KPMG

Assisting you in your transition to SAP S/4 HANA

Attend our exclusive Security and Controls client workshop
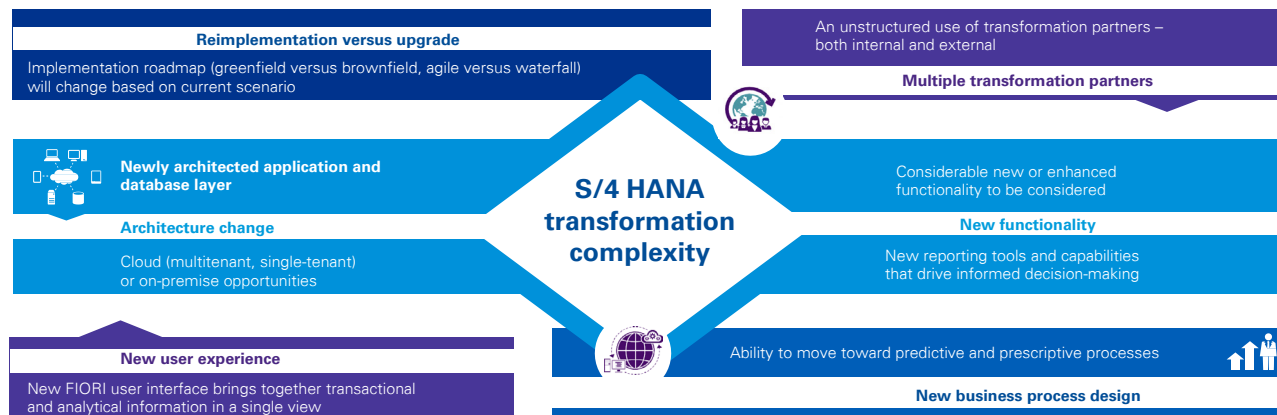
Helping you plan early

SAP's next-generation enterprise resource planning (ERP) platform is a key component of digital transformation. However, for many companies, these types of complex transformations and areas of security and controls are very often overlooked by system integrators. Inadequate planning and lack of attention can lead to devastating consequences, including:

— **Fraud:** Front, middle, and back office applications are priority targets for fraudsters and rogue employees

— **Cyber events:** cyber criminals have increased their attacks on front, middle, and backoffice platforms Denial-of-Service attacks, ransomware, data theft)

— **Significant audit deficiencies:** Auditors are getting involved early in the implementation process and raising deficiencies during implementation, cutover, and post go-live.
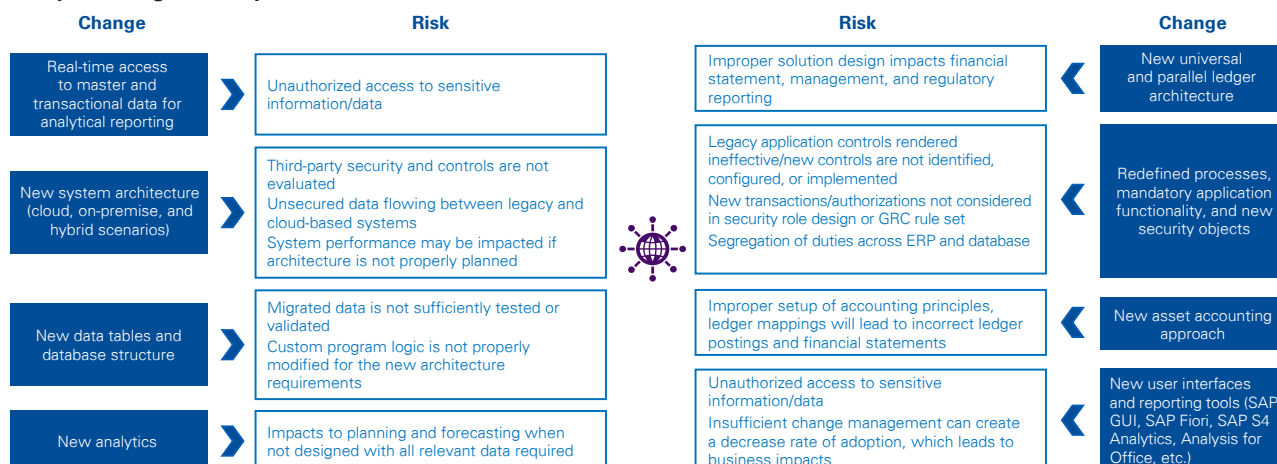
Is your organization protected against these potential threats as it transitions to SAP S/4 HANA?

At KPMG, we understand these challenges. We have seen first-hand that early planning can help mitigate these types of threats before they strike. We invite you to attend an exclusive SAP Security and Controls workshop, where you and your colleagues will have the chance to assess your organization's position during the transition to SAP S/4 HANA, uncover potential weak points, and manage the transition effectively to ensure success, manage the complexities that come with the transformation, and thwart and potential threats.

