

# EMA's 2008 Survey of IT Governance, Risk and Compliance Management in the Real World

Sponsored by:



Written by Scott Crawford, Research Director  
Enterprise Management Associates



## Introduction

In recent months, the theme of IT governance, risk and compliance (IT GRC) management has arisen as the point of convergence where the governance of the organization intersects with the governance of IT, where the control of risk in, of, and by IT serves to control risk to the business, and where regulatory compliance directly affects IT.

Already in this short time, IT GRC has become a loaded term, high on expectations but far too often short on specifics. What exactly does IT GRC mean to enterprises pursuing the broad mandates implied? How do businesses reckon success with these initiatives, and what are the qualities that make for success in IT GRC management?

In this study, the ENTERPRISE MANAGEMENT ASSOCIATES® (EMATM) team surveyed 224 IT as well as non-IT professionals to answer these questions. While organizations of all sizes were represented, a full one-third (34%) of all respondents were very large enterprises of 20,000 employees or more, with organizations between 1,500 and 20,000 employees making up another 48%. Nearly half (44%) of all respondents represented organizations having annual revenues of \$1 billion or more, with one-fourth (25%) reporting annual IT budgets in excess of \$100 million. Although most respondents (89%) were based in North America, nearly half (46%) had a presence in Europe, the Middle East and Africa, while 40% were represented in the Asia-Pacific region, and 30% in the Americas.

---

*IT GRC has become a loaded term, high on expectations but far too often short on specifics.*

---

## Issues and Challenges

The concerns expressed by respondents are substantial. Among those measured in this survey:

- 13% of all respondents say that their organization has no strategy in place to assure the confidentiality of sensitive information. 21% of those that do have such a strategy do not believe it is effective.
- 29% of all respondents indicate that the board of directors (or its equivalent) and senior executives do not adequately support IT governance, risk and compliance initiatives.
- One-third (33%) of all respondents do not believe their internal audit function is adequately skilled and staffed.

- 29% of all respondents never perform a risk assessment of external service providers, despite the growth of IT functionality offered as a service.
- Access control gaps have become a major concern. One IT auditor reported that, in one company of about 5,000 employees, 43% of existing access rights were either excessive or should have been retired.
- Disconnects between the business's understanding of risk management and IT's challenge the measurement—and management—of IT GRC effectiveness. Less than half of all respondents (47%) measure the cost of IT security events in terms of person-hour impact. Even fewer (31%) measure the dollar impact of security events. Despite the numbers who say they measure, only 6% of all respondents can quote a figure for the person-hour impact of security events over the previous year, while only 4% can quote a figure for the dollar impact.
- These disconnects become apparent in incidents where business risk exposure is directly related to gaps in IT risk control. In the case of alleged fraud at French bank Societe Generale, for example, the bank's exposure at its worst—approximately \$70 billion—was larger than the estimated GNP of Kuwait, in a case traceable to alleged abuse of risk controls in IT specifically.

## Key Findings

How are enterprises succeeding in IT GRC management? If there were one response to this survey that distills the answer to this question more completely than any other, it would be one respondent's galvanizing definition of IT GRC: **“Turning process into a strategic asset.”**

- The guidance most frequently adopted by all respondents is not a risk or compliance control framework. It is the process-centric IT Infrastructure Library. Some version of ITIL has been adopted by 55% of all respondents—19% ahead of the next most frequently referenced guidance
- That next-most-frequent guidance is not specific to IT management *per se*. It is in *quality* management. 36% of all respondents have adopted quality management standards such as Six Sigma or the ISO 9000 series.
- These numbers compare to rates of adoption of 30% for the ISO 27000-series and related BS 7799 risk management standards, 29% for COBIT, and 11% for COSO.

In order to understand the factors that drive IT GRC effectiveness, respondents were asked to describe their characteristics and performance in the following areas:

- **Organizational attributes**, particularly the criticality of IT governance, risk and compliance management to the business, as well as the criticality of IT to key business operations.
- **Business alignment**, as reflected in the structure of IT governance, the effectiveness of IT's cooperation with the business, and in integrating the values of the business in alignment with corporate governance, risk and compliance management.
- **IT management maturity and discipline** in key domains central to effective IT governance and the management of risk and compliance in IT
- **IT risk control outcomes** that indicate the effectiveness of IT GRC efforts

In general, those who answered consistently in any one of these areas tended to answer with the same consistency in all others. This enabled the identification of high performers (23%), medium performers (51%), and low performers (26%) in IT GRC management effectiveness.

For high performers, the criticality of IT as a strategic asset correlated to the criticality of IT GRC effectiveness. This, in turn, led to greater support among senior management for assuring accountability for adherence to defined objectives. This support for accountability means that some high performers see IT governance itself as the primary means of managing risk to sensitive information.

