



Shared responsibilities after RISE

Bo BAADE-PEDERSEN, SAP
October 20, 2026

SBN SAP Conference 2026

INTERNAL – SAP and External Parties under NDA Only



Agenda

Why shared responsibility matters



- 01 RISE operates on a strict shared responsibility model
 - 02 SAP manages cloud infrastructure, OS, Database and platform security
 - 03 Customers retain 100% responsibility for application layer
 - 04 Your data, users, roles, custom code, configurations - all your responsibility
- RISE is shared, not outsourced**

INTERNAL – SAP and External Parties under NDA Only

3

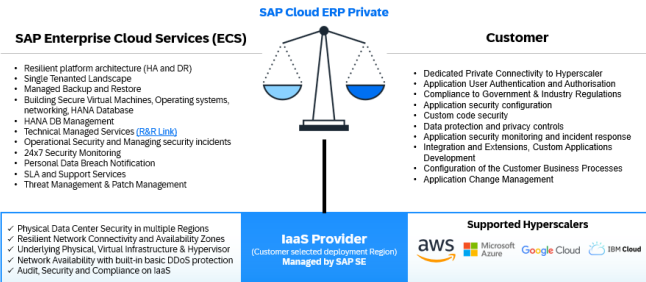
SAP Cloud ERP Private – Tenancy Model



INTERNAL – SAP and External Parties under NDA Only

5

Shared Security Responsibility Model



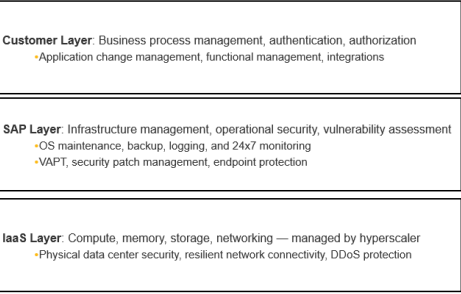
INTERNAL – SAP and External Parties under NDA Only

