KPMG

Protect your SAP ERP landscape

Secure your data in a cyber threat environment with KPMG and SAP

kpmg.com/sap

What's inside

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients.
All rights reserved.

01

The importance of protecting your SAP landscape

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients.
All rights reserved.

The importance of protecting your SAP landscape

In the rapidly evolving digital landscape, cybersecurity stands as one of the most pressing challenges confronting organizations across all sectors. The frequency and complexity of cyber-attacks have surged dramatically, resulting in a significant increase in data breaches that compromise sensitive customer information and disrupt system availability. As such, the imperative for robust cybersecurity measures has never been more critical. Organizations must prioritize the development and implementation of comprehensive cybersecurity strategies to safeguard their assets and maintain trust with their customers.

Redefining security

The sophisticated landscape of cyber threats requiring enhanced security and governance surrounding enterprise systems has never been more pronounced. Traditionally, organizations have perceived their SAP landscapes merely as internal financial systems. This limited perspective fostered a belief that security was primarily about managing user access, resolving segregation of duties conflicts, and enforcing robust change control measures. However, this mindset is evolving.

ERP as a target

ERP systems are increasingly under siege from cyber-attacks, primarily due to the high-value data they house. Attackers are now focusing on critical systems and components, exploiting known vulnerabilities within the technical and infrastructure layers of ERP systems. Historically, security measures have prioritized regulatory compliance, often limited to controls over financial reporting and centered on roles and authorizations. Unfortunately, this narrow focus has left significant gaps in security.

Protecting your ERP landscape

With the escalating threat landscape, existing security and governance frameworks are often inadequate in safeguarding the interconnected SAP environment. Organizations must shift towards a comprehensive SAP security and governance strategy that encompasses the entire SAP technology stack. This shift necessitates a proactive approach to identifying cybersecurity threats and implementing a robust security and governance framework that can adapt to evolving risks. At KPMG, we recognize that the time has come for organizations to rethink their approach to cybersecurity. By adopting a holistic strategy, businesses can not only protect their valuable data but also ensure the integrity and availability of their critical systems in the face of ever-evolving cyber threats.

54%

of CEOs say they are ‘well prepared’ for a cyber-attack[1]

78%

of respondents overall say that their staff training treats cybersecurity as a box-ticking exercise, and it is not embedded as required[2]

$50,000

average cost per hour in case of ERP system unavailability[3]

200

average number of security notes (patches) released each year[3]

KPMG

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

02

SAP S/4HANA transition from a cybersecurity perspective

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients.
All rights reserved.

Cybersecurity considerations in the face of increased threats

Numerous companies are embarking on transformation projects to migrate to SAP S/4HANA. From a technical perspective, this raises a variety of questions, starting with the operating model (cloud vs. on-premise) and ending with integration into the existing system landscape. The implementation leads to a changed IT architecture, often combined with many new components and interfaces.

At the same time, the threat posed by cyber attackers is increasing. The new way of operating and the more connections that come with using cloud systems mean that there are more possible ways for SAP systems to be attacked. KPMG professionals recognize the critical importance of conducting regular assessments of SAP systems to ensure their security and resilience against these threats. It is essential to adopt a proactive stance in evaluating and fortifying the security measures in place, thereby safeguarding valuable data and maintaining the integrity of critical systems.

Increased need for action

At KPMG, we understand that many organizations have successfully operated without significant security concerns for the past two decades. However, with the evolving digital landscape, it is essential to recognize that "business as usual" may not be sufficient to address the increasing risks organizations face. The transformation to SAP S/4HANA presents a valuable opportunity to enhance security measures to align with contemporary requirements.

SAP S/4HANA inherently offers improved security features compared to older versions, benefiting from a security-by-default approach. This advancement provides a solid foundation for organizations looking to increase their security posture. Moreover, there are various strategies and steps that can be implemented to ensure long-term system security and readiness for future challenges. It is crucial to integrate security considerations from the outset and throughout all phases of the SAP S/4HANA development process and beyond. Given that SAP's security design is minimally intrusive, it is advisable for clients to assess whether the default security settings are suitable for their specific context or if there is a need for more stringent measures.

By taking a proactive approach to security, organizations can not only protect their valuable data but also enhance the overall integrity and resilience of their systems in an increasingly complex threat landscape. Organizations need to start by asking the basic question of why security is a relevant aspect of a SAP S/4HANA transformation. To answer this, they must recognize that IT systems are crucial for core business processes. This means that there are opportunities and entry points to access vital areas where sensitive data is kept. It also means there is a danger that an attack could cause the worst-case scenario, such as a halt in production.

