

World Bank Register of Suppliers with Access to Sensitive Data

Preamble

Maintaining a comprehensive, accurate, and current inventory of all third-party suppliers with access to World Bank's sensitive data or critical systems is a foundational element of our cybersecurity, operational risk management, and regulatory compliance strategy. This Register of Suppliers with Access to Sensitive Data (hereafter "Supplier Register" or "Register") is not merely a static list; it is a dynamic and critical tool. It enables World Bank to understand its third-party risk landscape, respond effectively and efficiently to security incidents, ensure ongoing compliance with contractual and regulatory obligations, and make informed risk management decisions. This document outlines the policy, procedures, and responsibilities for the creation, maintenance, and utilization of this vital Register. Treating the Supplier Register as a controlled document with defined responsibilities, access controls, and regular audits underscores its importance as a critical information asset for the bank.

Section 1: Policy for Maintaining the Supplier Register

- **Purpose of the Register:** The primary purpose of the Supplier Register is to maintain an accurate, up-to-date, and centralized inventory of all third-party vendors that have been granted access to World Bank's sensitive data or critical systems. This Register serves as a definitive reference to support various risk management activities, including vendor due diligence, ongoing monitoring, incident response, audit support, and compliance reporting. It is a key component of World Bank's Third-Party Risk Management (TPRM) program. FFIEC guidance also recommends maintaining a current third-party inventory.
- **Responsibility for Maintenance and Updates:** The overall responsibility for the accuracy and completeness of the Supplier Register is assigned to the World Bank Vendor Management Office (VMO). The VMO will work in close collaboration with the Cybersecurity department, business unit relationship owners, Legal, and Procurement to ensure timely and accurate updates. Business unit relationship owners are responsible for notifying the VMO of any new vendor engagements, changes in existing vendor services, or vendor terminations. The Cybersecurity team is responsible for providing risk assessment data and verifying security-related information within the Register.
- **Access Control to the Register:** Access to the Supplier Register is strictly controlled and granted on a need-to-know basis. Authorized personnel typically include designated staff within the VMO, Cybersecurity, Enterprise Risk Management, Internal Audit, Legal, Procurement, and relevant business unit relationship owners who require access to perform their duties. The Register itself contains sensitive information about

World Bank's vendor ecosystem and security posture; therefore, robust access controls (e.g., role-based access, audit trails of access) must be implemented and maintained for the system housing the Register.

- **Frequency of Review and Audit of the Register:** The Supplier Register must be formally reviewed for accuracy and completeness by the VMO and Cybersecurity team at least annually. Additionally, the Register will be subject to periodic audits by World Bank's Internal Audit function to ensure compliance with this policy and the effectiveness of its maintenance procedures. Entries within the register are also reviewed and updated upon significant changes, such as the onboarding of a new critical vendor, a major change in a vendor's service scope, contract renewal, or vendor termination.

Section 2: Procedure for Adding/Updating/Removing Vendors from the Register

A defined workflow, integrated with the overall vendor lifecycle, governs all modifications to the Supplier Register. This ensures data integrity and timeliness, transforming the Register into a reliable source for operational and strategic decision-making. This structured approach also links the Register directly to financial controls, mitigating risks of unauthorized vendor setups.

1. **New Vendor Onboarding:** Upon successful completion of the Vendor Risk Assessment (VRA) process (as detailed in Document 3) and finalization of the contractual agreement, the VMO is responsible for creating a new entry in the Supplier Register. Essential data fields will be populated based on information gathered during the due diligence and contracting phases. The entry must be completed before the vendor is granted access to any World Bank sensitive data or systems.
2. **Segregation of Duties in Vendor Master File Management:** To prevent fraud and unauthorized changes, World Bank enforces segregation of duties concerning vendor master files in financial systems, which often serve as a source for basic vendor information. The employee who has the capability to set up new vendors or modify existing vendor information (e.g., bank account details, addresses) in the core financial systems must not be the same employee who can authorize or process payments to vendors, nor should they have administrative rights to modify the Supplier Register without an independent review and approval process. Changes to vendor master files that impact payment information must undergo an independent verification and approval step.
3. **Periodic Updates and Changes:** Business unit relationship owners are responsible for promptly notifying the VMO of any significant changes to existing vendor relationships. This includes changes in the scope of services, types of data accessed, key personnel, contract renewals, or any known changes in the vendor's risk posture. The Cybersecurity team will provide updates based on ongoing monitoring activities, VRA

re-assessments, or new threat intelligence. The VMO will update the Register accordingly after verifying the information.