A world of complexity

Reimplementation versus upgrade
Implementation roadmap (greenfield versus brownfield, agile versus waterfall) will change based on current scenario

An unstructured use of transformation partners – both internal and external
Multiple transformation partners

Newly architected application and database layer
Architecture change
Cloud (multitenant, single-tenant) or on-premise opportunities

S/4 HANA transformation complexity

Considerable new or enhanced functionality to be considered
New functionality
New reporting tools and capabilities that drive informed decision-making

New user experience
New FIORI user interface brings together transactional and analytical information in a single view

Ability to move toward predictive and prescriptive processes
New business process design

Complex changes invite potential risks

Change	Risk	Risk	Change
Real-time access to master and transactional data for analytical reporting	Unauthorized access to sensitive information/data	Improper solution design impacts financial statement, management, and regulatory reporting	New universal and parallel ledger architecture
New system architecture (cloud, on-premise, and hybrid scenarios)	Third-party security and controls are not evaluated Unsecured data flowing between legacy and cloud-based systems System performance may be impacted if architecture is not properly planned	Legacy application controls rendered ineffective/new controls are not identified, configured, or implemented New transactions/authorizations not considered in security role design or GRC rule set Segregation of duties across ERP and database	Redefined processes, mandatory application functionality, and new security objects
New data tables and database structure	Migrated data is not sufficiently tested or validated Custom program logic is not properly modified for the new architecture requirements	Improper setup of accounting principles, ledger mappings will lead to incorrect ledger postings and financial statements	New asset accounting approach
New analytics	Impacts to planning and forecasting when not designed with all relevant data required	Unauthorized access to sensitive information/data Insufficient change management can create a decrease rate of adoption, which leads to business impacts	New user interfaces and reporting tools (SAP GUI, SAP Fiori, SAP S4 Analytics, Analysis for Office, etc.)

The KPMG difference

At KPMG, we understand these challenges. Our approach delivers a holistic SAP security, controls, and governance strategy that protects the entire SAP environment. Let KPMG professionals show you how to make the most of your SAP capabilities, while helping to ensure the appropriate risk and security controls are in place.

SAP Security and Controls Workshop agenda

Workshop Kickoff

— Introductions and Workshop Objectives
— Key Concepts for SAP Risk Management
— Security and Controls Target Operating Model
— Current SAP Risk and Compliance Concerns

SAP Security and Controls Deep Dive

Application Controls
— Business Process Controls
— Application Controls
— Information Technology (IT) General Controls
— Orchestrated Manual Controls
— Access Controls
— Interface and Conversion Controls
— Controls Testing
— Controls Analytics

Application Security
— Application Roles (RBAC)
— User Lifecycle Management
— Segregation of Duties
— SAP Fiori
— Attribute-based Access Control

Cyber and Data Security
— SAP Governance
— SAP Configuration Management
— SAP Critical Functions
— SAP Technology Stack
— Data Privacy

GRC Technology Enablement
— Access Governance
— Enterprise Risk and Compliance
— Cybersecurity and Data Protection
— Risk Analytics
— Continuous Controls Monitoring

Audience

— Finance/Controllership
— Human Resources
— Supply Chain
— Risk Management
— Sarbanes-Oxley Teams
— IT Compliance
— Application Security
— IT Infrastructure Team
— Internal Audit
— Cyber Security
— Data Privacy Teams

— Customized for your audience

— 1–4 hour workshop depending on the detail needed

— We focus on topics not covered by many system integrators

— Information was developed through experience supporting multiple SI delivered S4 projects.

What SAP solutions for GRC and security is your company using to support the enterprise control environment after the project?

Access governance

SAP Access Control	SAP Access Violation Management by Greenlight
SAP Cloud Identity Access Governance	SAP Dynamic Authorization Management by NextLabs
SAP Identity Management	Fastpath Assure
SAP Cloud Platform Identity Provisioning Service	ERP Maestro
SAP Single Sign-On	Saviynt
SAP Cloud Platform Identity Authentication Service	

Enterprise risk and compliance

SAP Process Control	SAP Business Integrity Screening
SAP Risk Management	SAP Regulation Management by Greenlight
SAP Audit Management	Celonis Process Mining

Cybersecurity and data protection

SAP Enterprise Threat Detection	SAP Code Vulnerability Analyzer
SAP Privacy Governance	SAP Enterprise Digital Rights Management by NextLabs
SAP Data Custodian	SAP Fortify by Micro Focus
UI Masking for SAP	SAP Privacy Management by BigID
UI Logging for SAP	Onapsis

| — SAP Product | — SAP Solution Extension (SolEx) | — Alternative Vendor Product |

Our SAP Security and Controls framework is a cross-application view of on-premise and cloud application security and controls. It is positioned to help industry-leading organizations effectively balance the divergent tasks of leveraging modern applications to empower business users while simultaneously protecting sensitive data and transactions.

KPMG SAP Security and Controls

GRC Technology Enablement
— Access Governance
— Enterprise Risk and Compliance
— Cybersecurity and Data Protection
— Risk Analytics
— Continuous Controls Monitoring

Application Security
— Application Roles (RBAC)
— User Lifecycle Management
— Segregation of Duties
— SAP Fiori
— Attribute-based Access Control

Controls Integration
— Business Process Controls
— Application Controls
— IT General Controls
— Orchestrated Manual Controls
— Access Controls
— Interface and ConversionControls
— Controls Testing
— Controls Analytics

Cyber and Data Security
— SAP Governance
— SAP Configuration Management
— SAP Critical Functions
— SAP Technology Stack
— Data Privacy

SC Target Operating Model
— Strategy Workshops
— Security and Controls Target Operating Model

To learn more about our SAP security and controls workshop, please 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