KPMG

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Starting point for businesses and understanding the need

One of the reasons it is hard to develop cybersecurity skills in-house is the lack of qualified workers. Moreover, the threat landscape is vague and unclear, and creating a robust security concept is a complicated task and a rise in professionalism in cybercrime (such as ransomware-as-a-service), is making it more likely organizations will be attacked.

The first step to a secure business is a protection needs analysis of SAP S/4HANA, which establishes the fundamental security requirements and gives a view of the current situation. Once the basic architecture is determined, threat modeling can uncover possible attack paths and estimate related risks. Portals that have an internet connection or interface to external partners should be treated as gateways.

In this context, it is imperative to incorporate effective patch management and automated vulnerability scanning. These practices are fundamental to maintaining the integrity of the system, ensuring security updates are applied, and vulnerabilities are proactively identified and fixed.

Managing patches is a challenge, necessitating a systematic approach to assess and prioritize security notes. Careful planning is essential and conducting penetration tests before or after transitioning to new systems helps identify vulnerabilities. Integrating security requirements into project design and conducting threat modeling early on is another essential, while third-party testing verifies risks for connected systems, enhancing the overall security posture.

Cybersecurity as a holistic, continuous task

A SAP S/4HANA transition requires a strong conceptual foundation for cybersecurity. Organizations need to design their security measures according to their risk profile. However, this is not a one-time process. Security is a continuous task that must be established as a permanent process. To achieve this, adequate resources must be allocated, responsibilities must be assigned, and skills must be built.

For this purpose, all actions taken should be systematically documented during the transition. Logging is not only a key requirement for testing, but also for security and monitoring. Monitoring user activities for security-critical events is becoming increasingly important.

This way, a reliable base is gradually created which helps ensure long-term secure operations and a secure IT infrastructure.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Navigating a SAP S/4HANA transition

As organizations leverage the functional and technical advancements of SAP S/4HANA to enhance their digital transformation journeys, it is essential to recognize the accompanying changes and potential risks. By prioritizing security, businesses can effectively manage these risks and ensure a smooth transition:

New functionalities

New or mandatory application functionality may render some legacy application controls ineffective, while new controls have not been identified, configured or implemented.

Data migration

With new data tables and database structures, migrated data needs sufficient testing and validation, while the impact of data changes on custom program logic requires evaluation. With SAP S/4HANA, there is also a whole new security world with new security concepts. It's like an application beneath the application.

Real-time access

Real-time access to data opens the organization to unauthorized access to sensitive information. That access is available through multiple layers, such as reporting and analytics at the SAP S/4HANA database layer, advanced reporting at the application layer, and by a growing number of users across the organization.

Hardening

Multiple new interfaces may be insufficiently hardened. Between SAP's various interfaces, there are multiple touchpoints to the database through both public and private cloud environments. All that new exposure requires strong interface controls and monitoring.

Third-party access

Third-party security requires evaluation for a new system architecture. The new architecture is more complex, with more layers leveraging the public cloud and integrating with external solutions. Organizations need to consider which third-party security and controls they want to embrace.

Shared responsibilities

In the evolving landscape of SAP and its Hyperscalers/Providers, including SAP RISE, the delineation of responsibilities can often become blurred. Establishing clear lines of responsibility is essential to ensuring that each party comprehends their duties and commitments, thus reducing risk and fortifying the security framework.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

03

Key questions to determine your security posture

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients.
All rights reserved.

Ask yourself the right questions

Understanding the maturity level of your SAP landscape in terms of security is crucial for organizations aiming to fortify their defenses. By assessing aspects like access controls, vulnerability management, and incident response, organizations can pinpoint vulnerabilities and prioritize enhancements.

This knowledge allows for the optimization of resource allocation, focusing efforts where they can have the greatest impact. Understanding SAP security maturity fosters a culture of continuous improvement, enabling organizations to evolve their practices in line with emerging threats and regulatory requirements.

"The transition to SAP S/4HANA presents a significant opportunity for organizations to enhance their security posture. By taking a proactive approach and integrating security considerations from the outset, organizations can help ensure that their SAP systems are secure and resilient in the face of evolving threats."

