# Looking beyond compliance
## Focusing on strategic business risks

## Overview

Many organizations that rely on SAP software and technology to run their business and operations struggle to keep pace with an ever-evolving risk and compliance landscape. In response, SAP released a wide array of industry-leading governance, risk, and compliance (GRC) technology solutions. The significant cost savings that can be realized from automating compliance business processes should not be ignored. But many organizations are often unprepared for the operational cost to support SAP GRC technology infrastructure, data processing, and process adoption. As a result, more companies are considering outsourcing some or all of their SAP GRC solution management operations.

## The problem

The typical challenges that lead organizations to consider outsourcing IT operations are well-understood. But new SAP GRC technology, coupled with new risk and compliance processes, present a different set of concerns. Cost pressures are certainly a factor, along with scarcity of skilled resources, organizational change, technology adoption, sensitivity of data, and governance complexities.

### Managing GRC talent

The vast majority of SAP business solution customers have made investments in SAP GRC technology. These organizations are often challenged to attract, retain, and afford in-house personnel who have SAP GRC technology experience, along with industry experience and qualifications for risk and compliance process requirements. To make matters more complex, risk and compliance staff workloads fluctuate. Ideally, the size and composition of the team should include personnel with a balance of both business and technical skills, providing the flexibility to adapt to changing demand. This strategy can also allow organizations to redeploy management and process owners to higher value initiatives.

### Managing risk and compliance processes

With rapid changes in risk landscapes and competing compliance priorities, compliance and security teams are hard-pressed to respond. For example, keeping SAP GRC solution functionality and operations aligned with new business initiatives, technology investments, or updates to internal policy may be a daunting task. Add the growing burden from regulators and partners, and it's clear that a new approach may be needed — one that benefits from world-class resources, strategies, standardized methodologies, and consistent processes to create a responsive and agile SAP GRC program.

## Our services

Deloitte has been a Global SAP Partner since 1989. This long-standing strategic alliance has produced a synergy that enables the delivery of industry-leading GRC technology, along with specialized risk and compliance business process integration services.

### SAP GRC management services

Traditionally, managed services have been defined as the set of disciplines for managing, enhancing, and maintaining custom or packaged software. But Deloitte's Security Application Management Services (AMS) go beyond providing these baseline offerings to assist organizations with the management of critical risk and compliance across business processes. Security AMS is also part of Deloitte's broader Cyber Risk Services, which are designed to help companies reap the value of their strategic investments by becoming more secure, vigilant, and resilient.

Deloitte's AMS methodology, demonstrated tools, and resources — as well as the capabilities and deep experience of our global team — are focused on delivering managed SAP GRC support to meet each client's specific business requirements. We offer a full suite of managed security services, including:

| Solution | Technology Management | Process Management |
|---|---|---|
| Risk and Control Management | • Risk and compliance activity monitoring<br>• Risk and control master data maintenance<br>• Risk and compliance evaluation workflow, technical coordination, and error triage | • Risk and compliance self-assessment process deployment<br>• Control testing quality assurance and exception root cause analysis<br>• Consolidated compliance reporting<br>• Executive-level Sarbanes-Oxley (SOX) Section 404 exception reporting<br>• Continuous control monitoring support |
| Fraud Management | • Fraud analytic engine performance monitoring<br>• Fraud rule master data and configuration maintenance<br>• Error and issue support | • Fraud monitoring reporting and metrics<br>• Account analysis assistance<br>• User analysis assistance<br>• Journal entry analysis assistance |
| Access Management | • User provisioning workflow maintenance<br>• Emergency access security role maintenance and support<br>• Master data maintenance<br>• Configuration support | • User access review deployment and coordination<br>• User access inquiry assistance<br>• User access monitoring, reporting, and metrics<br>• Emergency account usage and access request reconciliation monitoring and exception reporting |
| Segregation of Duties (SOD) Management | • SOD rule set maintenance<br>• Identity and access management connector maintenance<br>• Analysis engine performance monitoring | • SOD rule baseline analysis and improvement recommendations<br>• Risk analysis, critical access, and cross-system monitoring<br>• SOD conflict security design root cause analysis support<br>• Mitigation selection support and quality assurance support |
| Application Security Role Management | • Role master data maintenance<br>• Role building workflow maintenance<br>• Error and issue support | • Business transaction usage monitoring and design improvement analysis<br>• Security role configuration quality assurance and root cause analysis<br>• Sensitive data restriction analysis<br>• Role certification process deployment and coordination |

