



# Securing the Core

## Navigating the Shared Responsibility Model in SAP Cloud ERP Private

By Robert Holland

As organizations accelerate their move to the cloud, the transition from traditional data centers to SAP Cloud ERP Private (formerly known as RISE with SAP) introduces a fundamental shift in how security is managed. For years, the SAP ecosystem has operated under the assumption that the customer maintains total control, and at the same time total responsibility, for the entire stack. In the cloud, this paradigm shifts to a Shared Responsibility Model, a framework that divides security and operational duties between SAP and the customer.

However, [research](#) from SAPinsider indicates a significant gap between the existence of this model and its actual implementation. While the model is designed to streamline operations and enhance protection, as many as a third of those already using SAP Cloud ERP Private are not following the model

### Key Takeaways

➤ SAPinsider research reveals that nearly one-third of organizations already running SAP Cloud ERP Private are not rigorously following the Shared Responsibility Model, leaving mission-critical SAP S/4HANA systems exposed to preventable security risks.

➤ SAP's Enterprise Cloud Services (ECS) has issued mandatory hardening requirements—including SAP Notes 3250501, 3381209, and 3480723—covering ABAP, Java, and SAP HANA systems, yet only 33% of live SAP Cloud ERP Private customers regularly audit for compliance.

➤ Understanding the division of security duties between SAP and the customer is not optional—failure to follow the Roles and Responsibilities (R&R) documentation means customers, not SAP, bear full liability in the event of a breach or cyberattack..

rigorously while nearly two thirds of those who are in the process of deploying or exploring remain unaware of their specific obligations, potentially leaving mission-critical systems exposed to evolving threats.

## Who Owns What?

The SAP Cloud ERP Private environment is a “single-tenant” managed landscape where SAP manages the infrastructure and creates customer-specific subscriptions, essentially a platform-as-a-service environment that is designed to support SAP S/4HANA Cloud Private Edition. This architectural setup is the foundation of the Shared Responsibility Model.

### SAP’s Responsibilities: The Infrastructure Layer

SAP acts as the Cloud Service Provider (CSP) and is responsible for securing what would traditionally be handled by the cloud or infrastructure provider. This encompasses the operations and management of the cloud environment, including:

- **Infrastructure Management:** SAP manages the underlying IaaS provider subscriptions (e.g. Amazon Web Services or Microsoft Azure), including the creation of logically isolated Virtual Private Networks (VNETs) and subnets.
- **Technical Basis Support:** This includes regular patching, maintenance, and HANA services management.
- **Physical and Data Center Security:** SAP ensures the physical integrity of data centers, whether owned by SAP, a hyperscaler, or a third-party partner.
- **Monitoring and Incidents:** SAP provides 24/7 security monitoring, personal data breach notifications, and manages vulnerability assessments and penetration testing.
- **Backups:** SAP handles standard file system and database backups as part of its standard service.

### Customer Responsibilities: The Application Layer

The customer is responsible for “Security in the Cloud”. Because the customer owns their data, they must manage:

- **Identity and Access Management:** Customers are broadly responsible for user identity, authentications, and application-level authorizations.
- **Data Governance:** Ensuring data is classified and protected according to business needs is a purely customer-driven task.
- **Application Audit Logging:** While SAP provides the infrastructure, the customer must manage and analyze application security audit logs.
- **Business Process Logic:** Managing the workflows, transports between environments, and custom code (In-App or Side-by-Side extensions) remains with the customer.
- **Connectivity Procurement:** While SAP assists with software configuration, the customer is responsible for procuring physical “dedicated connectivity” (such as AWS Direct Connect or Azure Express Route) if their compliance requirements demand it.

## A Growing Security Gap

The [RISE with SAP 2025 Benchmark Report](#) highlights a concerning trend regarding the adoption of this model. While nearly half of respondents (45%) report being aware of and actively following the model, nearly a third (32%) are aware but admit to not following it rigorously. Although more of those who are already using SAP Cloud ERP Private (62%) report that they are aware of the model and are following it rigorously, this is still less than two thirds of those organizations.

