

World Bank Guidelines on Cloud Shared Responsibility

Preamble

The transition to cloud services offers World Bank significant advantages in agility, scalability, and innovation. However, it also introduces a complex security paradigm: the Shared Responsibility Model. These guidelines are established to ensure every team at World Bank clearly understands our security obligations versus those of our Cloud Service Providers (CSPs). Misunderstanding these boundaries is a common source of security gaps, and this document is our definitive guide to navigating shared responsibilities effectively. The existence of this dedicated internal document reflects World Bank's recognition of cloud complexity and the need for internal clarity beyond relying solely on CSP documentation. It is a proactive measure to prevent internal teams from making incorrect assumptions about security ownership.

Section 1: Introduction to the Shared Responsibility Model at World Bank

The Shared Responsibility Model is a fundamental framework that dictates how security obligations are approached and implemented in the cloud environment, delineating responsibilities between World Bank (the customer) and its CSPs (e.g., Amazon Web Services, Microsoft Azure, Google Cloud Platform). It clarifies that cloud security is a collaborative effort, a partnership where both parties have distinct yet interconnected security duties. A clear understanding and diligent execution of these responsibilities are paramount for World Bank to effectively manage risk, maintain regulatory compliance, and build a secure foundation for all its cloud initiatives. World Bank is committed to upholding its share of these responsibilities to the highest standards.

Section 2: General Principles of Shared Responsibility

Several core principles underpin World Bank's approach to the Shared Responsibility Model:

- **World Bank's Ultimate Accountability:** While responsibilities are shared, World Bank remains ultimately accountable for the security of its data, the compliance of its operations with all applicable financial regulations (e.g., FFIEC guidance, GDPR, DORA), and the protection of customer information, regardless of where data is stored or processed. This principle is crucial as outsourcing a function does not outsource the inherent risk or the regulatory obligations associated with it. This stance preempts any attempt to fully delegate risk to the CSP and underscores the necessity for robust internal controls and diligent oversight by World Bank personnel.
- **Provider's Responsibility ("Security of the Cloud"):** The CSP is responsible for protecting the global infrastructure that runs all of the services offered in the CSP's cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run CSP cloud services. This includes the physical security of data

centers (e.g., access control, environmental protections), the security of the underlying compute, storage, and network hardware, and the virtualization layer (hypervisor) that enables cloud services.

- **World Bank's Responsibility ("Security *in* the Cloud"):** World Bank is responsible for security measures related to what it creates and puts *in* the cloud environment, or connects *to* the cloud environment. This encompasses customer data (its classification, confidentiality, integrity, and availability), platform configurations, applications (custom-developed or third-party), identity and access management (IAM), operating systems (in IaaS deployments), network configurations (e.g., virtual private clouds, subnets, firewalls), and client-side data encryption and data integrity authentication, as well as server-side encryption using customer-managed keys.

Section 3: Shared Responsibilities by Service Model (IaaS, PaaS, SaaS)

The specific division of responsibilities varies significantly depending on the cloud service model being utilized. The level of customer responsibility is highest in IaaS and progressively decreases through PaaS to SaaS; however, critical responsibilities always remain with World Bank.

The following table provides a high-level overview, using AWS as a representative CSP for examples:

Table 3: World Bank Shared Responsibility Matrix for IaaS (Example: AWS EC2)

Responsibility Area	AWS Responsibility	World Bank Responsibility	Key World Bank Control/Procedure Example
Physical & Environmental Security of Data Centers	AWS manages physical access, power, cooling, environmental controls for data centers housing EC2 infrastructure.	N/A (Relies on AWS controls and attestations like SOC 2).	Review AWS SOC 2 reports annually; select appropriate AWS Regions based on risk assessment.
Host Infrastructure (Hardware, AWS Foundational Services)	AWS manages servers, storage hardware, networking components up to the hypervisor.	N/A	N/A
Virtualization Layer (Hypervisor)	AWS manages and secures the hypervisor.	N/A	N/A
Guest Operating System (OS)	N/A (AWS provides OS images but does not manage the running OS in customer instances).	Patching (security updates, service packs), hardening (secure configuration according to World Bank baselines), anti-malware, host-based intrusion detection/prevention (HIDS/HIPS).	WB Security Operations team applies critical OS patches within 7 days using centralized patch management system (e.g., AWS Systems Manager Patch Manager). OS images hardened per CIS Benchmarks.
Network Configuration &	AWS provides networking	Defining VPC architecture, subnet segmentation, security group rules,	WB Cloud Engineering defines and audits Security Group templates. All