6

Shared security governance stack

Each layer has clear ownership — no grey areas

The shared responsibility model is a partnership built on trust and expertise



INTERNAL – SAP and External Parties under NDA Only

7

SAP Cloud ERP Private: Roles & Responsibilities

Standard Services, performed by SAP by default as part of the contract



INTERNAL – SAP and External Parties under NDA Only

13



Why shared responsibility matters



01

RISE operates on a strict shared responsibility model

02

SAP manages cloud infrastructure, OS, Database and platform security

03

Customers retain 100% responsibility for application layer

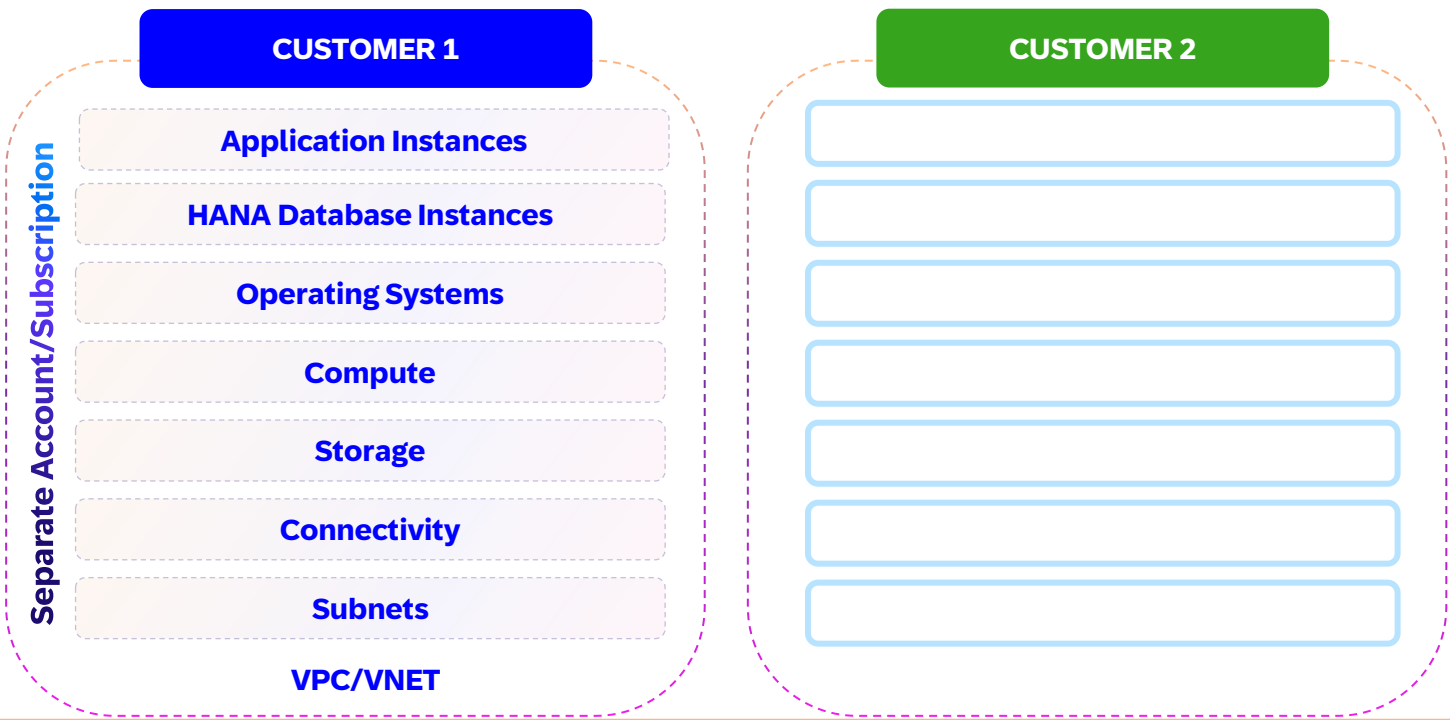
04

Your data, users, roles, custom code, configurations - all your responsibility

RISE is shared, not outsourced

SAP Cloud ERP Private – Tenancy Model

SAP Cloud ERP Private = single-tenant landscape
Dedicated infrastructure with no customer sharing
Choose your hyperscaler: AWS, Azure, or Google Cloud



SAP owns and manages the hyperscaler root account
Customer does not have access to underlying cloud subscription
SAP applies global security policies through secure-by-default deployment
SAP ECS policies enforced through compliance scans

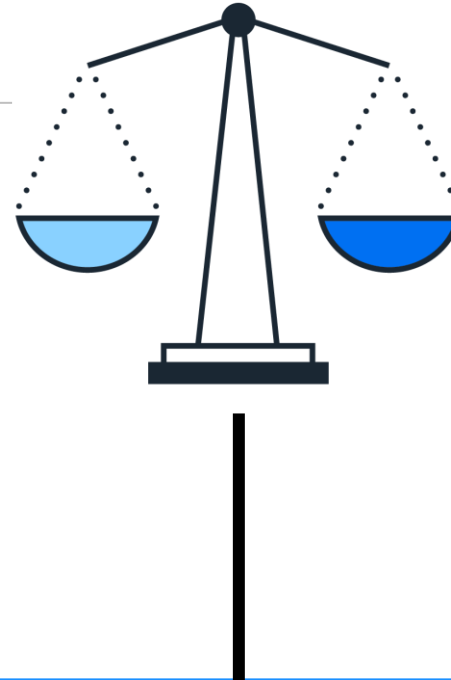
	IaaS Provider	Customer's Choice – AWS, Azure or Google Cloud	   
	Regional Admin VPC	Regional Admin Infrastructure Secure Admin Connectivity Jump Hosts	
	SAP Global Security Operations	Monitoring & Alerting Provisioning & Automation SIEM Asset & Lifecycle Management VAPT & Security Patch Management End Point Protection Capacity Management Admin Access	

Shared Security Responsibility Model

SAP Cloud ERP Private

SAP Enterprise Cloud Services (ECS)

- Resilient platform architecture (HA and DR)
- Single Tenanted Landscape
- Managed Backup and Restore
- Building Secure Virtual Machines, Operating systems, networking, HANA Database
- HANA DB Management
- Technical Managed Services ([R&R Link](#))
- Operational Security and Managing security incidents
- 24x7 Security Monitoring
- Personal Data Breach Notification
- SLA and Support Services
- Threat Management & Patch Management



Customer

- Dedicated Private Connectivity to Hyperscaler
- Application User Authentication and Authorisation
- Compliance to Government & Industry Regulations
- Application security configuration
- Custom code security
- Data protection and privacy controls
- Application security monitoring and incident response
- Integration and Extensions, Custom Applications Development
- Configuration of the Customer Business Processes
- Application Change Management

- ✓ Physical Data Center Security in multiple Regions
- ✓ Resilient Network Connectivity and Availability Zones
- ✓ Underlying Physical, Virtual Infrastructure & Hypervisor
- ✓ Network Availability with built-in basic DDoS protection
- ✓ Audit, Security and Compliance on IaaS

IaaS Provider

(Customer selected deployment Region)
Managed by SAP SE

Supported Hyperscalers



Shared security governance stack

Each layer has clear ownership
— no grey areas

The shared responsibility model
is a partnership built on trust and
expertise



Customer Layer: Business process management, authentication, authorization

- Application change management, functional management, integrations

SAP Layer: Infrastructure management, operational security, vulnerability assessment