Most alarming is the status of those earlier in the journey. Among organizations currently in the exploration or deployment phase, 30% are entirely unaware that a shared responsibility model exists. And 5% of those who are already using SAP Cloud ERP Private fall in the same category. This lack of awareness is not merely an administrative oversight; it is a critical security vulnerability. Failure to rigorously follow the shared responsibility model, combined with a lack of adherence to mandatory security parameters, leaves systems open to attack.

Furthermore, for those already running SAP Cloud ERP Private, only one-third (33%) regularly audit for compliance with mandatory requirements such as SAP Note 3250501. This suggests that many organizations view cloud migration as a “set and forget” activity, rather than an ongoing commitment to security hygiene.

The complexity of the shared responsibility model document may go some way to explaining why organizations are not following it rigorously. However, this is where working closely with an experienced partner can make a significant difference.

## Hardening the ECS Environment

To provide a baseline of security for subscription-based services sold by SAP, SAP’s Enterprise Cloud Services (ECS) organization has released mandatory hardening requirements. These are documented in specific SAP Notes and are mandatory for all ECS customers. The notes include areas such as critical ICF services, securing standard users, client settings, message server hardening, and restricting access to password hashes.

### 1. ABAP System Hardening (Note 3250501)

For ABAP-based systems, the security parameters must be set in the Default Profile (DEFAULT.PFL). Key requirements include:

- Password Policies: Minimum password length is set to 15 characters. Organizations must maintain a history size of 15 previous passwords to prevent reuse and set an expiration time between 30 and 90 days.
- Login Security: Automatic unlocking of users at midnight must be disabled, and invalid login attempts are limited to six before a user lock is triggered.
- RFC and Gateway Security: The system enforces strict ACL rules (secinfo/reginfo) to prevent the unauthorized launching of external programs. Global deactivation of authorization objects is prohibited.
- Logging: Gateway logging and HTTP logging in the ICM must be enabled to ensure an audit trail of all actions.

### 2. Java System Hardening (Note 3381209)

Java systems hosted in ECS must also meet elevated security policy standards.

- Session Security: The “httponlycookie” and “enforce\_secure\_cookie” properties must be set to TRUE to prevent malicious client-side scripts from reading logon tickets and ensure cookies are only sent over SSL.
- Protocol Security: Support for SSL/TLS is restricted to versions 1.2 and 1.3 to eliminate vulnerabilities in older protocols.
- User Management: Customers are advised to create their own “CUSTOMER\_MANAGED\_USER” policy profiles rather than relying on defaults.

### 3. SAP HANA Database Hardening (Note 3480723)

As the data foundation, SAP HANA requires the most stringent database-level hardening.

- Persistence Encryption: ECS standard requires Data-at-Rest Encryption (AES-256-CBC) to be enabled for data volumes, redo log volumes, and backups.
- Audit Policies: A set of default actions must be audited, including changes to audit policies, enabling/disabling

- auditing, and authentication method changes.
- Password Locking: Even the SYSTEM user must be locked after too many invalid connect attempts to prevent brute-force attacks.

Following the details provided in these notes is important for both customers and SAP to meet the requirements detailed in the shared responsibility model. By following these notes customers can ensure that they remain current with any requirements from SAP. This ensures that their systems remain in line with SAP's "secure by default" settings as standards evolve.

When these notes are not consistently followed issues can arise with these "secure by default" systems after hand-off. For example, the customer may alter the configuration which results in the system no longer being "secure by default". Or SAP may be unable to apply new requirements in systems that have already been delivered to customers. This can lead to configuration drift where systems become out of alignment with SAP security standards over time. The situation can be exacerbated by constant changes in requirements which constantly evolve to address new threats and vulnerabilities.

## Navigating Standard, Optional, and Excluded Services

To effectively use the shared responsibility model, organizations must understand the service catalog provided in the Roles and Responsibilities (R&R) documentation. The R&R document is the "Documentation of record" and categorizes tasks into several tiers:

1. **Standard Services:** These are included in the service fee and performed by SAP. Examples include system outage notifications, standard backups, and technical monitoring of system components.
2. **Optional Services:** These are not covered by standard fees and require specific contracting. This includes high-level scaling of compute capacity or specialized industry regulation support (e.g., GxP or HIPAA).
3. **Packaged Services:** These are tasks the customer can perform but may elect to have SAP deliver for an additional fee. This includes complex activities like Application Security Monitoring or Segregation of Duty (SoD) checks. An example of this is SAP's Cloud Application Services (CAS). However, partner solutions like the [Cybersecurity Extension for SAP](#) (CES) from Layer Seven Security may offer more coverage at a lower cost. CES is certified for SAP RISE and automates compliance checks for mandatory Cloud ERP security requirements.
4. **Excluded Tasks:** These can only be performed by the customer. SAP ECS cannot, for instance, define the customer's overarching security concept, design print forms, or approve solution signoffs.

