



SAP S/4HANA security from the start

**Kick off implementation
with cyber security**



kpmg.com

Introduction

A company spends tens if not hundreds of millions of dollars and an average of 12 to 18 months planning, building and deploying an enterprise software system. It can take hackers just hours to find and exploit it.¹



SAP cyber security – a sizeable global concern

64% of business-critical systems (SAP or Oracle) have been breached in the last two years. *

At risk of attack:

92% of the Forbes Global 2000 corporations that use SAP; and

77% of transaction revenues globally that touch these systems. **

*IDC survey sponsored by Onapsis (October 2019)
 ** SAPcom, SAP Corporate Fact Sheet and Company Information

Today's cloud-based enterprise resource planning (ERP) systems offer unprecedented data analysis, automation, speed and efficiency for companies to better manage everything from finance to human capital. More than 16,400 companies have adopted SAP's next-generation ERP, S/4HANA, through the first quarter of 2021.² Thousands more are in the process of migrating to the new platform, including current SAP Business Suite 7 customers facing a deadline at the end of 2027, when SAP ends its mainstream maintenance support for core applications.³

For all of its many benefits, SAP S/4HANA comes with increased complexity, and implementation planned without dedication to security can significantly increase risk.

¹ Onapsis, "Threat Intelligence Report: Active Cyberattacks on Mission-Critical SAP Applications (April 6, 2021)
² SAP, Q1 Financial Results (April 22, 2021)
³ SAP, "SAP Extends Its Innovation Commitment for SAP S/4HANA, Provides Clarity and choice on SAP Business Suite 7 (February 4, 2020)



Inherent vulnerabilities in modern ERP systems

The world's corporations rely on software systems with weaknesses that have led to some of the most significant cyber security hacks in recent years.

In the last five years, many companies have moved from one large ERP platform to multiple vendors with a mix of cloud and on-premise deployments. In this hybrid application landscape, companies can pick and choose among best-of-breed offerings, building an enterprise technology platform that meets their specific needs. This new "modern ERP" approach brings with it additional complexities in securing the connected enterprise.

The U.S. Computer Emergency Readiness Team (US-CERT) of the U.S. Department of Homeland Security has issued five alerts to date about cyber attacks targeting mission-critical enterprise systems, including SAP. One of the more high-profile breaches, uncovered by Onapsis in 2016, gave unauthenticated remote attackers potentially complete control of SAP business application information and processes at 36 organizations worldwide.⁴ Prior to that in 2015, a China-sponsored hack of the SAP system at U.S. federal government contractor USIS exposed the personal data of more than 27,000 personnel, leading the organization to lose its contract and ultimately file for bankruptcy.⁵

Meanwhile, countless attacks against corporations continue every day without making the headlines. SAP and Onapsis worked together to conduct research and found more than 300 confirmed exploitations of unprotected SAP applications, including more than 107 hands-on attacks on organizations in less than a year. Among the compromised data included sales, HR, customer PII, engineering, intellectual property and financial information.⁶

Many corporate technology and IT security practitioners say much more needs to be done to protect organizations at the enterprise application level, according to a study by Ponemon Institute.⁷

- 57 percent can't quickly identify vulnerabilities
- 63 percent can't monitor and prevent attacks
- 79 percent do not build security features into their application development

Another 58 percent surveyed said it takes too long to patch applications that are in production. It's important to note that SAP's security patches for S/4HANA are "opt in." If the capability is not in place at the point of implementation, it can take up to 18 months to roll out a patch—that's a year and a half of exposure to a critical vulnerability even as organizations are trying to fix it.


Additionally, SAP and Onapsis determined it takes less than 72 hours after a patch release for hackers to attempt to exploit.⁸

As chief information security, technology and risk officers well know, any patch deployment let alone a new system implementation can open a window for bad actors to infiltrate a company's systems. With so many companies migrating to SAP S/4HANA, a lot of windows are open.