4. **Vendor Offboarding:** Upon the termination of a vendor contract and successful completion of all offboarding security requirements (as detailed in Document 3, Section 8, including confirmation of access revocation and data return/destruction), the VMO will update the vendor's status in the Supplier Register to "Terminated" or "Inactive." The historical record will be retained for audit and compliance purposes according to World Bank's data retention policy, but the vendor will no longer be listed as an active supplier with data access.
5. **Approval Process for Critical Changes:** Any proposed changes to critical data fields within the Supplier Register for Tier 1 (Critical) or Tier 2 (High) vendors, such as an alteration in their risk tier, the scope of sensitive data they access, or key security controls, require formal review and approval from a designated authority within the Cybersecurity or Enterprise Risk Management department before the Register is updated.

Section 3: Supplier Register Template and Data Fields

The Supplier Register is maintained in a secure, centralized database or system. The structure of the Register includes the following minimum data fields for each vendor. The granularity of these fields, particularly those related to specific data types accessed, systems involved, and security controls verified, transforms the Register from a simple inventory into a rich risk intelligence tool, essential for effective incident response and proactive risk management.

Table 6: World Bank Supplier Register Template (Illustrative Fields and Example Entries)

Field No.	Data Field	Description/Example Data (Vendor: CloudServePro Inc.)	Description/Example Data (Vendor: FinConsult Ltd.)	Source/Rationale
1	Vendor ID	Unique identifier assigned by World Bank. (WBV001)	(WBV002)	Internal System;
2	Vendor Legal Name	Official registered name of the vendor. (CloudServePro Inc.)	(FinConsult Advisory Ltd.)	Contract;
3	Primary Business Contact	Key relationship manager at vendor. (Jane Doe, j.doe@cloudservepro.com, 555-0101)	(John Smith, j.smith@finconsult.com, 555-0202)	Contract/VMO;
4	Primary Security Contact	Designated security point of contact at vendor. (SecOps Team, secops@cloudservepro.com, 555-0102)	(Mark Allen, m.allen@finconsult.com, 555-0203)	VRA/Contract
5	Service(s) Provided	Brief description of services/products. (IaaS Cloud Hosting for Dev/Test Environments)	(Regulatory Compliance Consulting Services)	Contract/SOW

6	Types of Sensitive Data Accessed/Processed	Specific categories of data. (Non-production source code, anonymized test data, system configurations)	(Internal audit reports, draft regulatory filings, strategic risk assessments - (NDA in place))	VRA/Data Inventory;
7	Data Access Method/Level	How vendor accesses data and privilege level. (AWS Management Console Admin (Dev/Test OU), API keys with restricted permissions)	(Secure file share access (read/write), email communication, access to specific SharePoint sites)	VRA;
8	Key Systems/Platforms Accessed	Specific World Bank systems or platforms. (AWS Account ID 123456789012 - Dev/Test Organization Unit & associated VPCs)	(World Bank Internal Audit SharePoint, Designated secure project folders)	VRA;
9	Data Storage Location (Primary & Backup)	Geographic location(s) of data. (Primary: AWS us-east-1; Backups: AWS us-west-2)	(Vendor's secure servers in London, UK; Encrypted backups in Dublin, IE)	VRA/Contract;
10	Contract Start & End/Renewal Date	Effective dates of the current contract. (Start: 2023-01-15; End: 2025-12-31)	(Start: 2024-03-01; Renewal: Annually on March 1st)	Contract Management System;
11	Date of Last Full VRA	Date the most recent comprehensive VRA was completed. (2024-03-15)	(2024-02-10 (at onboarding))	VRA System;
12	Current Risk Tier	Assigned risk tier (Critical, High, Medium, Low). (Tier 2 - High)	(Tier 3 - Medium)	VRA System;
13	Key Security Controls Verified	Summary of critical controls confirmed. (MFA on console, IAM least privilege reviewed, S3 buckets private by default, regular OS patching)	(Data encryption on laptops, secure file transfer protocols used, confidentiality agreements signed by consultants)	VRA Report
14	SOC 2 Report Availability & Date	Status and date of latest SOC 2 Type II report. (Available: Yes; Report Date: 2024-02-01)	(Available: No; N/A for service type)	VRA Documentation;
15	ISO 27001 Certification Status & Expiry	Status and expiry of ISO 27001 certification. (Certified: Yes; Expiry: 2026-05-20)	(Certified: No)	VRA Documentation
16	BCDR Plan Tested & Date	Status and date of last BCDR test. (Tested: Yes; Last Test: 2023-11-10)	(BCDR Plan Reviewed: Yes; Test N/A for individual consultants, firm plan reviewed)	VRA Documentation;
17	Primary Fourth Parties Involved (if known)	Key subcontractors critical to service delivery. (MonitoringTool Inc. (for APM), BackupStorage Corp. (for offsite backups))	(None identified as handling WB data)	VRA Report;
18	Incident Response Contact (Vendor Side)	Specific contact for immediate IR. (IR Team, ir@cloudservepro.com, 555-0103 (24/7))	(Mark Allen, m.allen@finconsult.com)	VRA/Contract
19	Data Processing Agreement (DPA) in Place?	Confirmation of DPA execution. (Yes)	(Yes, as part of Master Services Agreement)	Contract Management System