Jan Stoelting
Partner and Global Cyber SAP Security Lead, KPMG in Germany

Asking the right questions is instrumental in this process and guides organizations to delve into key areas and uncover vulnerabilities. Questions about access controls can reveal discrepancies in user permissions, while inquiries about vulnerability management can shed light on patching practices and risk mitigation strategies. Monitoring capabilities can be assessed through questions about real-time visibility and anomaly detection, while incident response preparedness can be gauged by inquiring about response protocols and post-incident evaluation.

SAP security strategy
Have you adopted a SAP security strategy that covers all relevant aspects?

Responsibilities
Are responsibilities for the different aspects of SAP security defined?

Security standard
Which security standard do you use to harden SAP systems?

SAP security tools
Which SAP security tools do you use to monitor security?

Roles and authorizations
Is there a concept for the roles and authorizations of users and admins?

SAP landscape
How are the network layers, the operating systems, and databases secured?

Custom code
Have you considered custom code? Do you use SAST, DAST, and SAP-specific tools?

Security notes
How do you ensure the timely implementation of security notes?

Monitoring
How do you monitor suspicious activities? What use cases are implemented?

What are the key questions you need to consider?

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients.
All rights reserved.

04

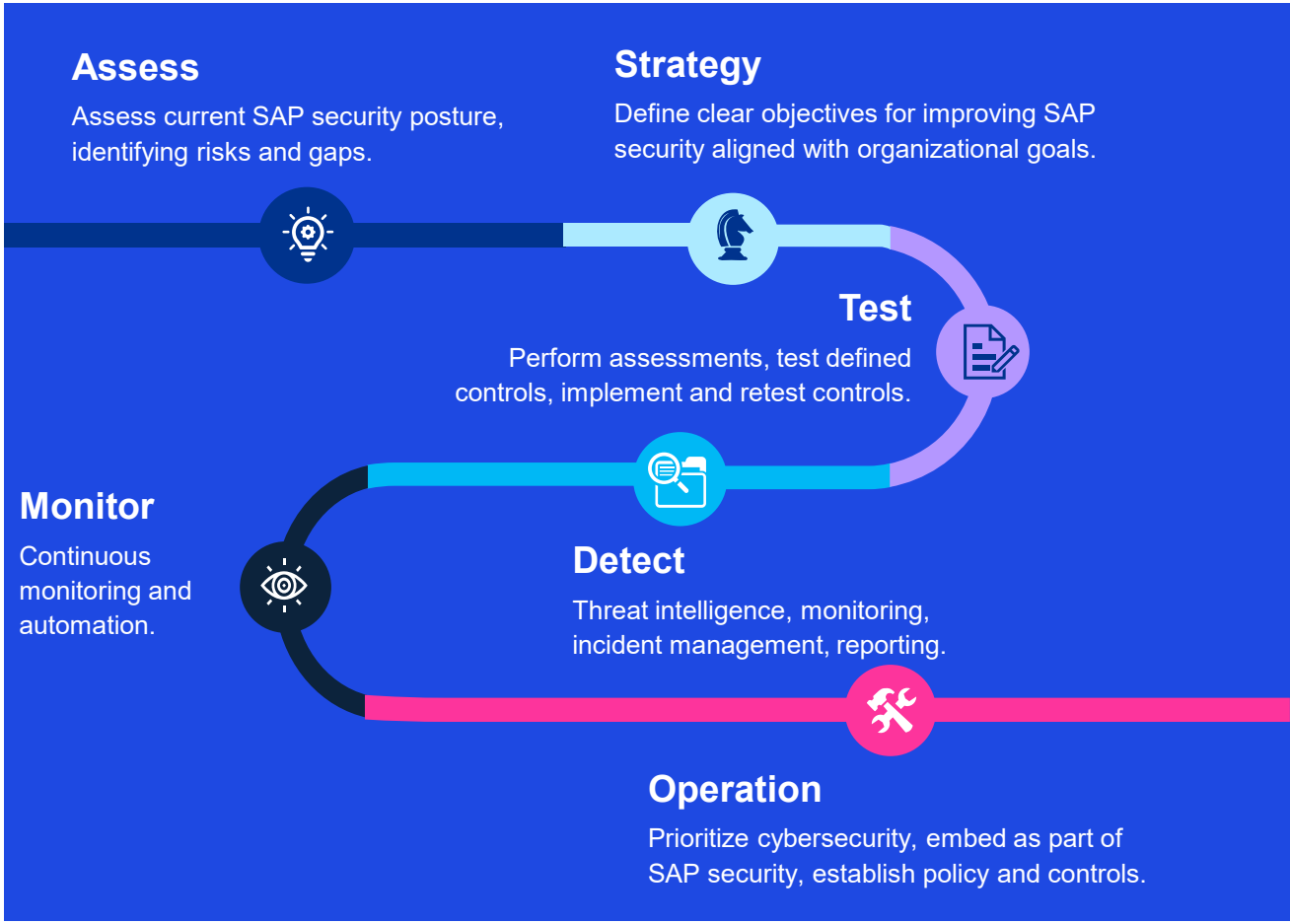
SAP security journey insights