- OS maintenance, backup, logging, and 24x7 monitoring
- VAPT, security patch management, endpoint protection

IaaS Layer: Compute, memory, storage, networking — managed by hyperscaler

- Physical data center security, resilient network connectivity, DDoS protection

Key security and compliance capabilities

Defend against cyberattacks

while you improve efficiency and reduce costs

~99%

cloud security posture management compliance, exceeding the industry average

Manage compliance

with global and regional regulatory requirements

~130

internal and external audits, conducted regularly

Mitigate skills shortages

through SAP security and compliance experts

~750k

managed cloud systems secured across 26 industries (including critical infrastructures)



Secure development lifecycle (DevSecOps)



Network and cloud security posture management



Data protection and sovereign cloud



Identity and access management



Threat and vulnerability management



Security logging and monitoring



Incident response



Business continuity and disaster recovery

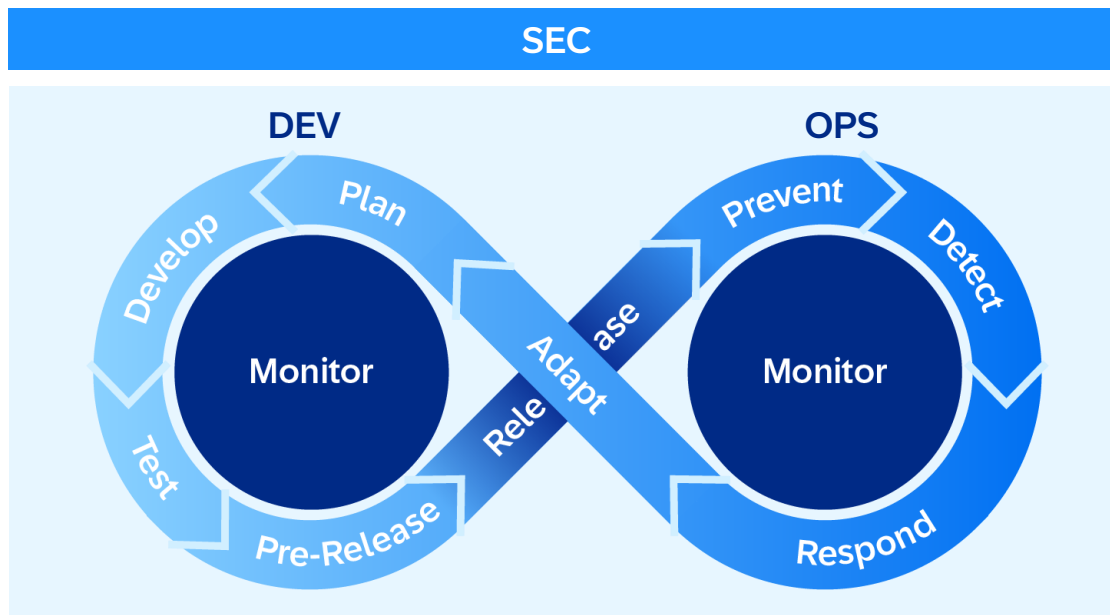


Governance and regulatory compliance

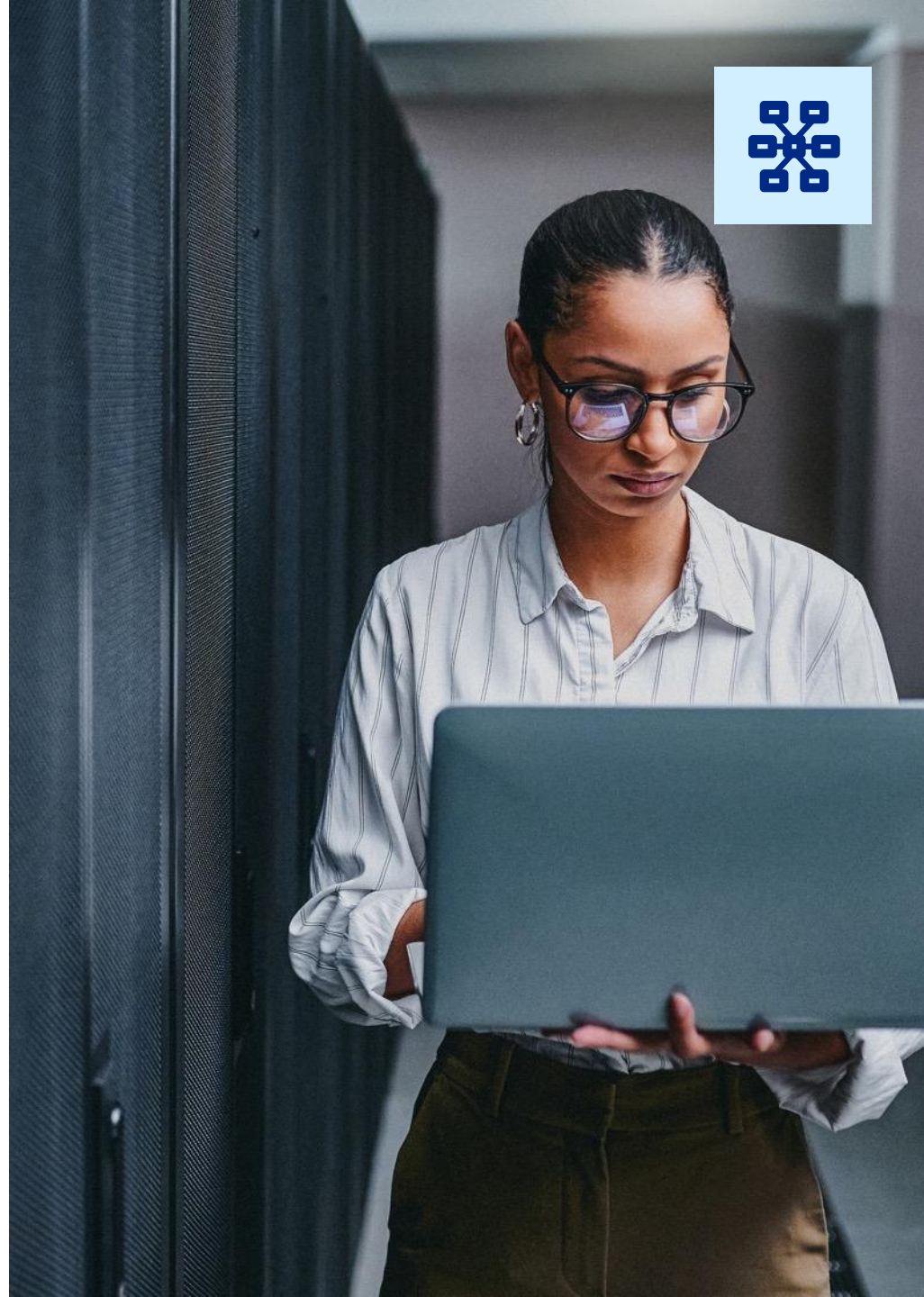
Secure development lifecycle (DevSecOps)

Incorporate security measures throughout the software development lifecycle to enable robust protection against vulnerabilities and deliver secure, high-quality applications.

Key objectives: Automating testing and code analysis, integrating security validation within CI/CD pipelines, and leveraging threat intelligence to address risks proactively.