Security (within VPC)	infrastructure (VPCs, subnets, route tables, internet gateways, etc.).	Network ACLs, routing, VPN/Direct Connect configuration, Web Application Firewalls (WAFs).	internet-facing applications protected by AWS WAF with World Bank-defined rulesets.
Application Security (deployed on EC2)	N/A	Secure coding practices, vulnerability scanning of applications, dependency management, runtime application self-protection (RASP) if applicable.	Development teams follow World Bank Secure SDLC; applications undergo SAST/DAST scanning before deployment.
Identity & Access Management (IAM) for AWS Resources	AWS provides IAM service.	Creating and managing IAM users, groups, roles, and policies; enforcing principle of least privilege; configuring MFA for IAM users; regular access reviews.	All IAM users must use MFA. IAM roles preferred over long-lived credentials. Quarterly access reviews for privileged roles conducted by Cybersecurity.
Data Security (on EBS, S3 accessed by EC2)	AWS provides encryption capabilities (e.g., EBS encryption, S3 encryption).	Classifying data; configuring encryption at rest (e.g., enabling EBS encryption, S3 server-side encryption with KMS) and in transit (TLS); managing encryption keys (if using customer-managed keys); data backup and recovery strategies.	All EBS volumes storing sensitive data must be encrypted using KMS. Data classification policies dictate encryption levels and key management strategies.
Logging and Monitoring (of Guest OS, Applications, Network Traffic)	AWS provides logging services (e.g., CloudTrail, VPC Flow Logs, CloudWatch).	Configuring and enabling appropriate logging; ingesting logs into SIEM; active monitoring of logs for security events; setting up alerts.	VPC Flow Logs and CloudTrail logs for all accounts are centralized and ingested into World Bank's SIEM. Custom CloudWatch alarms configured for critical security events.

- **Infrastructure as a Service (IaaS):**

- **World Bank Responsibility:** In IaaS (e.g., Amazon EC2, Azure Virtual Machines, Google Compute Engine), World Bank has the most extensive responsibilities. These include securing the guest operating system (including patches and configuration), any applications or software installed by World Bank, the configuration of virtual network firewalls (e.g., security groups, NSGs), identity and access management for the deployed resources, and the security of all data stored or processed on these instances. For instance, if World Bank deploys a custom banking application on an Azure VM, World Bank is responsible for patching the Windows Server OS, configuring the NSG to allow only necessary traffic, ensuring the application code is secure, and encrypting the data stored on the VM's disks.
- **CSP Responsibility:** The CSP is responsible for the security of the underlying physical infrastructure, the network fabric, the storage hardware, and the virtualization software (hypervisor).

- **Platform as a Service (PaaS):**

- **World Bank Responsibility:** In PaaS (e.g., AWS RDS, Azure SQL Database, Google App Engine), World Bank's responsibilities shift towards securing the application or service deployed on the platform and the data it uses. This includes managing user access to the application, configuring security settings offered by the PaaS service (e.g., database firewall rules, encryption options), securing the application code itself, and managing the data. For example, when using AWS RDS for a database, World Bank is responsible for defining database user credentials, configuring security groups to control network access to the RDS instance, and enabling encryption for data at rest.
- **CSP Responsibility:** The CSP manages the underlying infrastructure, the operating system of the platform, patching of the platform services, and the runtime environment. AWS would manage the OS patching for the RDS service and the underlying hardware.
- **Software as a Service (SaaS):**
 - **World Bank Responsibility:** In SaaS (e.g., Microsoft 365, Salesforce, Workday), World Bank's primary responsibilities revolve around managing user access (assigning licenses, configuring roles and permissions within the application), ensuring the security of data entered into or generated by the SaaS application (data classification, DLP policies), configuring application-level security settings provided by the vendor, and securing the endpoints used to access the SaaS application. For instance, when using Microsoft 365, World Bank is responsible for managing user accounts, setting up MFA, configuring email security policies, and defining data sharing permissions within SharePoint and OneDrive.
 - **CSP Responsibility:** The SaaS provider is responsible for securing the application itself, the platform it runs on, and all underlying infrastructure. Microsoft would be responsible for the security of the M365 application servers, data centers, and network infrastructure. It is important to recognize that even in a SaaS model, significant responsibilities related to data governance and user access management remain firmly with World Bank.

