KPMG

How intelligent is your SAP control environment?

Ways in which optimized controls and sustainable processes and GRC technology adoption can drive business value

kpmg.com

The increasing dependence on SAP technology for core business processes renders information confidentiality, integrity, and availability essential, and highlights the need for an effective governance, risk, and compliance (GRC) program. Organizations are striving to reap more benefits from their sizeable investments in SAP technology, while at the same time operating in an internal control environment that manages transactional risk and complies with regulatory requirements. By introducing optimized controls and sustainable processes while integrating GRC technology, organizations can achieve this balance and become top performers in their field.

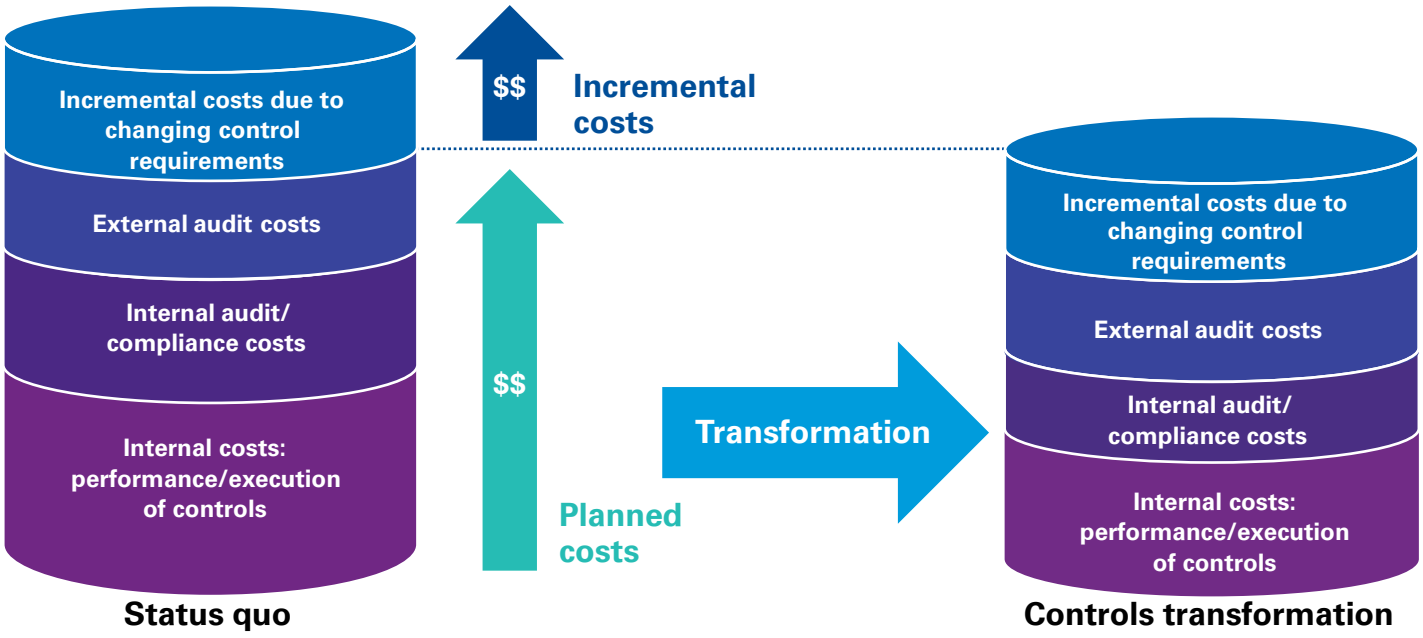
KPMG

A strong business need for smarter controls

The pace of growth and innovation, growing competition, and increased threat of security breaches have caused internal control requirements to become increasingly complex. This complexity has made effective governance, without a well-planned strategy, become unmanageable and costly.

