



SAP Security services

Cyber Security Advisory

KPMG Advisory Ltd.

Would you like to assess your SAP Security environment? We can also provide services in the respected areas.

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.

How can we help?

In the following brief summaries of our main SAP Security services you will see how KPMG's IT Risk Advisory Services practice tailors its services to the individual needs of your enterprise.

Role Design

A compelling authorization concept enables your colleagues to fulfil their duties effectively and timely, but in the same time, prevents fraudulent actions and adheres to common laws and regulations. We can provide an extensive review of current approach and the realization of it. Finally, we make suggestions for the actions to be taken in order to remedy deficiencies and ensure compliance. If you require, our project team is also able to deliver end-to-end solutions.

Segregation of Duties

We identify issues arising from complex access right structures and settings, particularly the inappropriate segregation of duties, conflicting roles which enable fraudulent activities. Modern ERP systems often cannot be analysed via simple methods, due to their complex nature. Therefore, we utilise various data analysis tools in our assessment. We possess outstanding expertise and tools for reviewing SAP access rights and SoD. If you do not have a Segregation of Duties Matrix yet, we can also assist you to create one.

Emergency Access Management

Whether you use the capabilities of the Emergency Access Management (EAM) module in SAP GRC system or established an alternative process, we can assess the effectiveness of your procedure. It is essential to have a compliant Emergency Access Management which enables users to promptly solve critical issues without causing incidents due to the extension of their regular accesses. We can also help you to implement a solution if you currently lack a satisfying one.

Security Audit Log

To keep a system secure, it's essential to have auditing and logging capabilities enabled. The SAP Security Audit Log (SAL) provides a framework to record security-related events in the system. As part of our assessment we review the settings and, if necessary, we propose implementation of appropriate security measures, including additional monitoring possibilities within the system. We can also assist you to integrate these functions into a Security Information and Event Management (SIEM) software solution by providing use cases tailored to your organization.

ABAP Development Standards

We review your existing documents which provide guidelines for ABAP Development and specifies programming standards. During the assessment, we verify that the organization's development policy ensures that security requirements are planned and implemented in the development lifecycle.

Patch Management

To ensure that both security vulnerabilities and program errors are fixed, SAP applications require occasional patching. Failing to keep up with patches increases the risk of unexpected system downtime and performance degradation. We can support you

to create a comprehensive, dependable and cost-effective patch management process.

Profile Parameters

One of the first steps to secure a SAP NetWeaver system is the setting of profile parameters. The profile parameters control many aspects of the system's behaviour and operation. We can review those settings and recommend solutions to possible problems.

Network and Transport Layer Security

Interfaces between systems have serious inherent risk. The data can be lost, altered or even duplicated; such incidents can significantly affect the operation of systems or even the general ledger data of the company. With the help of our audit techniques we can reveal functional errors and the security issues of interfaces and make suggestions for improvements. For example, we can help you to implement Unified Connectivity (UCON) to monitor your Remote-Enabled Function Modules.

User Management and Authentication

Different type of users can be created and authorized within an SAP system. We can verify your existing structure and related processes (e.g. Joiner-Mover-Leaver, User Access Review), review the utilization of User Groups and assess the settings of password and logon security. We also have extensive experience with Central User Administration tool and can support you in the implementation or operation activities of such a solution.

SAP Health Check

If you would like to get a comprehensive picture of the readiness of your system(s) or you are undecided which of our SAP Security services would bring the most value for your organization, please contact us so we are able to help you. We created a SAP Health Check package to offer a quick review of the above areas and support the decision-making process.

What advantages do we bring?

- Our colleagues vastly experienced professionals and they also have SAP S/4 HANA capabilities.
- With our help you can form a clear and true picture of the value-creating potential, weaknesses and future challenges related to your organisation's SAP landscape.
- Our services prepare your enterprise for the early recognition and standard-compliant management of risks which arise during its business operations.
- You can reduce the possibility of financial and reputational damages resulting from unintended or intentional mistakes or from malicious external attacks.
- Our services will help the SAP security process alignment to industrial best practices which will significantly decrease the cost of operation and maintenance in the future.

If you feel these issues are relevant to your business, please contact us for further details.

Contact



Kornél Lukács
Partner

T: +36 1 887 7472

E: kornel.lukacs@kpmg.hu

[kpmg.hu](https://www.kpmg.hu)

[kpmg.com/socialmedia](https://www.kpmg.com/socialmedia)



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

© 2022 KPMG Advisory Ltd., a Hungarian limited liability company 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.