Section 4: World Bank's Key Responsibilities in the Cloud (Regardless of Service Model)

Certain security responsibilities always remain with World Bank, irrespective of the cloud service model. These form the core of World Bank's cloud security posture and underscore that cloud security is critically dependent on the customer's active management and configuration of their cloud environment. This necessitates skilled cloud security personnel within the bank.

1. **Data Classification and Protection:** World Bank is solely responsible for identifying and classifying its data (e.g., public, internal, confidential, restricted) and applying

appropriate protection measures. This includes implementing strong encryption for sensitive data both in transit (e.g., TLS 1.2+) and at rest (e.g., AES-256), utilizing client-side encryption or server-side encryption with customer-managed keys (CMK) where appropriate, and deploying Data Loss Prevention (DLP) controls.

2. **Identity and Access Management (IAM):** World Bank must define and manage identities, and control access to its cloud resources and applications. This involves implementing strong authentication mechanisms (e.g., mandatory Multi-Factor Authentication - MFA), enforcing the principle of least privilege for all user and service accounts, conducting regular access reviews (e.g., quarterly for privileged access), and managing the lifecycle of identities.
3. **Secure Configuration of Cloud Services:** All CSP services utilized by World Bank must be configured securely, adhering to World Bank's security baselines, regulatory requirements (e.g., CIS Benchmarks), and industry best practices. This includes avoiding default permissive settings, disabling unnecessary services or features, and regularly auditing configurations for compliance.
4. **Application-Level Security:** For any custom applications developed and deployed by World Bank in the cloud, or third-party applications integrated with cloud services, World Bank is responsible for ensuring their security. This includes secure software development lifecycle (SSDLC) practices, regular vulnerability scanning of application code (SAST/DAST), and protection against common web application threats (e.g., OWASP Top 10).
5. **Network Security Configuration (Client-Side):** World Bank is responsible for designing and implementing its virtual network architecture within the cloud. This includes defining network segmentation (e.g., VPCs, subnets), configuring firewalls (e.g., security groups, network ACLs, Azure Firewall), implementing Web Application Firewalls (WAFs) for web-facing applications, and establishing secure private connectivity to on-premises environments (e.g., AWS Direct Connect, Azure ExpressRoute).
6. **Logging, Monitoring, and Incident Response:** World Bank must ensure comprehensive logging of activities within its cloud environments (e.g., API calls, login attempts, configuration changes), actively monitor these logs for suspicious activities and potential threats using tools like Security Information and Event Management (SIEM), and establish and test clear incident response procedures tailored to cloud environments.
7. **Compliance and Governance:** World Bank is responsible for ensuring that all its cloud deployments and operations comply with relevant legal, regulatory (e.g., FFIEC, GDPR, PCI DSS, DORA), and internal governance requirements. This includes conducting regular risk assessments, implementing necessary controls, and maintaining documentation to demonstrate compliance.

Section 5: Addressing Common Cloud Misconfigurations

Cloud misconfigurations are a leading cause of security breaches. Focusing on preventing these common pitfalls is a highly practical and impactful security strategy, significantly reducing World Bank's attack surface. This requires diligent configuration management and, where possible, automation to check for and remediate these issues.

