Key Risk Categories:** Risks are categorized to provide a structured view of potential exposures. Common categories include:
 - **Cybersecurity/Information Security Risk:** Potential for data breach, system compromise due to weaknesses in vendor's security controls.
 - **Operational Risk:** Potential for disruption to World Bank operations due to vendor service failure or inadequacy.
 - **Financial Risk:** Potential for financial loss to World Bank due to vendor instability or direct financial impact of a vendor-related incident.
 - **Compliance and Legal Risk:** Potential for World Bank to violate laws or regulations due to vendor non-compliance.
 - **Reputational Risk:** Potential for damage to World Bank's reputation due to vendor actions or failures.
 - **Strategic Risk:** Potential for vendor relationship to negatively impact World Bank's strategic objectives.

- **Geopolitical Risk:** Risks arising from vendor's location or operations in politically unstable or high-risk jurisdictions.
4. **Gap Analysis:** The vendor's security controls and practices are compared against World Bank's policy requirements (including Document 1) and relevant regulatory standards. Any identified gaps are documented.

Section 6: Risk Treatment and Mitigation

Identified risks must be addressed through a formal risk treatment process, ensuring that risks are not ignored and that decisions on handling each significant risk are made with accountability. For each significant risk identified, one or more of the following treatment options will be selected:

1. **Risk Acceptance:** For low-level risks where the cost of mitigation outweighs the potential impact, the risk may be formally accepted. This requires documented approval from the relevant Business Owner and the Chief Information Security Officer (CISO) or designated risk committee.
2. **Risk Avoidance:** If the identified risks are deemed unacceptable and cannot be adequately mitigated, World Bank may decide not to engage the vendor or to terminate an existing relationship.
3. **Risk Transference:** Transferring a portion of the financial impact of a risk to a third party, typically by requiring the vendor to maintain specific types and levels of insurance coverage (e.g., cyber liability, professional indemnity).
4. **Risk Mitigation:** Implementing controls or actions to reduce the likelihood or impact of the risk. This is the most common approach and may involve:
 - Requiring the vendor to remediate identified weaknesses or control gaps within an agreed timeframe. A formal Corrective Action Plan (CAP) from the vendor will be requested and tracked by World Bank.
 - Implementing compensating controls within World Bank's environment to reduce the impact of a vendor weakness.
 - Negotiating specific contractual terms, such as enhanced security requirements, stricter SLAs, or limitations of liability.

All risk treatment decisions and mitigation plans must be documented in the VRA report and tracked to completion.

Section 7: Ongoing Monitoring and Review

Vendor risk is not static; therefore, ongoing monitoring and periodic reviews are essential components of this VRA procedure. This dynamic and adaptive approach is resource-intensive but critical for managing long-term vendor relationships securely.

1. Frequency of Review:

- **Tier 1 (Critical) Vendors:** Full VRA conducted annually. Continuous monitoring through security rating services, threat intelligence, and review of incident reports.
- **Tier 2 (High) Vendors:** Full VRA conducted annually or biennially, depending on the stability of their services and risk profile. Periodic monitoring.
- **Tier 3 (Medium) Vendors:** VRA typically conducted at contract renewal (e.g., every 2-3 years) or if significant changes occur.
- **Tier 4 (Low) Vendors:** Review primarily at contract renewal, focusing on continued low-risk status.

2. Triggers for Ad-Hoc Re-assessment: A VRA may be initiated outside the scheduled cycle if triggered by:

- A significant security incident involving the vendor (even if World Bank data was not impacted).
- Material changes in the vendor's services, ownership, financial stability, or security posture.
- Merger or acquisition activity involving the vendor.
- Negative public news or regulatory scrutiny concerning the vendor.
- Emergence of new significant threats relevant to the vendor's services.
- Changes in World Bank's regulatory landscape or risk appetite.

3. Monitoring Activities:

- Regular review of vendor-provided reports (e.g., performance against SLAs, security incident summaries).
- Annual collection and review of updated SOC reports, ISO certifications, and other key due diligence documents.
- Monitoring of public threat intelligence feeds and security rating services for alerts related to key vendors.
- Periodic check-ins with business relationship owners to discuss vendor performance and any emerging concerns.

4. Automated Monitoring Tools: Where appropriate and cost-effective, World Bank will leverage automated tools for continuous monitoring of vendor security posture (e.g., security ratings platforms, dark web scanning for compromised credentials related to vendors).

Section 8: Vendor Offboarding Security Requirements

The secure termination of a vendor relationship is as critical as its onboarding. Formal offboarding procedures prevent lingering access and potential data exposure after a contract ends.

Upon the decision to terminate a vendor relationship, the following minimum security requirements must be met and documented:

1. **Access Revocation:** All logical and physical access granted to the vendor (personnel and systems) to World Bank systems, networks, applications, and data must be revoked promptly upon termination or cessation of services, in accordance with contractual terms. This includes disabling user accounts, VPN access, API keys, and revoking any digital certificates.
2. **Data Return and/or Destruction:** All World Bank data held by the vendor, including any copies, backups, or derivatives, must be securely returned to World Bank or securely destroyed (e.g., using cryptographic erasure or physical destruction methods compliant with standards like NIST SP 800-88). The vendor must provide a formal, written certification of data destruction, signed by an authorized representative.
3. **Asset Retrieval:** All World Bank physical assets (e.g., laptops, tokens, access badges) and logical assets (e.g., software licenses, intellectual property) in the vendor's possession must be returned.
4. **Final Contractual Obligations Review:** A final review of the contract must be conducted to ensure all security-related exit clauses, confidentiality obligations, and other surviving terms are understood and will be adhered to by the departing vendor.
5. **Update Vendor Inventory/Register:** The World Bank Register of Suppliers must be updated to reflect the termination of the relationship and the completion of offboarding security requirements.