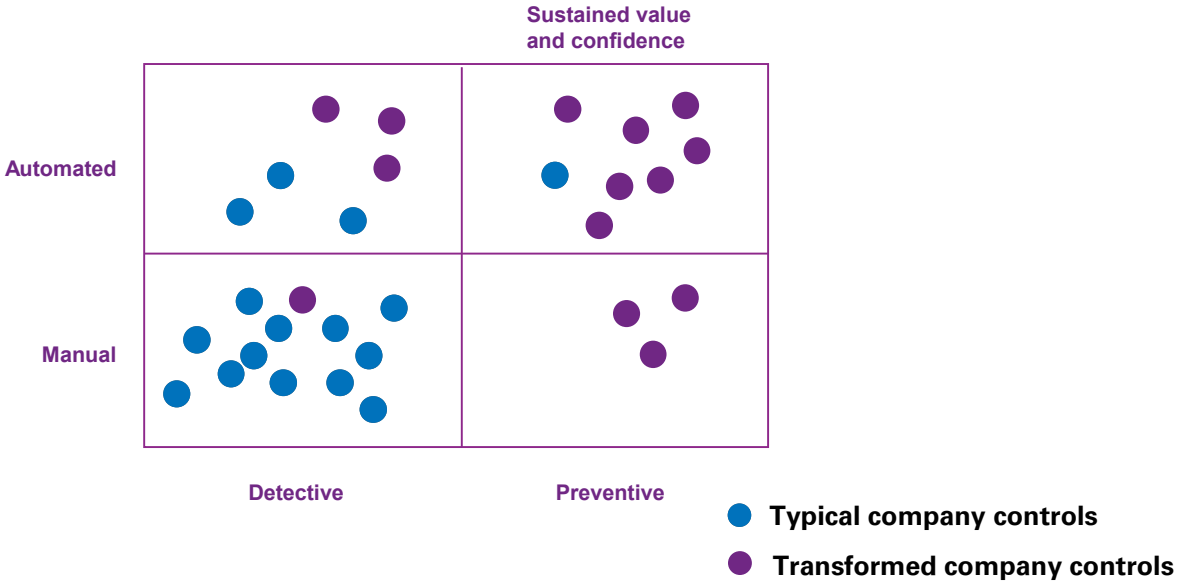
By transforming to an optimal control environment and better leveraging GRC technology, organizations can not only manage their risks effectively, but also gain efficiencies over known (and possibly unknown) planned costs associated with compliance.

Additionally, in the face of the increased scrutiny by regulators and increased control requirements from auditors, keeping the status quo becomes unmanageable.



The dos and don'ts of successful transformation

What exactly does transformation entail? The aim is to take both a "bottom-up" and "top-down" approach to the design, analysis, and evaluation of all controls across the entire enterprise (not just in the field of GRC) for the purpose of eliminating redundant processes, controls, and data environments. It is an ambitious concept. By moving from a mostly manual, detective model to a more automated and preventive one, organizations can begin to reap the benefits from transformation.