## Conclusion

The move to SAP Cloud ERP Private offers unparalleled opportunities for business transformation, but it requires a mature approach to security. The Shared Responsibility Model is the blueprint for this maturity. By understanding the division of labor, adhering to mandatory hardening requirements for ABAP, Java, and SAP HANA, and rigorously auditing compliance, organizations can protect their most vital assets.

The data is clear that those who follow the model are better protected, but too many are still falling through the cracks. For those considering, evaluating, or moving to SAP Cloud ERP Private it is vital to treat the Roles and Responsibilities document as your primary security manual, and ensure your team is among those who are not just aware, but actively and rigorously following the model. The security of SAP systems and data running in cloud environments depends on it.

## What This Means for SAPinsiders

As the threat landscape evolves, awareness of the shared responsibility model is no longer sufficient. Organizations must move toward operational excellence by following these steps, and security vulnerabilities can increase over time unless customers make efforts to monitor the changes in the requirements and perform regular audits to remain compliant.

With more than two thirds of those responding to SAPinsider research not regularly auditing for compliance there is a significant risk as systems move further out of alignment with “secure by default” requirements. Any security incident, for example a cyber attack leading to a data breach, could lead to a breakdown of the shared model. In that situation, the customer would be liable for any repercussions, not SAP. Only when customers maintain their responsibilities will liabilities be shared.

» **Regularly audit against the reference roles and responsibilities.** The roles and responsibilities document is not static. Version 7.2025 (July 2025) reflects the most current division of labor, but information is updated regularly. Organizations must review this document in collaboration with their SAP Cloud Architect Advisor (CAA) or Client Delivery Manager (CDM) to ensure no gaps exist in their specific computing environment. SAP provides these updates for legal reasons of liability management, not simply as best practices. Not following them can have significant consequences.

» **Institutionalize change request reviews.** A significant portion of organizations (49%) exploring RISE do not yet review all change requests to ensure they do not impact mandatory security requirements. For those already live, 67% do perform this review, but the remainder are at risk. Every technical or functional change must be vetted against the mandatory parameters in SAP Notes 3250501, 3381209, and 3480723 to ensure that customization does not degrade the system’s security posture.

» **Close the exploration phase knowledge gap.** The fact that 30% of those in the exploration phase are unaware of the shared responsibility model is a call to action for project leads. Security must be a “day zero” conversation. Organizations should not wait until the build phase to define who will manage user roles, who will analyze audit logs, and how identity federation (e.g., via Azure AD) will be handled.

» **Augment standard services with experienced cybersecurity partners.** The research highlighted significant operational gaps: although SAP is managing the infrastructure, many are either not following or are unaware of the shared responsibility model. To bridge this gap, organizations should move beyond relying solely on standard offerings and engage with knowledgeable partners like Layer Seven Security. By taking this approach, organizations can access a unified alternative to what can be fragmented standard offerings. Working with a specialized partner ensures visibility into “excluded” or “optional” areas that are often left unmonitored such as deep forensic visibility, custom code and UI5 security, and unified compliance dashboards.



Layer Seven Security is an SAP Services Partner and a leading provider of security services and solutions for SAP customers. It's SAP certified Cybersecurity Extension for SAP automates vulnerability management, custom code security, and threat detection as part of the shared model of responsibility in SAP RISE / Cloud ERP. The solution also supports automated compliance monitoring for SAP ECS security requirements. The Cybersecurity Extension for SAP ensures your SAP systems are compliant, protected and equipped for audits and certifications. Flexible licensing options are available for both one-time assessments and sustained monitoring.

[www.layersevensecurity.com](http://www.layersevensecurity.com)