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients.
All rights reserved.

Security is not a destination, it's a journey

KPMG SAP-certified consultants have the skills to help protect SAP systems from malicious attacks and vulnerabilities. But security can be challenging and complex, especially in a fast-paced and dynamic environment. Organizations should consider:

- How they can keep up with the latest threats and best practices
- How they can integrate security into development workflows without compromising your productivity and quality
- How they can measure and demonstrate security progress and achievements



"SAP has evolved from a system of records to a central decisioning engine for organizations. Ensuring the security of their SAP environment is vital. A cyber-attack could be immobilizing, leading to significant business disruption and substantial financial impact."

Akhilesh Tuteja
Partner and Global Cyber Security Lead, KPMG in India

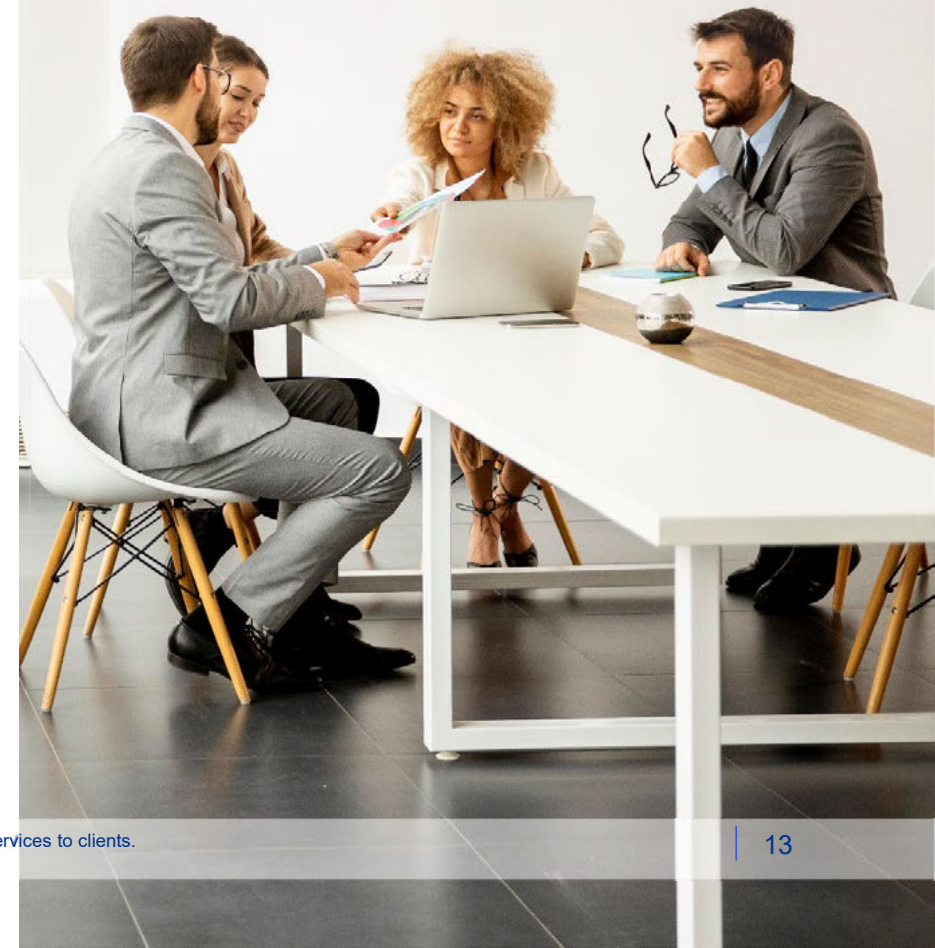
© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Exploring some benefits of SAP security

- Assess SAP systems security posture. Identify security gaps and vulnerabilities.
- Prevent and detect cyber threats and incidents for SAP with advanced analytics and automation.
- Respond and recover from cyber-attacks with incident management and remediation capabilities.
- Comply with regulatory and industry standards and best practices.
- Enhance trust, improve brand reputation and market competitiveness, and prevent fines.
- Be ready for SAP transformation, migration and overall digital transformation.
- Accelerate digital transformation and cloud adoption.