20	Date Added to Register / Last Updated	Audit trail for register entry. (Added: 2023-01-10; Last Updated: 2024-03-20)	(Added: 2024-02-15; Last Updated: 2024-02-15)	Register System Log
21	Business Unit Owner	WB internal owner of the vendor relationship. (Digital Innovation Department)	(Internal Audit Department)	VMO Records
22	Justification for Sensitive Data Access	Brief reason why vendor needs this access. (Hosting and management of non-production application development platforms.)	(Provision of specialized regulatory advice requiring review of sensitive internal documents.)	VRA/Business Case
23	Data Exfiltration Controls Monitored	Specific controls to prevent unauthorized data removal. (VPC Endpoints, DLP scans on S3, egress traffic filtering)	(Endpoint DLP on consultant laptops, secure managed file transfer)	VRA/Cybersecurity Team
24	Offboarding Date (if applicable)	Date vendor relationship was terminated. (N/A)	(N/A)	VMO Records
25	Confirmation of Data Destruction/Return (if offboarded)	Y/N and date of certification. (N/A)	(N/A)	VMO Records

Section 4: Use of the Register in Security Operations and Risk Management

The Supplier Register is not a passive repository; it is actively integrated into World Bank's daily security operations and strategic risk management activities. This active utilization maximizes its value, transforming it into a living document that informs critical decisions across the bank and demonstrates a mature approach to embedding TPRM into organizational processes.

1. **Incident Response:** In the event of a security incident potentially involving a third party (either as a source or impacted entity), the Supplier Register is a primary resource for the CSOC and Incident Response Team. It allows for rapid identification of:
 - Which vendors have access to the compromised or potentially compromised data, systems, or applications.
 - The type and sensitivity of data involved.
 - The vendor's security contact information for immediate communication and coordination.
 - Relevant contractual obligations regarding incident notification and cooperation.

2. **Audit and Compliance Reporting:** The Register provides essential evidence to internal and external auditors, as well as regulators, demonstrating World Bank's structured approach to managing its vendor ecosystem. It supports reporting on:
 - The completeness of the vendor inventory.
 - The application of risk tiering.
 - The status of VRAs and due diligence activities.
 - Compliance with regulations requiring oversight of third parties handling sensitive data (e.g., GLBA, GDPR, DORA).
3. **Proactive Risk Management and Strategic Sourcing:** The Cybersecurity and Enterprise Risk Management teams utilize the Register to:
 - Identify potential concentrations of risk (e.g., multiple critical vendors relying on a single fourth-party provider, over-reliance on vendors in specific high-risk geographic locations).
 - Inform the scope and prioritization of targeted VRAs and continuous monitoring efforts.
 - Support strategic sourcing decisions by providing insights into the existing vendor landscape and associated risks when considering new engagements or consolidating services.
 - Identify vendors that require enhanced scrutiny due to the criticality of the services they provide or the sensitivity of the data they access.
4. **Change Management:** When significant changes are proposed to World Bank's IT systems or applications, the Register is consulted to identify which vendors might be impacted or might require changes to their access rights or configurations. This ensures that vendor-related dependencies are considered as part of the change management process.
5. **Business Continuity and Disaster Recovery (BCDR) Planning:** The Register helps identify critical vendor dependencies that are essential for World Bank's BCDR plans. Understanding which vendors support critical functions allows for better planning of contingency measures and communication strategies in the event of a major disruption affecting either World Bank or a key vendor.