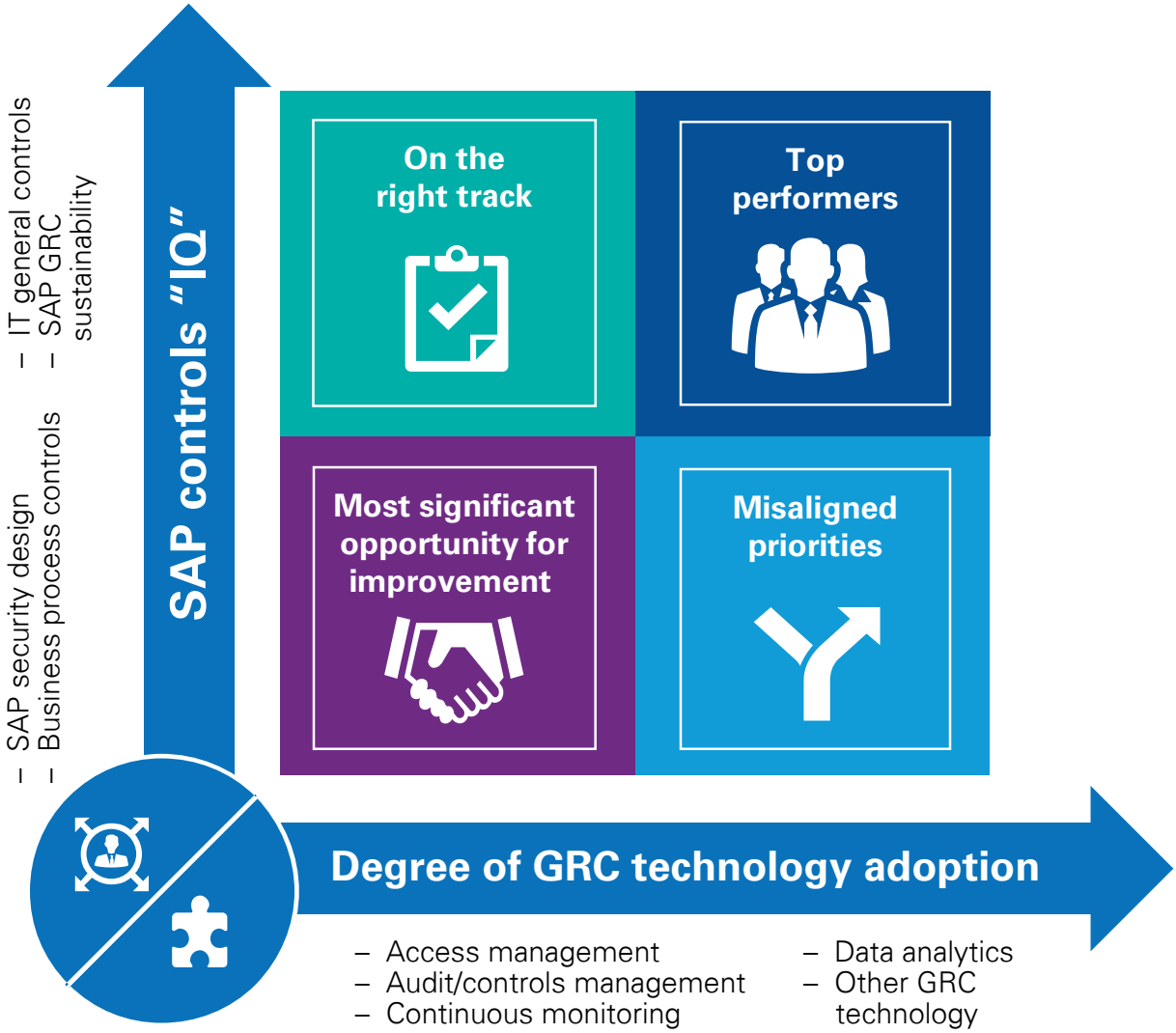


This journey is not easy, but it can be undertaken successfully if organizations follow a number of dos and don'ts. In the former category, it is necessary to consolidate and standardize processes, controls, and IT systems across the organization. Wherever possible, this should include those of acquired entities with different technology platforms. The control environment should be automated as fully as possible and GRC technology leveraged to help in the monitoring and management of controls. Look beyond traditional Sarbanes-Oxley-type controls and focus on opportunities to improve operational efficiency.

It is important to avoid thinking of this as yet another exercise to satisfy annual compliance activities. Do not try to address complex risks with manual controls that will inevitably push up costs. It would be shortsighted to ignore the impact of process changes on personnel and their responsibilities; change management is a fundamental part of the transformation. And do not assume the controls are working well because the auditors have found nothing wrong recently. The GRC landscape is changing rapidly and the controls need to change along with it.