By leveraging security into your SAP landscape, you can safeguard critical assets, protect against evolving threats, maintain regulatory compliance, and foster a culture of trust and reliability.

The potential benefits of SAP security extend beyond just protecting data; this should contribute to the overall resilience, compliance, and success of an organization in an increasingly interconnected and data-driven world. Embrace SAP security to help protect your data.



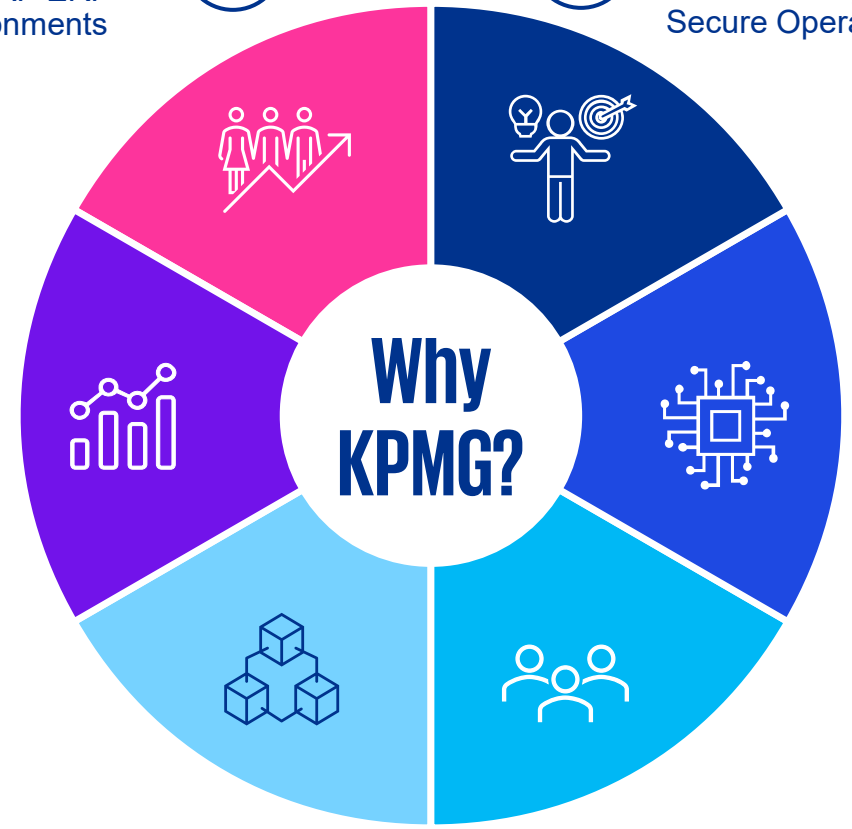
© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients.
All rights reserved.

05

How KPMG can help

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients.
All rights reserved.

Why KPMG?



1. A global network of professionals who can handle large projects, harvest collective insights and offer broad security advice on all topics on the SAP Secure Operations Map

2. KPMG SAP-certified tech and business-orientated consultants have expertise in design and project implementation of SAP solutions

3. Effective training and workshops, strategies and action plans to guide security governance and educate employees

4. Relationships built on trust and long-term commitment to providing effective and efficient solutions that help ensure SAP systems are safe and secure

5. Delivery of data-driven solutions for the design and administration of SAP authorizations, with post-implementation monitoring to proactively identify and mitigate security threats

6. Trusted adviser with extensive experience in providing SAP security advice that goes beyond SAP ERP into industry specific environments

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

A thorough approach in a complex environment

SAP strategically organizes the realm of security within its framework known as the 'SAP Secure Operations Map', which encompasses 16 key topics distributed across five levels.