<https://www.sap.com/documents/2016/03/a248a699-627c-0010-82c7-eda71af511fa.html>



Security Patch Management



SAP manages security through regular vulnerability advisories from software vendors and NIST, complemented by periodic system scans. Testing and validation are thoroughly documented and reviewed by the Change Advisory Board (CAB). Customers can view the patch schedule on the Customer Portal, with deployment managed in a coordinated manner. An effective incident management process swiftly addresses any issues with system patches.

Regular Vulnerability Assessment and Classification



- SAP publishes vulnerability advisories using inputs from software vendors and the NIST database, prioritizing based on severity and impact.
- Vulnerabilities are rated with CVSS v3.1 scores. SAP also strategizes the automated scanning procedures to detect and report vulnerabilities in the cloud environment.

Comprehensive Testing and Verification



- SAP tests and validates patches, including those for operating systems, databases, and third-party software, in lab environments (vLAB) before creating a Mass Change Ticket (MCT) for Change Advisory Board (CAB) approval.
- Critical patches with a CVSS score above 9.0 are expedited through an Emergency Patching Procedure.

Managed Deployment and Monitoring



- Patches that don't require downtime are applied automatically, starting with non-production systems and followed by a cooling period before production patches.
- For offline patches requiring downtime, customers can schedule them with thorough testing in non-production environments and coordinated release planning between SAP and the customer.

