



Internal Audit Transformation

A commissioned point-of-view on behalf of Deloitte & Touche LLP and RSA
Conducted March 2011



Internal audit (IA) is recognized as an essential element of the enterprise risk assessment framework.

The Internal Audit Conundrum

Internal audit (IA) is recognized as an essential element of the enterprise risk assessment framework. Many enterprises are undertaking efforts to upgrade their internal audit capabilities to strengthen their risk framework. How to synchronize IA's work products (e.g., audit work programs and control reviews) and results, meaningfully, within the risk framework remains a pressing question of the day. Essential elements must be considered when addressing this conundrum. How can organizations:

- Achieve enhanced assurance coverage at lower cost to the enterprise,
- Move away from lower value work (i.e., Sarbanes-Oxley Act [SOX], regulatory, etc.),
- Recast internal audit as a strategic partner of the enterprise,
- Focus internal resources on higher value advisory work, and
- Enhance delivery quality.

Many enterprises face the Internal Audit Transformation (IAT) question of "Where do we begin?" Outlined in this point-of-view is an example that demonstrates one firm's approach to addressing IAT through use of a convergence model framework.

The Convergence Model

Historically, assembling governance, risk management, and compliance (GRC) data was a series of time-consuming exercises relying on manual data capture, consolidation, correlation, and interpretation. Inconsistencies in data and its collection gave spotty results. Satisfying the "Are we compliant with the Sarbanes-Oxley act?" remained unclear. Timely access to quality GRC data promises reliable determination of compliance status, consistent and proactive decision-making and enterprise-wide governance, risk management and compliance (eGRC).

The convergence model demonstrates its value in shaping dissimilar systems to bring order to seemingly unrelated issues. Under Deloitte's direction¹, the convergence model uses eGRC to shape technology and process into the enterprise's risk management framework including:

- RSA Archer eGRC technology,
- Deloitte's risk assessment and deployment practice methodologies, and
- Client-oriented consultative process (technology, methodology and practice)

As a tool, eGRC provides information that enhances decision-making, anticipates issues arising, and encourages collaboration.

Deloitte tailors state-of-the-art technologies, assessment methodologies, and collaborative processes to address an enterprise's unique requirements in the following manner:

Technology

Applications bring the business to technology. RSA Archer eGRC provides flexible solutions that build an efficient collaborative program across IT, finance, operations, and legal domains. By configuring and mapping business requirements against risk and controls templates linked to policies based on authoritative sources, eGRC provides a chain-of-trust that demonstrates compliance.

Integrating other RSA Archer solutions, such as Compliance, Risk and Policy, brings a governance structure to the business. A robust issue tracking and reporting capability provides clear, complete and concise reporting across the enterprise hierarchy. Easy to develop on-demand reporting and dashboards provide access to underlying data. The technology deploys quickly, displays informative results, allows adjustment based on results, and responds to changing business objectives.

Methodology

Deloitte's time-tested Risk Assessment Methodology provides a consistent approach for:

1. Conducting an assessment,
2. Identifying and prioritizing risk components,
3. Tailoring the technology against the assessment,
4. Deploying the technology,
5. Evaluating outcomes, and
6. Refining against results.

¹ As used in this document, "Deloitte" means Deloitte & Touche LLP, a 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.

Using the RSA Archer eGRC core suite of tools to highlight risk-relevant relationships, Deloitte's convergent vision of eGRC overlays client requirements and improves the governance process.

Process

Deloitte's consultative approach engages the client, technology and methodology iteratively to adapt enterprise processes to a risk-based approach. RSA Archer eGRC offers out-of-the-box templates that help expedite project start by giving early functional alignment, budget optimization, and risk awareness. Frequently, the process reveals deficiencies that demonstrate eGRC's value almost immediately.

The convergence model visibly improves governability. The model is easily replicated and allows organizations to add new business function incrementally. The working approach that follows demonstrates its practical use for a major financial services organization across major functions.