The high cost of a breach

Targeted organizations can experience data theft, financial fraud, business disruption, ransomware and more. The potential impact of an ERP-related cyber attack can be measured in several ways:

52% of security events leading to operational outages impacting productivity*



> \$50,000 per hour in average ERP application downtime costs**



\$5m average annual cost of business disruption and \$2m average annual cost in fines and penalties due to non-compliance***



8.6% average decrease in stock price within one year of a security breach****



* Fortinet, "The CIO and Cybersecurity" (2019)

** IDC survey sponsored by Onapsis (October 2019)

*** Ponemon Institute LLC, "The true cost of compliance with data protection regulations" (December 2017)

**** Comparitech, "How data breaches affect stock market share prices" (February 9, 2021)

⁴ U.S. Computer Emergency Readiness Team, US-CERT Alert (TA16-132A) (revised September 29, 2016)

⁵ CSO Online, "The OPM Hack Explained: Bad Security Practices Meet China's Captain America" (February 12, 2020)

⁶ Onapsis, "Threat Intelligence Report: Active Cyberattacks on Business-Critical SAP Applications" (April 6, 2021)

⁷ CPO Magazine, "Application Security Backsliding, Over 70% Say Their Portfolio Is More Vulnerable" (March 2, 2021)

⁸ Onapsis, "Threat Intelligence Report: Active Cyberattacks on Business-Critical SAP Applications" (April 6, 2021)

Security can't be an afterthought

Given the speed at which breaches can occur, companies must take action before launch to uncover and address security issues. The potential impacts are too great to ignore—downtime and project delays, increased compliance risk, and brand and reputational damage affecting relationships with customers, shareholders and regulators.

Organizations can't rely on Tier 1 systems integrators (SI) to cover their bases, either. Security simply isn't a primary focus of most SIs, and gaps can remain. The effort requires internal focus.

What follows are suggestions and guidelines for how technology and risk leaders can ensure that development, security and operations—DevSecOps—are integrated into every phase of a major system implementation for a modern ERP system that is safe and secure from minute one.