Swift Incident Response and Remediation



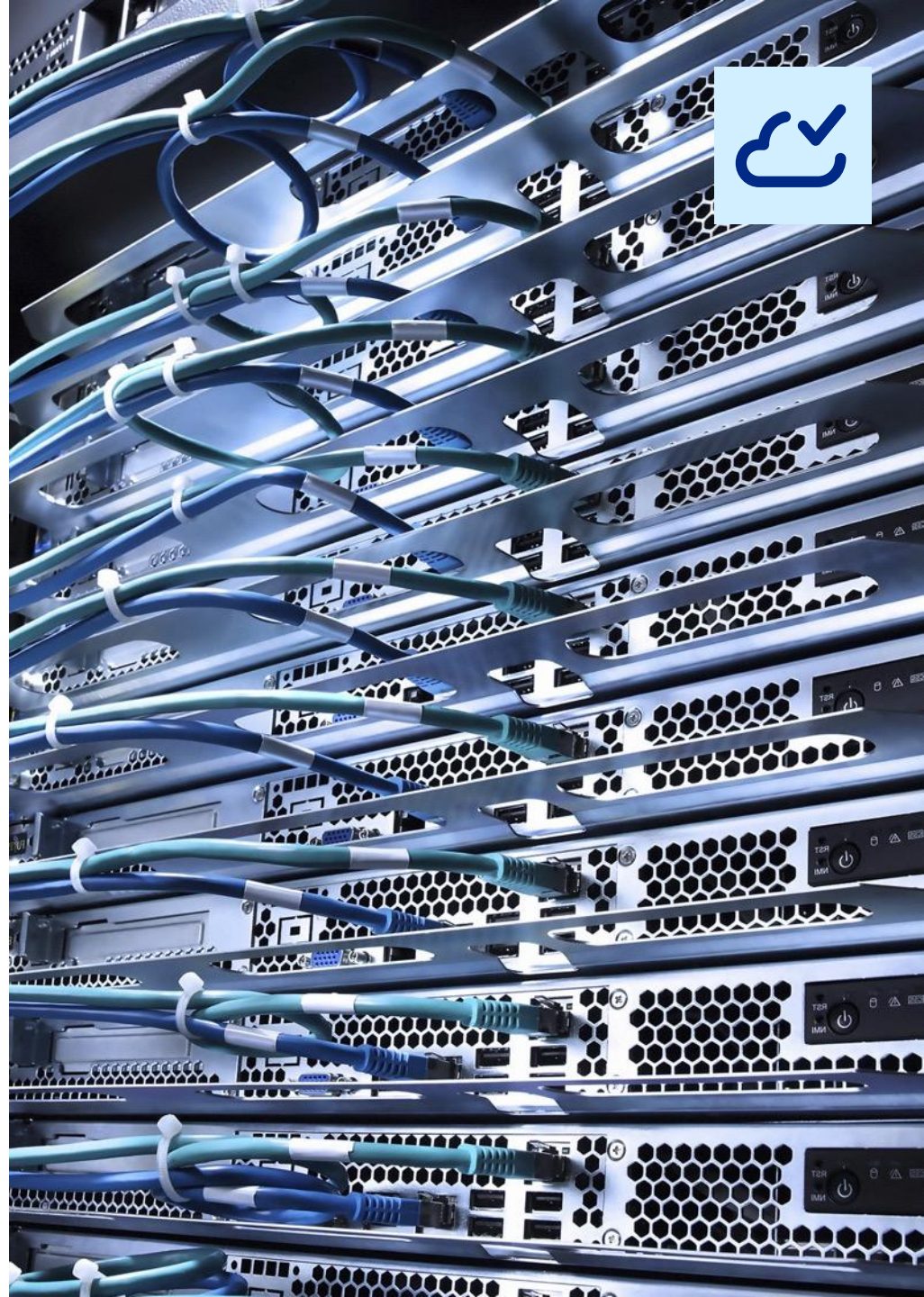
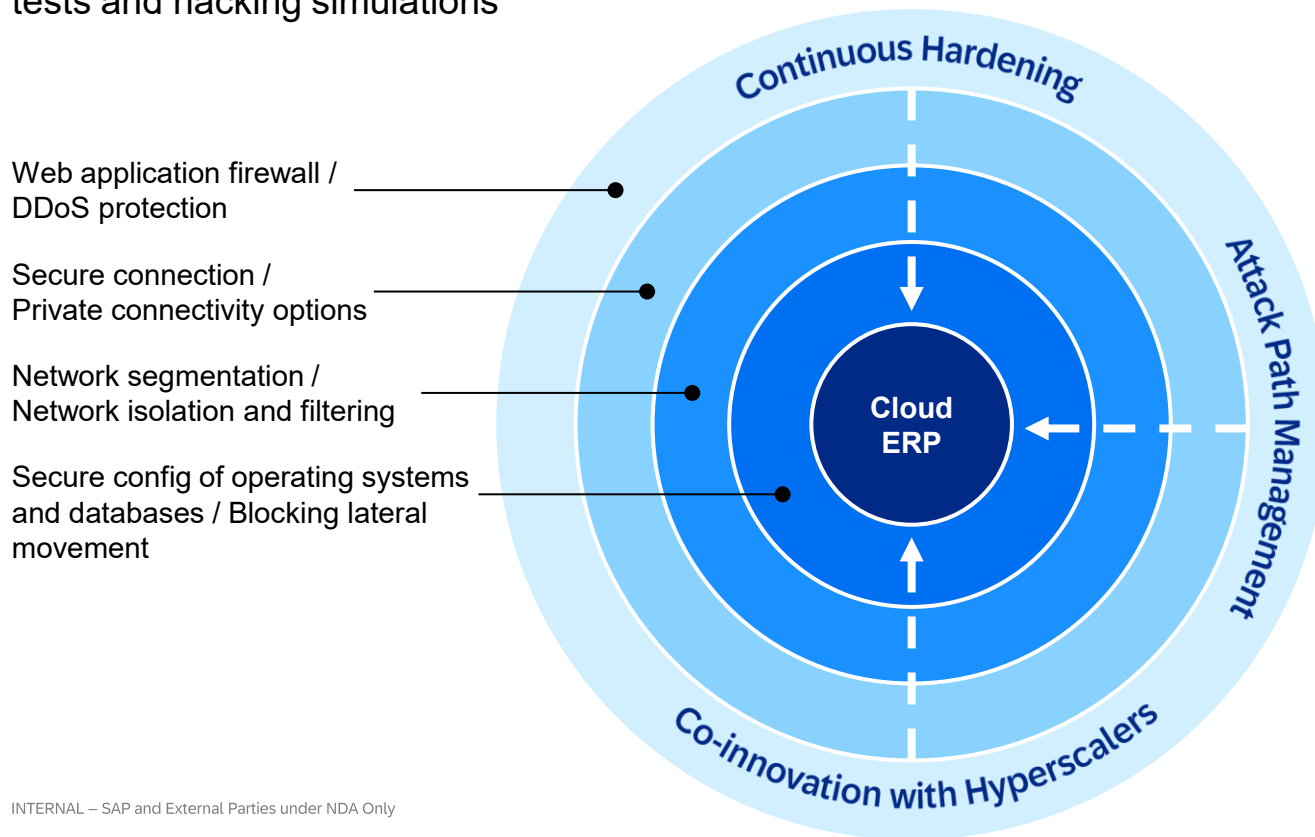
- Systems are continuously monitored, with events managed through an Alert Management framework that generates incident tickets for issues following patching.
- For critical incidents affecting production, classified as "Very High," there is a 20-minute response time and a 4-hour for resolution or workaround or action plan.

