KPMG

KPMG SAP cyber security

kpmg.com

SAP Cyber security—Overview

Focus areas

- Identify key systems and components of the SAP landscape
- Assess existing SAP landscape for advanced security threats
- Implement security for the entire SAP technology stack
- Monitor SAP landscapes, databases, operating systems, and networks for developing cyber threats

Secure the SAP® landscape from cyber attack

The threat of cyber attack is one of the greatest risks facing organizations today. The volume and sophistication of threats has increased exponentially leading to a wave of data breaches involving the theft of customer information and intellectual property.

Increased security and governance around enterprise systems is critical in the face of these sophisticated attacks. Until recently, an organization's SAP landscape was viewed as simply an internal financial system. This narrow focus led to the belief that security was simply a matter of controlling user access, eliminating segregation of duties conflicts and implementing strong change control. Those views are slowly beginning to change due to recent events.

SAP systems are increasingly becoming the target of cyber attackers due to the high value of data often stored within the system. Attackers are targeting business-critical SAP systems and components by exploiting known security vulnerabilities in the related technical and infrastructure layers of SAP. These critical aspects of security have not been a priority since regulatory compliance objectives are limited to controls over financial reporting.

Due to the increased threat of cyber attack, existing security and governance strategies are simply no longer adequate to protect the interconnected SAP landscape. Organizations must change their approach to securing the SAP landscape and adopt a holistic SAP security and governance strategy that protects the entire SAP technology stack. This requires the ability to proactively identify SAP cyber security threats and implement a security and governance strategy to address evolving risk.

KPMG

SAP Cyber security—Advanced threats

SAP cyber security advanced threats

SAP systems are not secure by default. As a result, SAP landscapes are inherently exposed to a host of internal and external risks that threaten the integrity of the SAP environment and its sensitive data.

Cyber attackers recognize this as well and are exploiting these vulnerabilities for their personal gain. Given the standard confirmation and existing security posture of organizations, the most common threats are focused on technology, infrastructure and communication layers of SAP.

Common SAP security threat vectors:

- Missing SAP security notes
- Users with default passwords
- Unsecured SAP gateway
- Unsecured SAP authentication
- Insecure RFC interfaces
- Unsecured SAP message service
- SAP network filtering
- SAP Web applications
- Insecure SAProuter©
- Access to administration services
- Unencrypted SAP communications

Focus areas

- A secure network alone cannot prevent cyber attackers from exploiting your SAP system
- SAP must be configured properly to reduce exposure to known security vulnerabilities
- Secure SAP critical functions to prevent unauthorized access
- Lock down SAP communication protocols

SAP Cyber security—KPMG framework

KPMG's SAP Cyber security framework

As an organization, you want to know whether you have an adequate approach to SAP cyber security. At KPMG LLP (KPMG), we view SAP security through the lens of four key dimensions: SAP governance, configuration management, critical functions and technology stack. Together, these dimensions provide a framework for securing the SAP landscape from cyber attack. This integrated approach to securing the SAP landscape is based on the principle of "defense in depth".

SAP Governance

— Governance strategy
— Master data protection
— Third party risk
— Risk and compliance
— SAP GRC

SAP Configuration management

— Transport management
— SAP patch and notes management
— Configuration management
— Code security and testing

SAP Technology stack

— SAP Networking security
— Database and OS security
— SAP Communication protocols
— Logging and monitoring

SAP Critical functions

— User administration
— Password configuration
— Emergency access
— Access to sensitive TCodes
— Table maintenance