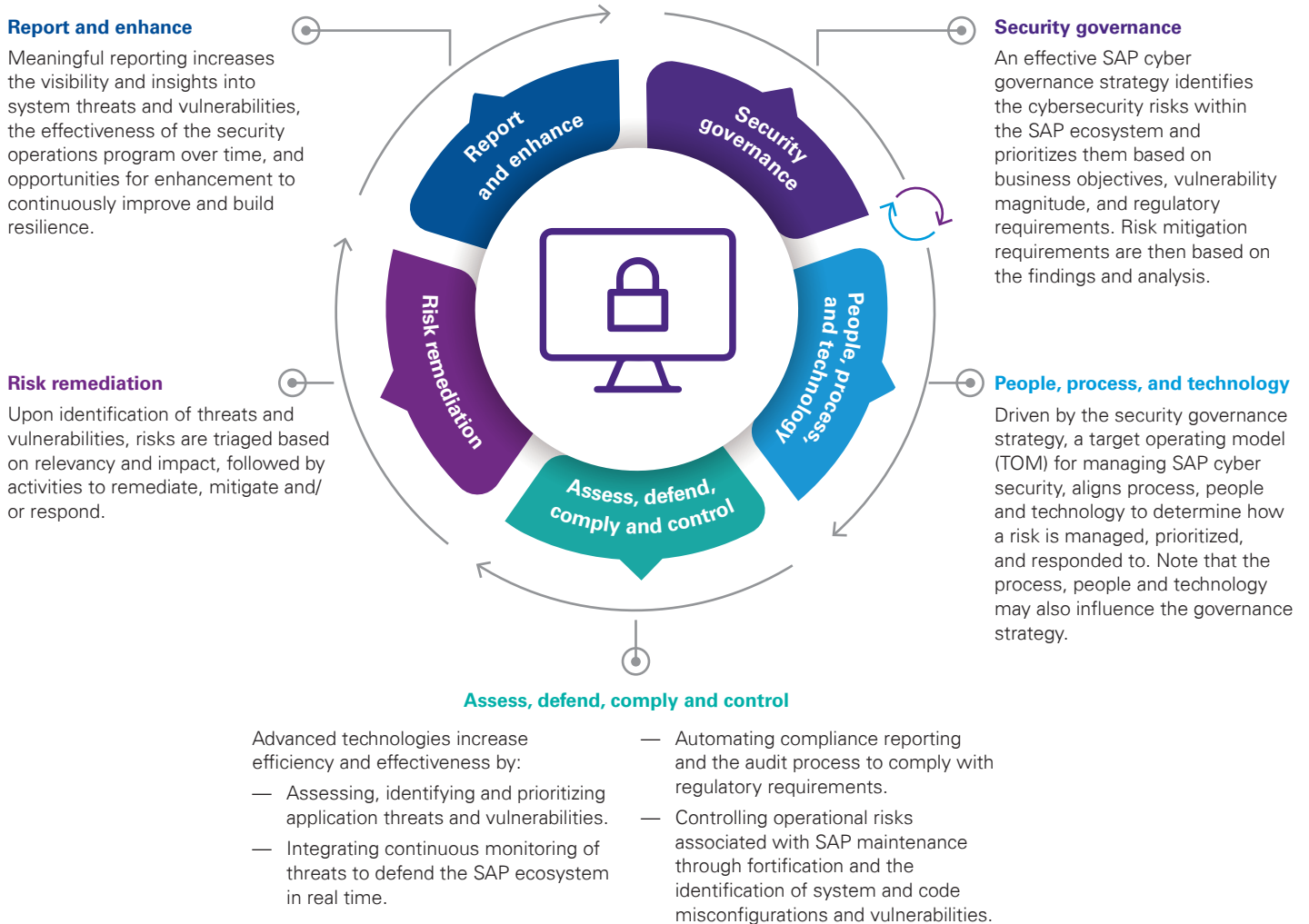


We could have waited to implement security after the migration, but it would have been too expensive. We were better off doing it as part of our 'build.' As a result of our investment, we were able to decrease the project timeline and significantly reduce our estimated budget. A project that as originally scoped to be completed in 2020 finished a year early."

Vice President of Global SAP at a multi-national advertising firm.





The target security operations model

Given the growing potential and high risk of ERP breaches, companies are searching for the most effective way to safeguard their assets across all businesses and functions as they transition to S/4HANA. A strong cyber security framework is a good start, including one that integrates leading practices and technologies that enable organizations to continuously detect and monitor their core business systems long past implementation.



Integrate cyber security into SAP S/4HANA implementation

With the target operating model serving as a guide, organizations can establish a more secure and efficient SAP system by incorporating security operations into every phase of the SAP S/4HANA software development lifecycle (SDLC). Here we discuss key activities companies should include in each phase.

SDLC Phases				
	Design Establish security requirements and responsibilities from the start to take a holistic approach to implementation and prevent security from falling through the cracks. 	Build Set rules for security and take advantage of tools that will help the organization adhere to the framework. 	Test Confirm business critical functions and security maintenance processes operate simultaneously without disruption. 	Deployment & Continuous Compliance Implement SAP S/4HANA security and leverage capabilities to monitor and adjust security operations based on regular feedback. 
TOM Elements	People Put together a project team with defined roles and broad SAP and security knowledge.	Provide additional training for team members on SAP security operations processes and integrate these processes into traditional build activities.	Supplement the project team with skillsets to provide penetration, vulnerability, and non-functional security testing.	Define and confirm roles and responsibilities that will continue after SAP implementation.
	Process Complement traditional SDLC process planning with a workstream specifically dedicated to defining security operations requirements and processes.	Stand up and deploy security capabilities during the build phase to support build efforts and production security processes.	Test the security operations processes, integrations and configurations to support effective deployment of your security architectures.	Monitor and address issues based on advanced security capabilities.
	Technology Establish security and compliance technology baselines and tooling requirements.	Select, configure and deploy security technology to support SAP security operations processes.	Build the security technology testing plan into your project timeline and deploy solutions timely in your S/4HANA implementation project.	Deploy and utilize technology to support your SAP security operations processes.

The implementation spectrum

Regardless of the transformation approach selected, organizations must build tenants of SAP cyber security program into their implementation project to better manage security risks in their future SAP S/4HANA system.

Start clean, stay clean

Implementations leveraging a greenfield approach have the opportunity to define requirements and expectations from the start. These projects should build their SAP security operations target operating model into their system development plan either as part of their security and controls workstream or as a standalone component. This will help ensure that requirements for SAP cyber security are captured and built out along with the other newly developed processes.

Get clean, stay clean

Those organizations adopting either a brownfield or bluefield approach must consider how to get their systems clean, and what needs to be done to keep them clean in the run state. Some organizations will have to challenge the mindset of "this is how we have always done it" in order to effectively deploy the change to people, process and technology required to secure their SAP systems from the evolving cyber security risks.

Case study: S/4HANA lessons learned from a CISO

“SAP was already a complex system—and now it’s becoming much more complex because it has so many more points of entry,” according to Glenn Haddox, the former Chief Information Security Officer at Southern California Edison (SCE) who helped the utility upgrade to SAP S/4HANA while improving its security. “The days of just using SOX protocols to protect SAP are over.”

Haddox shared his insights from SCE’s multi-year migration during a webcast hosted by Americas’ SAP User’ Group (ASUG) in April 2021.

To start, customization of SAP’s already complex code over the years has created a significant threat within many companies, Haddox said.