Refer the Cloud Services from [SAP Vulnerability Management Guide](#) for more details.

Network and cloud security posture management

Continuously assess and monitor the security configurations and compliance of network and cloud resources, helping to ensure adherence to best practices and standards.

Key objectives: Continuous compliance with cloud security configurations, periodic assessments in the form of penetration tests and hacking simulations



SAP Cloud ERP Private: Roles & Responsibilities

Standard Services, performed by SAP by default as part of the contract



SAP Cloud ERP Private: Roles & Responsibilities

Optional Services, itemized in the customer's contract (or via a change request)



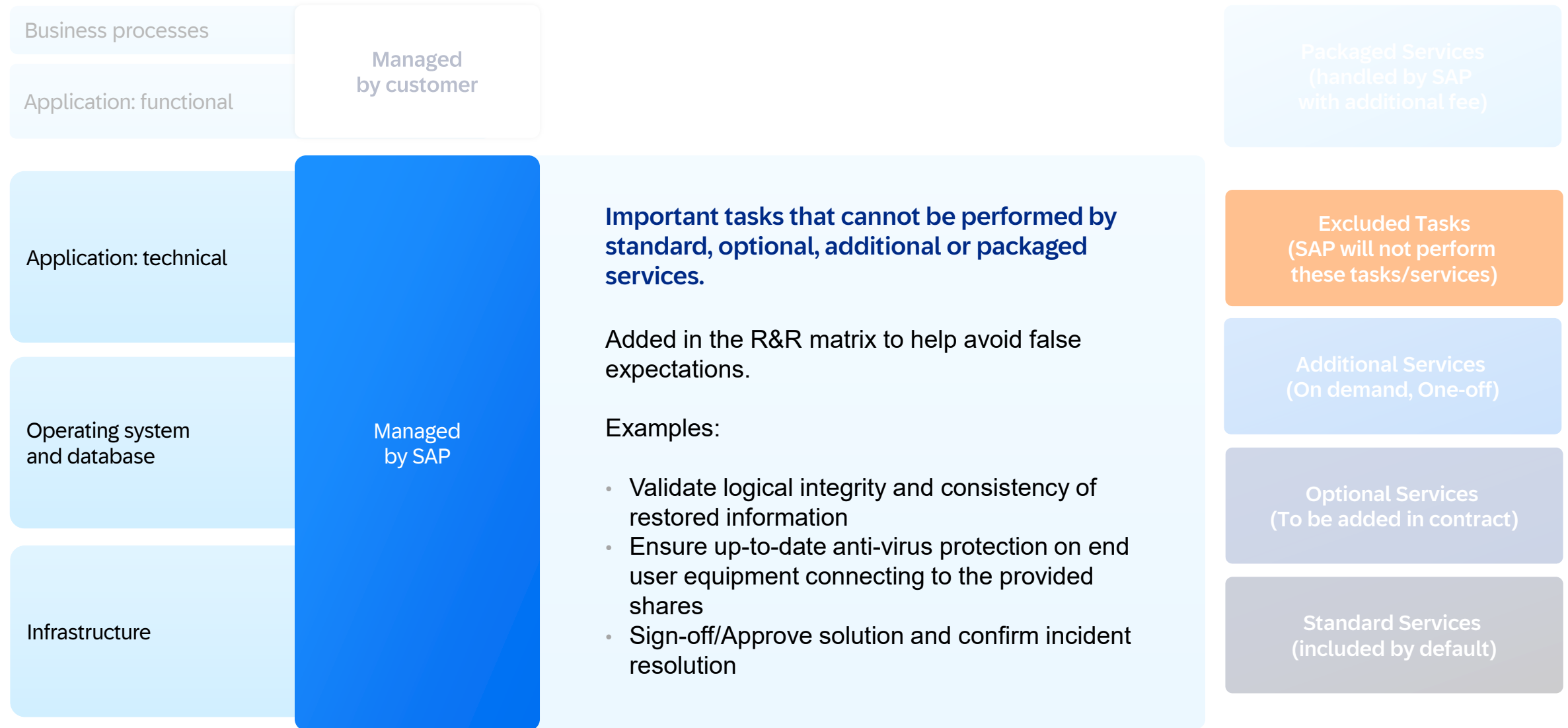
SAP Cloud ERP Private: Roles & Responsibilities