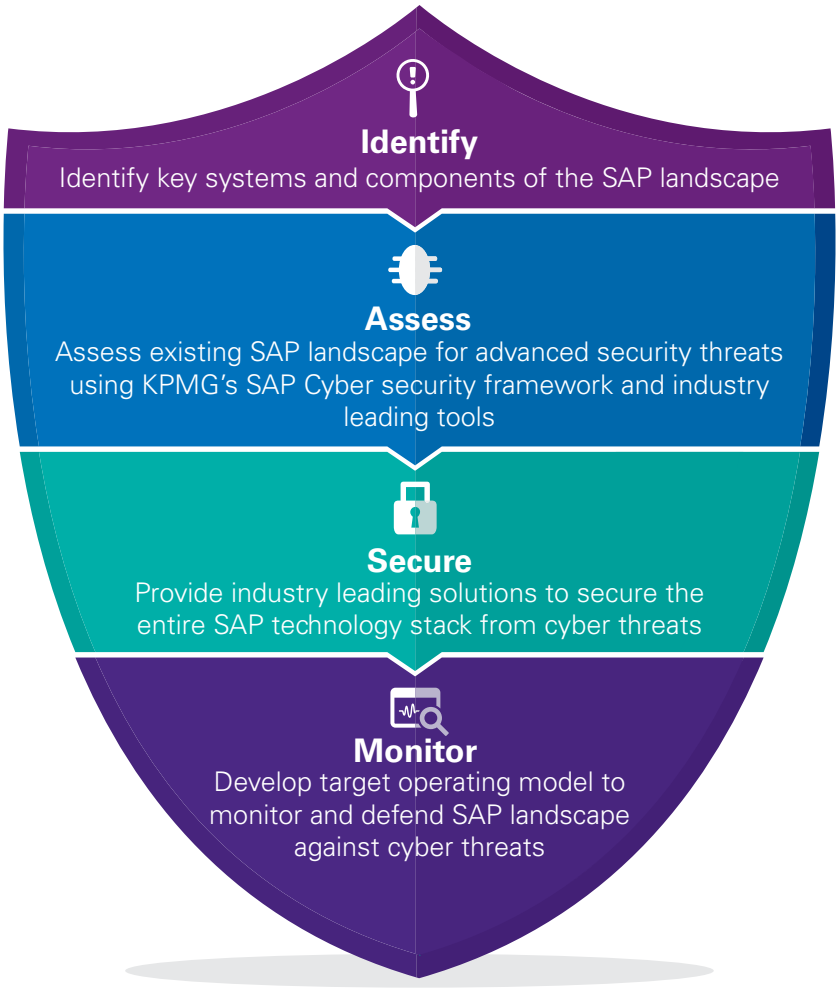
KPMG

SAP Cyber security—KPMG assessment

KPMG's SAP Cyber security assessment

KPMG's four-step SAP Cyber security assessment provides an in-depth review of the SAP landscape and the organization's ability to protect its most important information assets against cyber attack. We will leverage KPMG's SAP Cyber Security Framework to assess the SAP landscape for cyber security threats and develop tailored solutions to enhance the security and governance of your SAP systems.

Our SAP Cyber security assessment looks beyond the traditional lens of financial and regulatory compliance and provides a holistic view of security for the entire SAP technology stack.



SAP Cyber security—KPMG's approach

Identify

— Utilize KPMG's SAP Cyber security framework to identify focus areas for the assessment

— Discover and map components of the SAP landscape

— Information gathering of SAP and landscape properties

— Produce RFC Topology map

Assess

— Assess SAP landscape for threats against KPMG's SAP Cyber security framework

— Leverage industry leading tools to perform:

– Blackbox vulnerability assessment

– Whitebox security audit and compliance

– Penetration test

– Produce detailed security and vulnerability reports

Secure

— Analyze the results of the SAP Cyber security assessment and vulnerability reports

— Prioritize and rank identified risk

— Provide industry leading solutions to secure the SAP environment from cyber threats

Monitor

— Develop target operating model to monitor and defend SAP landscape against cyber threats

— Provide observations and recommendation to reduce the cyber threat risk

— Update existing regulatory and compliance frameworks to include the additional elements of SAP cyber security

KPMG

SAP Cyber security—Why KPMG

KPMG's SAP Governance, Risk and Compliance professionals combine deep SAP security and controls knowledge to help organizations protect their SAP environment. We draw upon professionals in our global network of member firms in 148 countries to tailor an approach relevant to your risk appetite and SAP cyber threats your organization faces.

KPMG member firms are:

- **Issues-led**—We are constantly enhancing our capabilities to meet heightened client demand for robust information protection and business resilience services.
- **Global**—Through the member firm network, KPMG firms employ over 155,000 professionals in 155 countries. We have deep experience wherever you operate.
- **Award-winning**—KPMG in the United Kingdom was awarded "Information Security Consultant of the Year" at both the 2011 and 2012 SC Magazine Europe Awards. In addition, KPMG's Information Security consulting services capability was named a "Leader" in the Forrester Research, Inc. report, "The Forrester Wave™: Information Security Consulting Services, Q1 2013". Of the 10 firms evaluated for this report, KPMG was specifically recognized for its drive to take on the toughest consultancy tasks, often taking over from other firms.
- **Shaping the cyber agenda**—Through I-4, KPMG's Cyber Security Services professionals help the world's leading organizations work together to solve some of today's and tomorrow's biggest security challenges.
- **Committed to you**—Relationships with member firm clients are built on mutual trust and long-term commitment to providing effective and efficient solutions. KPMG's practitioners are dedicated to providing a service that is second to none.

Contact us

Eric M. Bloesch
Partner, GRC Technology and
National Leader, SAP Risk Consulting Group
KPMG LLP
T: 267-256-8311
E: ebloesch@kpmg.com

Mick McGarry
Principal, GRC Technology
KPMG LLP
T: 214-840-8249
E: hmcgarry@kpmg.com

Engel H. Schmidt
Solution Relationship Director,
Risk Advisory Solutions
KPMG LLP
T: 713-319-2000
E: engelschmidt@kpmg.com

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

kpmg.com/socialmedia