Organizations typically made software changes outside of the governance process, and often introduced numerous mistakes with implications that were difficult to uncover. On average, organizations have two million lines of unlocked code, according to Onapsis. Unfortunately, many CISOs had been lulled into the idea that the necessary security is already built into SAP.

Previously, “you couldn’t ‘look inside,’ but you didn’t need to, just guard around the perimeter, life is good,” Haddox said. “There wasn’t really a perception of the level of threats that we’re seeing now. It was all designed around the user.”

With SAP and multiple JAVA interface connections to the cloud and cyber threats on the rise, security patches can’t be applied to highly customized code, or applied quickly enough. Organizations need tools to uncover evidence of breaches and attempts that they would otherwise not see with traditional end-point security, as well as tools to provide verification and governance during code development, Haddox said.

“That’s why I think it’s so important if you’re going

through an upgrade to use these tools and integrate them in your controls, because the amount of damage [hackers] can do and how fast they can do it is unbelievable these days.”

The new SAP configurations require a substantial budget to implement and secure, and those costs need to be justified, Haddox said. Boards are increasingly focused on cyber security and seek reassurance, if not outright proof, that systems are secured for the investment made.

“Get a good test plan—not just of the functionality, but the internal works,” Haddox said. SCE used Onapsis tools, and the penetration-testing team verified the system was hardened and that they would be able to see activity inside the system should it be breached.

Organizations also should upskill their Basis teams, providing additional training for the system administrators and expanding their access and roles to better protect the new versions of SAP coming to market, Haddox added. He recalled the success of including the Basis team in the pen-testing process “so they got to see things that adversaries would do up close and in detail.

And I think it really enhanced their understanding.”

Of course, continue to work closely with the SOX team, he said. “Make sure you develop controls that truly deliver what you’re trying to achieve and don’t give you a false sense of security.”

“CISOs have so many things on their plate, and so many threats. But do not take it for granted that a large system like SAP is inherently protected.”

Listen to the entirety of Haddox’s comments in his interview with Onapsis Vice President of Business Application Cybersecurity, Jason Fruge, for the ASUG Express: Utilities Insights 2021 webcast, available to members at www.asug.com/events/asug-express-utilities-insights-2021.



Do not take it for granted that a large system like SAP is inherently protected.”

Glenn Haddox

Securing the SAP S/4HANA environment

KPMG and Onapsis work side by side with organizations throughout their migration to SAP S4/HANA to help achieve a more secure and efficient outcome.

KPMG helps clients to identify risks and implement leading practices and solutions to better secure their SAP landscape. This approach incorporates cyber security process design and technology adoption into your modern ERP project to enable a leading practice SAP security target operating model. Tools and benchmarks are leveraged implement proper SAP S4/HANA security controls based on a cyber security framework established by the National Institute of Standards and Technology (NIST).

Whatever your approach to SAP S/4HANA transformation—starting from scratch or migrating legacy, deploying on-premises or in the cloud—Onapsis can help. Vulnerability management, threat monitoring, application security testing, and compliance automation solutions help prepare legacy applications and code for migration and accelerate development of new HANA and Fiori apps. Using these tools from the start of your project can help ensure that applications and data are protected throughout the project and helps prevent project delays due to security, compliance, or quality issues.

Contact us

About KPMG

KPMG has advised companies how to design and implement effective application security for more than two decades, including helping them implement leading practice processes and tools to manage SAP security risks. Our dedicated SAP security and controls technology specialists bring together various skills to help security, basis, and risk management teams understand SAP application security risks, and how to implement processes and technology to address those risks. KPMG professionals are trained in SAP cyber security and have a wide range of industry, functional, and application security experience to assist companies with their unique needs. For more information, visit [read.kpmg.us/GRC](https://www.kpmg.us/GRC)

Mick McGarry
SAP Security & Controls
Solution Leader
KPMG LLP
hmcgarry@kpmg.com

About Onapsis

Onapsis has spent more than a decade focused on securing business-critical applications, including those running on SAP. In that time, our vulnerability management, threat monitoring, application security testing, and compliance automation solutions have helped hundreds of organizations protect their most critical systems and data, and, ultimately, keep their businesses functioning properly. With our tools and expertise, you can build security into your project from the start to ensure a successful transformation to SAP S/4HANA. For more information, visit www.onapsis.com

Darren Gaeta
VP, Worldwide Alliances
Onapsis
dgaeta@onapsis.com

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



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 upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2021 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

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

Designed by **EMA Design Team** | CRT136882 | July 2021