As used in this document, "Deloitte" means Deloitte & Touche LLP, which is a separate subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

# The Deloitte difference

### End-to-end SAP GRC services from a single provider

With more than 40 Service Centers around the globe, Deloitte has the ability to leverage a large pool of security and risk professionals, located on-site, near-site, and offshore, to provide the right level of support for your organization. This includes flexible engagement models for support during the work day, evenings, overnight, and on demand.

We offer multiple delivery models to suit the maturity and security needs of our clients, including:

- A reactive support augmentation model that supplements a client's current resources and practices
- Several joint management models, which allow Deloitte to share responsibilities with a client's team
- A value-level management model that streamlines GRC and security practices to decrease risks, improve resources, and increase return on investment

### Market leader in security consulting and outsourcing

- Ranked #1 in security consulting, globally and in North America, by Gartner[1]
- Listed as a global leader in cyber security consulting by Kennedy[2]
- Named a global leader in security consulting by Forrester[3]
- Ranked #1 in 2013 World's Best Outsourcing Advisors List by the International Association of Outsourcing Professionals®[4]

Our methodologies and tools represent innovative industry-leading thinking for SAP GRC solutions, and we continually evaluate and integrate new capabilities into GRC solutions as they become available.

Deloitte's specialized SAP GRC and security professionals help organizations address nearly every security and risk challenge or need they may face. Not only have they completed intensive immersion security training, but they also have working knowledge of cyber and application risks from their regulatory and auditing backgrounds — making them aware of compliance concerns.

Our Security Application Management Services focus on resource alignment, information protection, and risk management, while leveraging leading practices, driving efficiencies, and helping our clients achieve their targeted risk and compliance results.

[1] Lawrence Pingree, "Market Share Analysis: Security Consulting, Worldwide, 2012," Gartner, Inc., 16 May 2013.

[2] Kennedy Consulting Research & Advisory; Cyber Security Consulting; Kennedy Consulting Research & Advisory estimates © 2013 Kennedy Information, LLC

[3] Ed Ferrara and Andrew Rose, "Forrester Wave™: Information Security Consulting Services Q3 2103," Forrester Research, February 1, 2013.

[4] "The World's Best Outsourcing Advisors for 2013," International Association of Outsourcing Professionals® (IAOP®).

> "The firm (Deloitte) continually develops, tests, and launches methodologies that reflect a deep understanding of clients' cyber security and help the firm stay ahead of the curve and set the bar in terms of addressing cyber security consulting needs."

—Kennedy Consulting Research & Advisory; Cyber Security Consulting; Kennedy Consulting Research & Advisory estimates © 2013 Kennedy Information, LLC. Re-produced under license.

## Contact us

To discuss your unique challenges and how Deloitte can help, please contact any of the Deloitte professionals below. Or visit us online at www.deloitte.com/us/cyberrisk

**Ed Powers**
National Managing Principal
Cyber Risk Services
Deloitte & Touche LLP
+1 212 436 5599
epowers@deloitte.com

**Tapan Shah**
Director
Security Application
Management Services Lead
Cyber Risk Services
Deloitte & Touche LLP
+1 571 766 7469
tapanshah@deloitte.com

**Manoj Bhale**
Senior Manager
Cyber Risk Services
Deloitte & Touche India
Private Limited
+1 615 718 5756
mbhale@deloitte.com

**Chirag Patel**
Senior Manager
Cyber Risk Services
Deloitte & Touche LLP
+1 713 982 3172
chirpatel@deloitte.com

**Stephen Sutherland**
Specialist Leader
Cyber Risk Services
Deloitte & Touche LLP
+1 415 783 5846
stsutherland@deloitte.com

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.