The Working Approach

The convergence model was used to transform a major financial services organization's resource management systems into enterprise-wide capabilities. Starting with information technology resource management (ITRM), the organization's remediation efforts improved compliance status. Moving to the enterprise resource management (ERM) system, the organization saw improvements in productivity. Finally, the model achieved further productivity gains with by transforming the used to transform operational resource management (ORM) system. Because the three systems relied on similar data, adding each system to RSA Archer required an incremental data capture. Reuse of processes, controls, and reporting resulted in considerable efficiencies across all systems.

Traditionally, the firm's IA function relied on manual audit processes to produce consistent results. Manual processes scale poorly. As demand for audit results increased, automation was used to improve productivity. Automation improved efficiency, but lacked extensibility: each audit area, e.g., operational audits, required separate automation projects and, often, increased audit scope. For instance, compliance automation expanded each audit's data capture requirements. Even with better results, automation was not game changing.

Given eGRC results, the firm asked Deloitte to leverage their existing deployments in support of IA by adding RSA Archer's internal audit transformation solution. By applying advanced audit techniques Deloitte tailored the model to help align management objectives across business units and enhance risk management.

Alignment

Before the engagement IA activity was viewed as redundant, required excessive time on routine items, and was treated with disdain! Because results were viewed as unreliable, external auditors repeated internal audit's data gathering and controls testing. The redundant audit efforts annoyed business units

After the engagement, IA now relies on the repository for data capture, posting findings, and issuing reports. New audits leverage the repository by adding incrementally as necessary, giving more time for analysis and review. Changing their view, business units, external auditors, and senior management now see IA as adding value and contributing, positively, to key performance indicators (KPI).

Capability

RSA Archer's reporting and dashboards (summarized KPI views) were tailored to include control and compliance categories. The initial deployment relied on standard templates of risks and controls in the IAT solution. Display of control and compliance KPI status was used to correct issues arising.

Perhaps the most important aspect of RSA Archer is enterprise communication through workflow technology. By providing clear concise reporting to the Audit Committee and business management hierarchy, remediation of findings can rely on priorities based on an enterprise-wide risk assessment. Timely issue tracking, reporting and resolution are the result.

Risk Management

Deloitte's tailored Risk Assessment Methodology shortened the deployment timeframe by leveraging RSA Archer's out-of-the-box risk and control libraries. Several audit findings were highlighted and action was taken to immediately address them.

The eGRC litmus test is in the demand for its use by unrelated business units. Now the businesses view eGRC as "a way to get things done!" and ask to use it for their business units. Less repetitive, routine work allows IA to adopt a consultative and strategic role. Deloitte's convergence model enables a business view of internal audit and makes it available for use across all business units.

Indicative Costs

Internally, routine audit activities, such as data gathering, use data repositories that encourage the “capture once, use many” approach. Front-end audit work shortens by eliminating redundant data capture, which gives more time for testing, review, and analysis. Tracking of findings, timely remediation of findings, and visibility within the controls hierarchy, reduces overall risk, while improving IA’s value.

The internal savings from improved resource allocation and higher productivity contribute to a positive return on investment. The intangible benefits accruing to IA are greater enterprise-wide value and strategic impact.

External audit fees may decline with greater reliance on internal audit’s findings and reports. Such reliance preserves external audit’s effectiveness, shortens timing, encourages review of complex controls, and increases the value of results. Project deployment costs may be offset with savings from reduced redundancy between internal and external audit efforts.

Contacts

To discuss your business challenges and solutions, contact a Deloitte or RSA professional below.

Sean Peasley

Principal
Deloitte & Touche LLP
+1 714 436 7410
speasley@deloitte.com

Kim Altern

Senior Manager
Deloitte Services LP
+1 212 436 3634
kaltern@deloitte.com

Rick Hedeman

Alliance Manager
RSA, The Security Division of EMC²
+1 781 515 5332
rhedeman@rsa.com

Scott Cogan

Strategic Alliances
RSA, The Security Division of EMC²
+1 703 864 1613
scott.cogan@rsa.com