World Bank has established specific preventative controls and policies for the following common misconfigurations:

1. **Unrestricted Inbound/Outbound Ports (Overly Permissive Security Groups/Firewalls):**

- **Risk:** Exposes services to unauthorized access and attack, allows data exfiltration or command-and-control communication.
- **World Bank Control:** All cloud network firewalls (e.g., AWS Security Groups, Azure Network Security Groups) must adhere to a "deny-all by default" policy. Explicit "allow" rules are only permitted for necessary, documented traffic, subject to review and approval by the Cloud Security team. Regular automated compliance checks are performed to identify and flag overly permissive rules. External access is restricted to specific IP ranges where feasible.

2. **Inadequate Secrets Management (e.g., API keys, credentials in code, default passwords):**

- **Risk:** Compromised secrets can grant attackers extensive unauthorized access to cloud resources and data.
- **World Bank Control:** Mandatory use of approved secrets management services (e.g., AWS Secrets Manager, Azure Key Vault, HashiCorp Vault) for storing and rotating all API keys, database credentials, and other secrets. Hardcoding secrets in application code, configuration files, or environment variables is strictly prohibited. Source code repositories are regularly scanned for exposed secrets. Default credentials for any service must be changed immediately upon provisioning.

3. **Disabled or Insufficient Logging and Monitoring:**

- **Risk:** Inability to detect security incidents in a timely manner, investigate breaches, or meet compliance requirements for audit trails.
- **World Bank Control:** Comprehensive logging (e.g., AWS CloudTrail, Azure Monitor logs, VPC Flow Logs, application logs) must be enabled for all cloud resources and services. Logs must be configured for long-term retention in a secure, tamper-evident manner and ingested into World Bank's central SIEM system for continuous monitoring, correlation, and alerting. Regular reviews are conducted to ensure adequate log coverage and alert effectiveness.

4. **Publicly Accessible Storage Buckets/Containers (e.g., AWS S3, Azure Blob Storage):**

- **Risk:** Accidental exposure of sensitive data to the public internet, leading to data breaches and regulatory penalties. The Capital One breach is a notable example of risks associated with misconfigured cloud storage and firewalls.
- **World Bank Control:** All cloud storage buckets/containers are to be configured as private by default. Public access is strictly prohibited unless a documented business justification is provided and a formal risk assessment and exception approval are granted by the CISO. Automated tools (e.g., AWS S3 Block Public Access, Azure Policy) are implemented to prevent public exposure and continuously scan for misconfigured buckets. Data classification labels must be applied to all storage.

5. **Overly Permissive IAM Roles and Policies:**

- **Risk:** Excessive user or service privileges increase the potential impact (blast radius) if an account or role is compromised, facilitating lateral movement and privilege escalation.
- **World Bank Control:** Strict adherence to the principle of least privilege for all IAM users, groups, roles, and policies. Permissions should be narrowly scoped to only what is necessary for the intended function. Regular (e.g., quarterly) access reviews for all privileged roles and accounts are mandatory. Use of condition-based IAM policies and permission boundaries is encouraged to further restrict access. Wildcard permissions (e.g., `*:*`) are prohibited in IAM policies without explicit CISO approval for specific, justified use cases.

6. **Insecure Automated Backups (e.g., unencrypted, overly accessible, not tested):**

- **Risk:** Backup data, if not properly secured, can become an attractive target for attackers or lead to data exposure if access controls are weak. Untested backups may fail during a recovery scenario.
- **World Bank Control:** All cloud backups must be encrypted at rest using strong encryption standards (e.g., AES-256). Access to backup data must be strictly controlled, logged, and subject to permissions that mirror or exceed those on the primary data. Backup and restore procedures must be documented and regularly tested (at least annually for critical systems) to ensure data integrity and recoverability within defined RTO/RPO targets.

Appendix A: Shared Responsibility Matrix Template for

(This appendix would contain a detailed matrix template for a specific service like AWS S3, outlining tasks such as bucket creation, enabling versioning, configuring server-side encryption, defining bucket policies, setting up lifecycle rules, managing object ACLs,

monitoring access logs, and delineating responsibilities between AWS and World Bank for each task.)