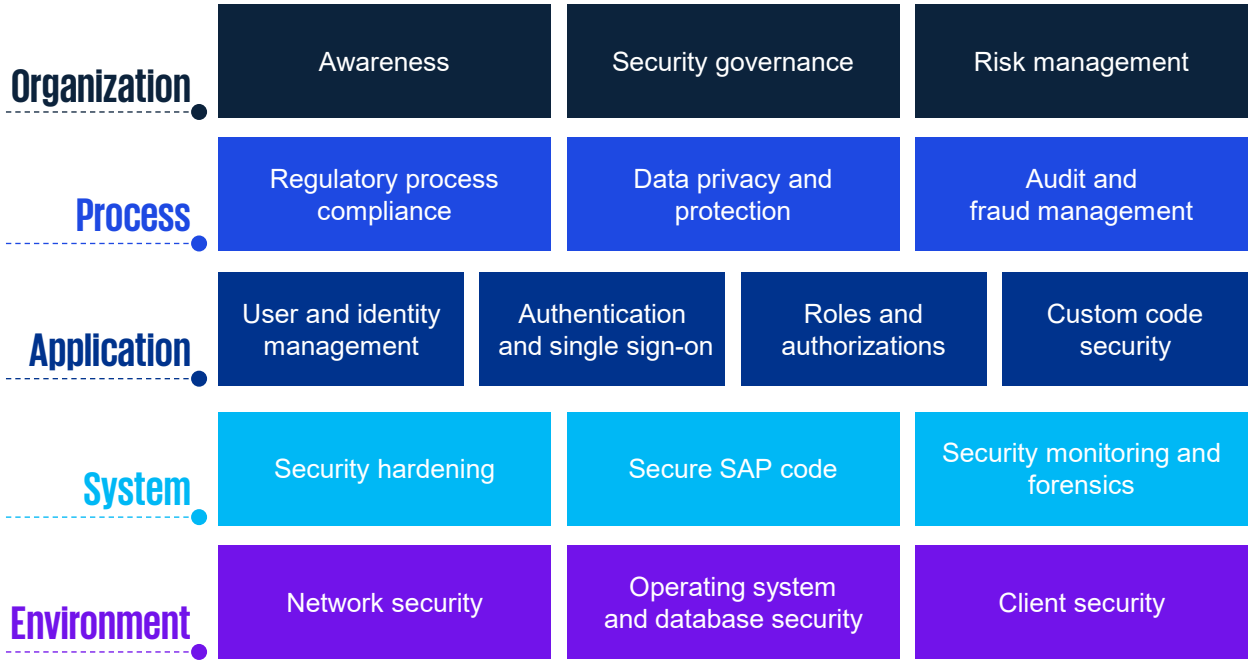
KPMG firms go beyond adherence to SAP's recommendations by supplementing them with enhanced practices and customized strategies. This involves a thorough examination of all operational facets, through a combination of KPMG best practices and experience in securing SAP systems in complex and changing environments. Frameworks like the KPMG Secure Operations Map and KPMG Trusted AI framework leveraged together display KPMG firms' deep industry knowledge and commitment to quality.

"A proactive SAP security approach enables organizations to identify risks early and take preventive actions to avoid any disruption to operations, compliance, or business continuity."

Alex Esteban
Director, Cyber and Technology Risk, KPMG in Spain

Through this meticulous process, KPMG professionals have a detailed and broad understanding of a client's security within the SAP ecosystem and can provide clients robust and tailored security solutions that can address their specific needs and concerns.

SAP Secure Operations Map



© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

The KPMG approach

KPMG professionals understand the critical importance of securing SAP environments to protect the integrity and confidentiality of data. Our proposal focuses on offering a wide range of specialized SAP security services to help your organization mitigate risk and strengthen its cyber defenses.

SAP security assessments

KPMG firms' SAP security assessment provides an in-depth technical and organizational review of your SAP landscape. Based on the SAP Secure Operations Map, this approach looks beyond the traditional lens of financial and regulatory compliance and provides a holistic view of security for the entire SAP technology stack.

SAP security governance

KPMG professionals can help in defining effective strategies and action plans based on your current SAP security maturity level and risk exposure. These strategies are informed by current procedures, metrics, and key performance indicators.

SAP security operation definition

Definition and roadmap of security measures and solutions within SAP systems to protect against threats and vulnerabilities, such as: Vulnerability management, patch management, threat management, code scanning, among others.

SAP security monitoring

KPMG firms' suite of SAP security monitoring services includes threat intelligence and managed services tailored specifically to SAP environments. KPMG professionals provide comprehensive solutions to identify and mitigate threats, continuously monitor suspicious activities, and efficiently manage security incidents within SAP systems.