Appendix A: Vendor Risk Assessment Checklist (Excerpt)

This appendix provides a sample of key questions from the World Bank VRA checklist, categorized by control domain. The full checklist is more comprehensive.

Table 5: Excerpt from World Bank VRA Checklist

Assessment Domain	Control Objective	Example Question/Check	Expected Evidence/Verification Method
1. Information Security Governance	Ensure vendor has a formal information security program.	Does the vendor have a documented information security policy suite, approved by senior management and reviewed at least annually?	Copy of Information Security Policy; evidence of management review/approval (e.g., meeting minutes, sign-off).

	Ensure clear roles and responsibilities for security.	Is there a designated individual or team responsible for information security (e.g., CISO, Security Manager)?	Organizational chart; job descriptions for key security personnel.
2. Data Security & Privacy	Ensure sensitive data is protected throughout its lifecycle.	How does the vendor classify data? What specific controls are applied to protect World Bank sensitive data (e.g., PII, financial data)?	Data classification policy; data handling procedures; examples of controls for sensitive data.
	Ensure data encryption at rest and in transit.	Is World Bank data encrypted at rest (e.g., on servers, databases, backups) and in transit (e.g., over public networks, internal networks)? Specify encryption algorithms and key management practices.	Encryption policy; technical documentation on encryption implementation; key management procedures.
3. Access Control	Ensure access to World Bank data and systems is restricted to authorized users.	Is Multi-Factor Authentication (MFA) enforced for all administrative access and remote access to systems processing or storing World Bank data?	Access control policy; screenshots of MFA configuration; list of systems where MFA is enforced.
	Ensure principle of least privilege is applied.	How does the vendor ensure that user access rights are based on the principle of least privilege and reviewed regularly (e.g., quarterly)?	Access control policy; role-based access control matrix; evidence of access reviews.
4. Incident Response & Management	Ensure vendor has a documented and tested incident response plan.	Does the vendor have a documented Incident Response Plan (IRP)? When was it last tested, and what were the results/lessons learned?	Copy of IRP; incident response test plan and report; evidence of lessons learned implementation.
	Ensure timely notification of security incidents to World Bank.	What are the vendor's procedures and timelines for notifying World Bank of a security incident affecting its data or services? (Must align with contractual requirements).	IRP section on client notification; contractual clauses.
5. Business Continuity & Disaster Recovery (BCDR)	Ensure vendor can maintain service continuity in case of disruption.	Does the vendor have a documented BCDR plan? What are the RTOs and RPOs for services provided to World Bank? When was the BCDR plan last tested?	Copy of BCDR plan; BCDR test plan and report; stated RTOs/RPOs.
6. Vulnerability Management	Ensure vendor has a process to identify and remediate vulnerabilities.	Does the vendor conduct regular vulnerability scans (internal/external) and penetration tests? What is the process for remediating identified vulnerabilities, and what are the timelines based on severity?	Vulnerability management policy/procedure; sample vulnerability scan/pen test report (redacted if necessary); patch management policy.
7. Physical & Environmental Security	Ensure physical security of facilities where World Bank data is processed or stored.	What physical security measures are in place at data centers and office locations (e.g., access controls, surveillance, environmental controls)?	Physical security policy; SOC 2 report (if it covers physical security); description of controls.
8. Human Resources Security	Ensure personnel with access to sensitive data are trustworthy and trained.	Does the vendor conduct background checks for personnel in sensitive roles? Is security awareness training provided to all employees at least annually?	HR security policy; background check policy; security awareness training materials and completion records.

9. Subcontractor (Fourth-Party) Risk Management	Ensure vendor manages risks associated with its own critical suppliers.	Does the vendor have a process for assessing and managing the security risks of its own subcontractors that handle World Bank data?	Third-party risk management policy (for their vendors); contractual clauses flowed down to subcontractors.
10. Secure Software Development (if applicable)	Ensure applications developed by or for the vendor are secure.	Does the vendor follow a Secure Software Development Lifecycle (SSDLC)? Are security testing (SAST, DAST) and code reviews part of the development process?	SSDLC policy/documentation; evidence of security testing in development.
11. Cloud Security (if vendor uses cloud services)	Ensure vendor securely configures and manages its cloud environments.	If the vendor uses CSPs, how do they manage shared responsibilities? What specific controls are in place for cloud security (e.g., IAM, network security, data protection in the cloud)?	Cloud security policy; configuration standards for cloud services; evidence of cloud security assessments.
12. Compliance & Certifications	Verify adherence to relevant standards and regulations.	Does the vendor maintain relevant certifications (e.g., ISO 27001, SOC 2, PCI DSS)? Provide copies of current certificates/reports.	Copies of valid certificates and audit reports (e.g., SOC 2 Type II).
13. Data Return/Deletion	Ensure secure data handling upon contract termination.	What is the vendor's process for securely returning or destroying World Bank data upon contract termination? Will a certificate of destruction be provided?	Data retention/destruction policy; contractual clauses on termination.
14. Logging and Monitoring	Ensure adequate logging and monitoring of systems handling WB data.	Are security logs generated, retained, and monitored for systems processing World Bank data? What is the log retention period?	Logging and monitoring policy; examples of log review processes; SIEM information if applicable.
15. Network Security	Ensure network is adequately segmented and protected.	How is the vendor's network segmented to protect systems handling World Bank data? What firewall and intrusion detection/prevention systems are in place?	Network diagrams; firewall policies; IDS/IPS documentation.

Appendix B: Vendor Tiering Criteria Table

(This appendix would contain the detailed Table 4: World Bank Vendor Risk Tiering Criteria as shown in Section 3.)