KPMG in power and utilities—energizing risk and compliance on your SAP journey

Power and utilities companies are going through continuous technology adoption and business transformation to meet the growing expectations of customers, to address regulatory requirements, and to manage ongoing interruptions to their business.

SAP S/4HANA and its industry solution for utilities (IS-U) is a key component of digital transformation in offering increased efficiencies, simplified processes, and the ability to respond to the ever-growing digital needs of their customer base. But this also requires equally transformative risk, security, and compliance strategies. KPMG has the industry-experienced professionals, an established and market-leading portfolio of methodologies, and tools and accelerators to successfully guide you through this journey.

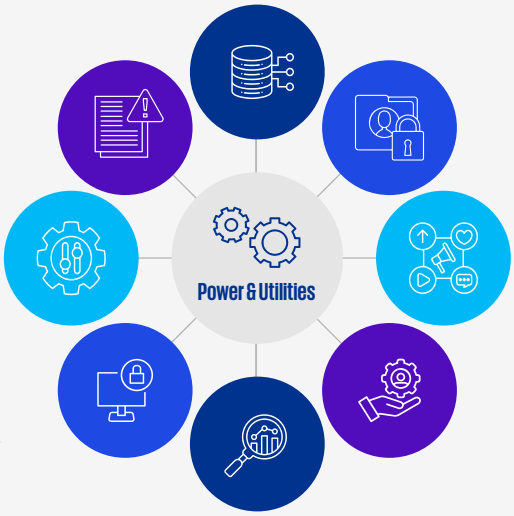
Considering risks in power and utilities and impact with SAP

We have a deep-rooted stake in power and utilities, which affords us the opportunity to have a holistic view of risks that are unique to this industry versus risks inherent in SAP solutions. SAP S/4HANA, IS-U, and associated technologies across front- and back-office operations deliver new functional and technical innovations both on-premise and in the cloud. Power and utilities companies must assess these impacts' current regulatory requirements, guidelines, and leading practices.

Key challenges and risks to consider

Data governance—master data management that enforces data integrity, separation, availability, and responsibility

Regulatory—controls framework covers regulatory risks and objectives



Data privacy (GDPR, CCPA, etc.)—understanding customer data, where it is stored, and requirements for its use

Internal controls—proper balance of controls to manage risk

Digital and social media—digital and social media customer relationship management must be governed by a framework balancing control, accountability, and permission

Cybersecurity—detecting vulnerabilities in complex system landscapes, establishing strategies to monitor threats and vulnerabilities post-go-live

Resource capacity—bandwidth issues may delay addressing key risk areas, individuals may not possess the required skill sets to meet the demands of the industry

Data analytics—lack of proper collection and categorization of data, research data analysis capabilities are limited, inability to prioritize key data, poor quality and inaccessible data

Risks in SAP S/4HANA

01 **New transaction codes and Fiori apps**—new transaction/authorizations not considered in security role design or governance, risk, and compliance (GRC) ruleset, thus adversely impacting business processing and increasing the likelihood of Segregation of Duties (SOD) conflicts

02 **New or replacement functionality**—new controls not identified, configured, or implemented; legacy application controls rendered ineffective

03 **New system architecture** (cloud or hybrid scenarios)—third-party security and controls not considered or evaluated; unsecured data between legacy and cloud systems

04 **New data tables and database structures**—migrated data is not sufficiently tested or validated; custom program logic is not properly modified for new architecture requirements

05 **Real-time access to master and transactional data with new entry points**—unauthorized access to sensitive information/data

06 **Existing legacy system data must be accurately migrated into HANA** insufficient testing/validation of critical financial, procurement, logistics, manufacturing, etc., data; inadequate documentation of data enrichment, testing/validation, and reconciliation activities

07 **New user interfaces and reporting tools (i.e., SAP GUI, Fiori, Analytic Cloud, etc.)**—unauthorized access, insufficient change management leading to decreased adoption rate of new application

Established methodology

Our established approach to security, controls, and GRC integration allows our multi-faceted team to address risk and control considerations as embedded workstreams within the overall implementation program.

This is an outcome-driven, business transformation solution that combines deep industry knowledge, global delivery capability, and cloud technology that is built on years of KPMG leading practice knowledge of business processes, operating models, delivery methodologies, and industry experience. The industry-specific risk and compliance solution comes with prebuilt GRC reference model, industry ruleset, accelerators (i.e., risk and controls matrix, templates), security roles, and position mappings. This enables KPMG to accelerate compliance requirements through each project phase, lowering risk and improving adoption.

Vision

- Evaluate financial, regulatory, and compliance risks associated with processes
- Identify security, controls, and GRC requirements required to enhance the SAP S/4HANA, IS-U, and associated technologies

Validate

- Integrate security, control, and GRC requirements into functional design and SAP configuration
- Develop a compliant, leading practice, security model free from inherent SOD violations
- Address security and control requirements in test plan

Construct

- Develop security and controls test scripts to support the effectiveness of identified control points
- Execute SOD analysis on configured security model
- Resolve defects and revise controls as required

Deploy

- Support training of control owners and GRC users
- Validate effectiveness of data conversion controls
- Provide governance over security, control, and GRC environment during cutover and hypercare

Evolve

- Post-go-live support and stabilization
- Establish continuous improvement track and monitoring for security, control, and GRC environment
- Manage project close and transition

Sample outcomes

	People	Process	Technology
Controls	• Clearly defined control ownership to drive accountability • Continuous collaboration with audit teams and business stakeholders • Smooth controls transition	• Controls aligned with Sarbanes-Oxley (SOX), utilities-specific regulatory requirements, cyber and information technology guidelines • Controls design supports business processes, financial reporting, and critical transactions • Reduction of manual, detective procedures	• System configuration aligned with key controls • Accuracy and completeness of interfaces and data conversions • Increased reliance on preventative automated controls
Security	• User access rights aligned with job responsibilities • Security role definition to facilitate change management/end-user training • Efficient provisioning of end-user groups	• Business processes, financial reporting, and critical transactions govern security design • Security design that follows leading practices	• Active monitoring of user access and SOD violations • Security design to support application infrastructure and enable the business to execute processes
Compliance	• Organizational awareness of corporate and regulatory policies • Corporate governance and oversight • Roles and responsibilities supporting compliance	• Defined risk and control management processes • Pragmatic approach to compliance • Adherence to industry-specific regulatory requirements	• Real-time GRC management and monitoring • Technology-enabled compliance program • Centralized view of security and control risks

Service offerings

- Controls integration/ optimization
- Application security
- Cyber and data security
- GRC technology
- ERP assurance (SOX, internal audit)
- Data analytics/ process mining
- Managed services

Contact us

Mick McGarry
US Leader, SAP Security and Controls
T: 214-578-2225
E: hmcgarry@kpmg.com

Jim Hoover
Managing Director, SAP Security and Controls
T: 614 314 4695
E: jhoover@kpmg.com

Jonathan Levitt
Managing Director, SAP Security and Controls
T: 949 382 5554
E: jclevitt@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