Shared Security Responsibility Model (SSRM)

Update July 2025

Contents

Purpose

xPlatform is a DevOps-as-a-Service platform provided by SCB TechX, designed to enable development teams to efficiently build, deploy, and operate applications within a secure, compliant, and multi-tenant cloud environment. Security and compliance within xPlatform are governed by a shared responsibility model between SCB TechX (as the Cloud Service Provider - CSP), and the customer (as the Cloud Service Customer - CSC). This shared model enables customers to design and implement a highly flexible, customizable, and scalable solution to meet their business requirements while minimizing operational responsibilities and costs.

In general, SCB TechX is responsible for the following:

- Developing and maintaining secure core application code
- Maintaining the security of the platform
- Ensuring the platform is compliant with relevant industry standards and compatible with technology components that meet applicable security requirements
- Responding to security issues concerning the core platform
- Working with cloud service provider and customer to resolve any issues that occur

Customers are responsible for the following:

- Maintaining security for customer code and integrations with third-party applications
- Ensuring secure application development
- Reacting and responding to security incidents

SCB TechX Responsibilities

SCB TechX is responsible for the security and availability of the xPlatform environment and the core solution code. In addition, SCB TechX is responsible for the necessary activities and mechanisms that maintain the security of the xPlatform solution, including:

- Applying server-level security and patches for applications supported by xPlatform
- Conducting penetration testing and scanning of the core xPlatform code
- Conducting semi-annual reviews and audits of authorized users, including SCB TechX employees
- Conducting annual testing of backup and restore functionality
- Configuring server and firewalls

- Connection and configuring the xPlatform repository
- Defining, testing, implementing, and documenting disaster recovery (DR) plans for the areas within xPlatform's scope of responsibility
- Defining platform web application firewall (WAF) rules
- Hardening the operating system (OS)
- Implementing and maintaining the integration of customer and xPlatform
- Monitoring, logging, and remediating security incidents concerning the xPlatform
- Provisioning of production and staging environments refer specifically to the creation of resource
- Assessing potential security threats to platform operations and infrastructure
- Testing the platform for security vulnerabilities

Customer Responsibilities

The customer is responsible for following security best practices for their specific, customized instance of xPlatform solution:

- Setup landing zones or cloud accounts
- Adding the necessary configuration files to the repository
- Applying security and other patches to the tenant's cloud infrastructure
- Creating, deploying, and testing application code
- Designing, theming, installing, integrating, and securing all custom extensions and code
- Managing user access to the tenant's cloud infrastructure, applications and platform instances, including granting and revoking access as needed
- Handling security issues related to the tenant's internal network, servers, infrastructure, and any custom applications built on cloud infrastructure platform
- Monitoring all application activities that might reveal a potential security threat, including penetration testing, vulnerability scans, and logs
- Monitoring and responding to security incidents on the tenant's cloud infrastructure and applications, including forensic investigation and remediation
- Running performance tests on the customized application
- Securing access to the platform accounts

- Testing and QA of the custom application
- Maintaining the security of any systems or networks within the tenant's cloud infrastructure and applications

Cloud Service Provider Responsibilities

SCB TechX relies on well-established cloud service provider to host the cloud server infrastructure for xPlatform. The provider is responsible for security of the network, including routing, switching, and perimeter network security via firewall systems and intrusion detection systems (IDS). In addition, the provider manages the physical and environmental security of the data centers hosting the xPlatform solution.

Cloud service provider is also responsible for:

- Maintaining PCI DSS, SOC 2, CSA, and ISO 27001 certifications for their cloud services
- Secure the hypervisor
- Securing the data center, including both physical and network access
- Power, fire detection and suppression

RACI Matrix

Responsibility Area	Platform Team (IDP Provider)	Customer Team (Tenant)	Note
Platform infrastructure (HA, Patching) includes orchestrator and executor components	R, A	I	Infrastructure availability, patching, performance
Identity & Access Management (SSO, RBAC)	R, A (xPlatform)	R, A (Customer Tenant)	Enterprise customer manages IdP and mapping internal roles
Tenant Isolation (Company)	R, A	I	Strong tenant boundaries enforced
Service Catalog (CI/CD, IaC, Templates)	R, A	R, C	Platform offers reusable components
Application Deployment	C	R, A	Tenants deploy via IDP
Secrets & Configuration Management	C	R, A	Customer stores app secrets
Observability (Logs, Metrics, Dashboards)	R, A (xPlatform)	R, A (Customer Applications)	Provide and operate observability stack
Audit & Security Logs (Platform-level)	R, A	I	Maintained by provider for all actions
Audit & Security Logs (Tenant-level)	I	R, A	Tenant manages and reviews their app/system logs
Security & Compliance (Policy, Scanning) (Platform-level)	R, A	I	Maintained by provider for all actions
Security & Compliance (Policy, Scanning) (Tenant-level)	I	R, A	Tenant manages and reviews their security policies and tools
Cost Governance	R, A (xPlatform)	R, A (Customer Tenant)	Maintained by provider for all actions
Incident Management	R, A (xPlatform)	R, A (Customer Applications)	Split between platform-level and app-level
Developer Self-Service UI/AP	R, A (xPlatform)	R (Customer Applications)	Self-service tooling provided by platform
Data Lifecycle Management	R, A (system metadata, logs, CICD Artifacts and Backup)	R, A (Customer Applications)	Platform defines lifecycle for platform data; Tenant defines for their data (creation, usage, sharing, retention, deletion)
Backup & Disaster Recovery	R, A (xPlatform)	R (Customer Applications)	Platform backs up configs; Tenant owns application/data backups

*R – Responsible: The person(s) who do the work to complete the task

*A – Accountable: The person who is ultimately answerable for the task and has decision-making authority

*C – Consulted: People who provide input and expertise before or during the task

*I – Informed: People who need be kept updated on progress or outcomes