Additional Services, One-off Services/services subject to additional fee per delivery



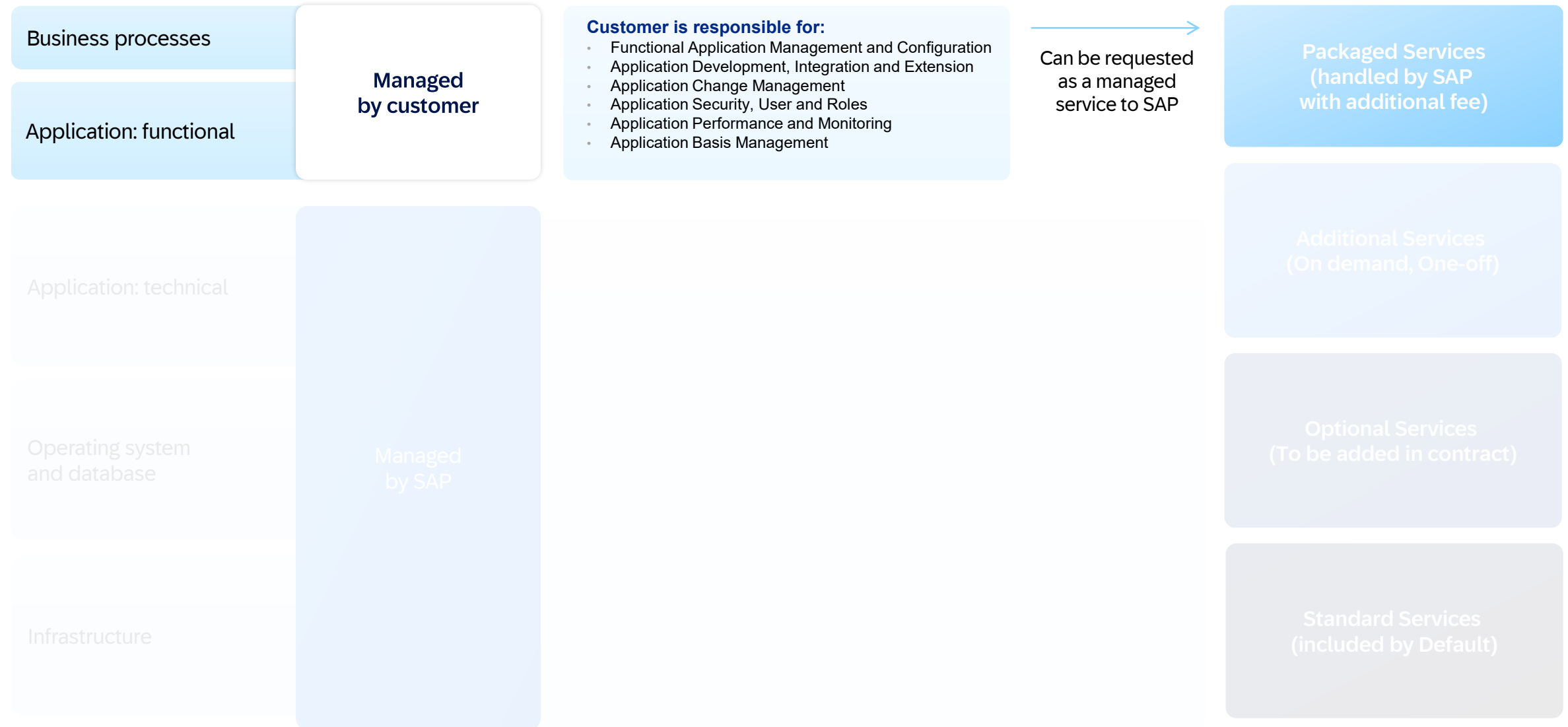
SAP Cloud ERP Private: Roles & Responsibilities