SAP security incident management

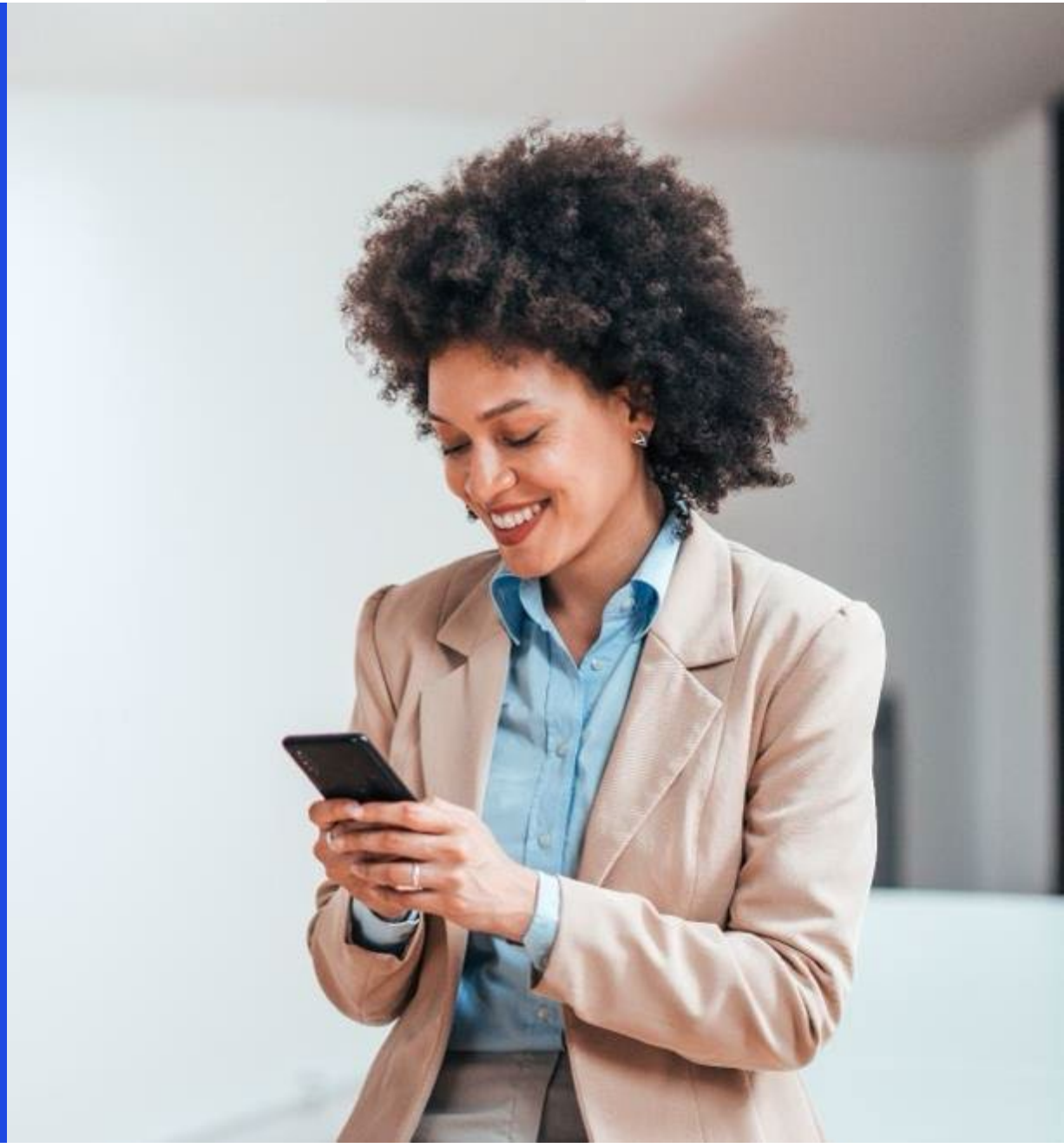
If your SAP systems have been compromised, KPMG firms have dedicated incident response teams that can assist in containing, recovering and performing forensic investigations.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients.
All rights reserved.

A team at your disposal

KPMG professionals leverage their deep understanding in SAP security to assist organizations in safeguarding their SAP infrastructure. Through our extensive global network of KPMG firms, we harness the collective insights of professionals to customize an approach that addresses the specific SAP cyber threats confronting your organization.