An SAP controls maturity model

To reach for the top right quadrant of the maturity model and be among the top performers, organizations need to make improvements along two dimensions, the smartness of SAP controls, sustainable governance processes, and the degree of GRC technology adoption. If only one dimension is focused on, organizations are liable to make only partial gains or, worse, find the implementation is not aligned with priorities, leading to higher costs, a lack of effectiveness, and a number of audit issues that require expensive remediation.



Case study

A multinational consumer products manufacturing client launched a multiyear controls transformation project with the intention of driving operational efficiency, while advancing along their GRC journey. The project began with a focus on their SAP environment and how to transform to smarter controls. KPMG LLP (KPMG) helped the company along the maturity model as follows:

Control Area	Before Transformation	After Transformation
IT General Controls	A segregation of duties (SOD) framework was not integrated into end-user provisioning. End users were given significantly more access than was required based on job responsibilities.	Critical access and SOD controls were integrated into user access provisioning.
Business Process Controls	The company's controls portfolio consisted of more than 90 percent manual controls. Furthermore, it was found that many of the controls were redundant across control objectives.	By leveraging process automation and configurable SAP controls, manual controls were greatly reduced to the point where more than 50 percent of the controls portfolio consists of automated controls.
SAP Security Design	SAP roles contained a large number of SOD conflicts. Roles did not align with key job functions and ownership of roles within the business were not defined.	Role-level SOD conflicts were eliminated, roles became aligned with job functions, and business role owners are closely involved in role design and maintenance.
SAP GRC Sustainability	SOD rules had not been updated in more than eight years since initial SAP GRC implementation. Roles and responsibilities for the maintenance, use, and governance of SAP GRC did not exist.	Processes and controls over SAP GRC are documented and training materials are established for greater sustainability. Risks monitored by SAP GRC evolve as the company's risk profile changes.

Through control transformation, the company was not only able to remediate significant recurring audit issues, but was also able to achieve significant cost savings in the execution of controls. Most importantly, the company had set a firm foundation for continuing their journey through further adoption of GRC technology. With an SOD framework clearly defined and an SAP security design that was more in line with business use, the company was able to automate end-user provisioning through SAP GRC Access Control. With a more automated control portfolio, the company next looked to automate the testing of these controls through SAP GRC Process Control. Through further integration of GRC technology, the company was able to gain operational efficiencies in access provisioning and decrease control testing efforts by relying on automation. The company continues on its GRC journey, as there are future plans to further expand and integrate data analytics to drive efficiency and gain insights into business risks.

KPMG

Measuring the benefits

A shift in the maturity of the organization is difficult and may add to costs in the short run. All the more reason, therefore, to make the business case for this kind of transformation. Fortunately, the benefits are clear and quantifiable. The effects of improving the intelligence of controls are manifold. They include cost savings in the operation of controls, a more efficient security model, compliance that is aligned more closely with regulatory risks, a decrease in audit issues and fees, and a more sustainable GRC program. The benefits of enhanced GRC technology adoption include reduced resources for security maintenance and support, less effort in testing the controls, and increased visibility into enterprise risks.

The transformation of GRC controls and technology may seem like a luxury, but given the pace of change, organizations are finding that they cannot afford not to undergo the sometimes difficult process of moving to a higher level of maturity.

Why choose KPMG

KPMG's SAP GRC practice consists of a group of professionals focused exclusively on SAP security, risk, and controls. Supported by field-tested tools and methodologies, KPMG can help you:

- Strengthen the GRC organization and processes to manage SAP risk effectively
- Enhance business value by helping to identify operational efficiencies
- Capitalize on opportunities and help minimize losses through enhanced risk management and informed decision making.

About the author

Mick McGarry
T: 214-840-8249
E: hmcgarry@kpmg.com

Mick is a managing director in the GRC Technology practice, based in Dallas. He specializes in SAP advisory and assurance projects, including SAP GRC and security implementation, SAP controls transformation, and data analytics.

kpmg.com/socialmedia