Additional Services, One-off Services/services subject to additional fee per delivery



SAP Cloud ERP Private: Roles & Responsibilities

Customer Responsibility, can be performed by customer or requested to SAP (with additional fee)



Excluded Tasks — your responsibility

Activities that remain outside the scope of SAP services

Managed by you or your partners — only when genuinely required and in scope

Examples from the R&R document and 'Operate' guide:

- End-user device management
- Antivirus protection at application level
- Approval and validation processes
- Application security notes (All, even HotNews/CVSS ≥ 9.0)
- User monitoring and threat detection at application level
- User and permission management (creation, change, lock, unlock)
- Role maintenance (creation, change) — except SAP initial admin role
- Configure security audit logging
- Testing and sign-off after SAP changes

All tasks not purchased or provided by SAP = customer responsibility

Your action checklist

1. Review the R&R document (v3-2026) with your SAP Cloud Architect Advisor
2. Read 'Operate your cloud ERP with confidence and control' guide
3. Delegate authentication to your own identity provider — do not rely on SAP default
4. Configure application security audit logging
5. Set up LOGSERV and integrate with your SIEM
6. Establish your own application penetration testing schedule
7. Review and clean up role-based access controls regularly
8. Address application security notes (CVSS < 9.0) promptly
9. Evaluate Packaged Services for areas where you need SAP expertise
10. Document your side of shared responsibility in security policies

Key references:

- R&R documents: sap.com/about/agreements/policies/hec-services.html
- SAP Trust Center: sap.com/about/trust-center/security.html
- SAP Community: community.sap.com/t5/technology-blog-posts-by-sap/securing-rise-with-sap/ba-p/13519419

Quote

RISE is shared — not outsourced
Know your R&R. Invest in application-level security.



Shared Responsibilities After Moving to SAP RISE

20TH OF OCTOBER 2026

Your perspective matters

Join the conversation

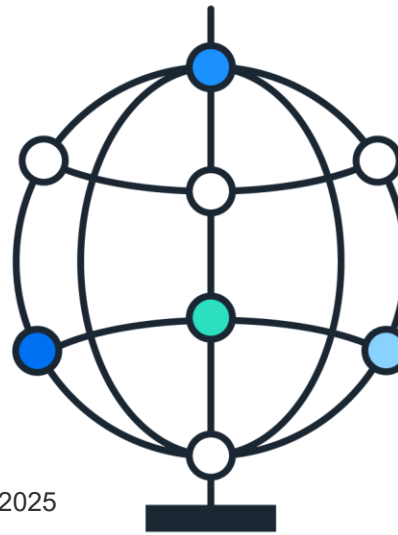
You ask. We answer.



RISE Above

Global momentum

- 8,500+ cumulative RISE customers (May 2025) — representing ~40% of global GDP
- 25,000+ S/4HANA Cloud customers across all editions
- Cloud ERP Suite revenue growing 30% year-over-year (Q1 2026)
- Current cloud backlog: €22.9B, up 26% at constant currencies (Q2 2026)



DACH and Nordics — close to home

- 48% of DACH companies using or planning RISE (was 16% in 2024) — DSAG 2025
- Resistance collapsed: only 23% say no to RISE (was 61%)

Migration urgency — the 2027 deadline

- Only 39% of ~35,000 ECC customers have started transition (Gartner, Q4 2024)
- 30% of organizations fully live on S/4HANA Cloud Private (was 19% in 2024)
- 73% at some stage of transition — but 27% have not started
- Legacy ECC/Business Suite usage fell below 50% for the first time

Industry breadth

- Energy
- Pharma
- Automotive
- Retail:
- Public sector
- and more



Thank you.

Bo BAADE-PEDERSEN
BDE CyberSecurity
Marmorvej 4
2100 Copenhagen
b.baade-pedersen@sap.com