- **SAP PartnerEdge:** By combining KPMG firms' industry-focused approach with SAP market-leading technology, KPMG professionals aim to fast-track digital transformation journeys and help businesses become future-ready.
- **Global network:** KPMG firms operate in 143 countries and territories with more than 273,000 partners and employees working in member firms around the world.
- **Award-winning:** KPMG firms were named a worldwide Leader in Systems Integrators/Consultancies for Cybersecurity Consulting Services in 2024 by IDC MarketScape.
- **Committed to you:** KPMG firms' client relationships are built on mutual trust and long-term commitment to providing effective and efficient solutions.



© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

06

Case studies

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Case study

Comprehensive strengthening of SAP security via configuration validation, automated monitoring and standardized guidelines at a chemical company

Client challenges

- Heterogeneous landscape with unclear responsibilities
- No uniform view of SAP security
- Challenges in the areas of monitoring, secure SAP code, custom code security, dashboard, etc.
- Ongoing SAP S/4HANA transformation projects
- Ongoing global security initiative with effects and requirements for the operation of the SAP landscape

KPMG approach

- Assessment of current SAP security state for 24 SAP lines via workshops and data-driven checks with 200+ controls/baseline in accordance with SAP Secure Operations Map
- Governance and KPMG best practices for both classic/legacy and SAP S/4HANA systems
- Design of SAP security future state, including tool selection for SAP vulnerability management, ABAP code security scan, monitoring and compliance/baseline checks

Outcome

- Assessment of the maturity level of SAP security for on-prem and cloud systems
- Created a clear roadmap for improving the SAP security maturity level
- Provided SAP security support to the organization
- Support with tool selection for improved processes in the areas of security monitoring, patch management, code scanning and hardening of SAP systems

Client context

- A chemical company with 48 production facilities and 63 service and research laboratories worldwide, about 7,000 employees and a yearly revenue of €3bn.
- The customer operates a diverse landscape of SAP solutions across several subsidiaries, for which a uniform security standard is to be achieved. In addition to typical ERP systems, this also includes cloud applications.

Key figures

> 200
SAP specific security controls

24
Analyzed systems

6
SAP products in scope

11
KPMG professionals involved

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Case study

Conceptualization and implementation of IT security measures for the central SAP-based HR system of a state-owned IT service provider

Client challenges

- Extensive regulatory requirements on a state and federal level
- Extremely high security requirements and concerns from certain customers
- Wide variety of customers with different requirements towards accessing the solution
- Complex SAP landscape involving several third-party solutions

KPMG approach

- Inclusion of SAP specific security guidelines into general security policies based on BSI IT-Grundschutz
- Supporting the SAP basis team in the implementation of security best practices
- Developing a concept for the secure usage of SAP cloud products to extend the solutions offerings
- Supporting the selection of an SAP monitoring solution

Outcome

- Policies for cryptography, baseline hardening, authorization and monitoring with SAP specific components created
- Security best practices implemented in the SAP HCM system
- Proposed scenarios for monitoring SAP and non-SAP systems with a single solution
- Customers convinced of the security of the solution through multiple workshops and frequent communication

Client context

- Central IT provider for a German state. The client implements and operates IT projects for the state government and agencies.
- The project is intended to standardize and aggregate HR processes for most ministries and agencies of the state, creating a single HR solution.

Key figures

460,000
Individuals managed by the SAP HCM system

4
Years (project runtime)

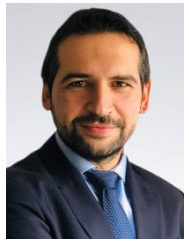
9
SAP systems in scope

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Contacts

Jan Stoelting
Partner and Global Cyber SAP Security Lead
KPMG in Germany
jstoelting@kpmg.com

Akhilesh Tuteja
Partner and Global Cyber Security Lead
KPMG in India
atuteja@kpmg.com



Alex Esteban
Director, Cyber and Technology Risk
KPMG in Spain
aesteban@kpmg.es

Endnotes:

1 KPMG 2024 Insurance CEO Outlook, KPMG International, October 2024
2 KPMG Global Tech Report 2024, KPMG International, September 2024
3 Ponemon Institute: 2024 Cost of a Data Breach Report

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/sap

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

KPMG refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity. KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. For more detail about our structure please visit kpmg.com/governance.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Throughout this document, "we", "KPMG", "us" and "our" refers to the KPMG global organization, to KPMG International Limited ("KPMG International"), and/or to one or more of the member firms of KPMG International, each of which is a separate legal entity.