High performers placed high value on key domains of management—particularly those with high relevance to IT Service Management, such as configuration management:

- 94% of high performers **define** configuration change control processes, **assure** that defined processes are followed, and **enforce accountability and consequences** for deviations.
- 91% of high performers monitor the IT environment for changes, and use monitoring information to enforce change control. Among all respondents, configuration and change audit was the tool most frequently used for IT GRC management (50%).
- High performers also showed higher maturity than medium or low performers in the adoption of best practices in configuration-related IT management such as the CMDB.

High performers also place high value on access control, access monitoring, and detection of anomalous events that indicate actual or potential risk:

- 77% of high performers monitor IT access and use for indications of fraud or other business risks, *before* a suspicion exists.
- 77% of high performers monitor the internal IT environment for anomalous behavior or other indications of potential security risks, *before* a suspicion exists.

Other domains of management where high performers showed highest maturity include:

- Security management, and the integration of security processes across multiple domains.
- Event management and incident response, which often integrates with service support processes such as the service desk.
- Business continuity planning and management, where processes as well as metrics such as mean time to recovery (MTTR) are among the most mature in IT risk management, because of their criticality to the business.
- Realism in defining risk management processes, as well as in *proving* effective risk and compliance management, through techniques such as penetration testing, detailed visibility into network activity, and leveraging the findings of internal audit.

---

*Not only did high performers have overall better outcomes in risk and compliance management than medium and low performers, in many cases medium and low performers showed significant overlap, while high performers often stood substantially apart.*

---

## More Positive Outcomes

Not only did high performers have overall better outcomes in risk and compliance management than medium and low performers, in many cases medium and low performers showed *significant overlap*, while high performers often stood substantially apart. For example:

- 64% of high performers (but only 37% of medium performers) reported that 10% or fewer security incidents were disruptive to IT performance, availability or resource integrity in the past year (2007).
- In comparison, half (50%) of all medium performers (but only 31% of high performers) indicated that *more* than 10% of security events in the past year were disruptive to IT.

High performers had similarly more positive outcomes relative to medium and low performers in the success of IT projects, IT change success, and percentages of unplanned work.

## High Performers Lead in Adoption of IT GRC Management Tools

Given the criticality of IT GRC to high performers, it is not surprising that the top three management technologies where high performer adoption is farthest ahead of all others are:

- Configuration and change audit (high performers are 23% ahead of medium performers).
- Business or financial GRC management systems (high performers are 18% ahead of medium performers).
- Tools purpose-built for IT GRC management (high performers are 17% ahead of medium performers).

Tools for GRC management enable high performers to lower the total impact of the broad and varied range of IT GRC priorities in four primary ways:

- Rationalization of a number of IT governance, risk and compliance requirements, control frameworks, standards and best practices, better enabling enterprises to “implement once, comply with many.”
- Monitor the effectiveness of IT GRC management by integrating with IT GRC management tools in multiple domains. The long-range objective of these solutions is to become the system of record for IT GRC management across a number of domains, relieving auditors as well as risk and compliance managers from having to refer to multiple control systems, thereby improving the efficiency of audit as well IT GRC management efforts.
- Flexibility in reporting adaptable to the satisfaction of multiple compliance and management requirements, again reflecting the value of “implement once, comply with many,” and reducing the total cost of compliance to the organization.

- New approaches to IT risk analytics that give enterprises tools for closing the gaps in communicating IT risk and compliance management effectiveness in terms meaningful to the business.

For the highest performers, GRC management systems also help achieve more strategic objectives such as mapping the most relevant aspects of multiple best practices and control frameworks to the specific requirements of their organization.

---

*The experience of high performers confirms not only the value of a strong approach to defining IT governance and processes for risk control, but also the tools, technologies and techniques that make control real.*

---

## In Conclusion

Over and over again, the recurring theme of all these aspects of IT GRC management is constant: the strategic value of process—not just empty processes conceived to fulfill some vague best practices ideal, but the processes enterprises actually rely on to define IT governance, assure a systematic approach to risk management across multiple domains, and attain regulatory compliance.

The experience of high performers confirms not only the value of a strong approach to defining IT governance and processes for risk control, but also the tools, technologies and techniques that make control real. As EMA continues to explore this broad and dynamic domain, we expect high performers to continue to define the reality of IT governance, risk and compliance, and we expect to visit this topic again as the field continues to expand.

## About Symantec

Symantec's Control Compliance Suite supports IT Governance, Risk and Compliance (IT GRC) initiatives within global organizations. It provides customers with the ability to automate key IT compliance processes including policy management, assessing and monitoring IT controls compliance, remediation of deficiencies and reporting in order to reduce the risk to their information assets and reduce the costs of managing compliance.

Increasingly, IT management is being called on to align the business objectives amidst shrinking budgets. Business executives are asking IT to achieve compliance for internal and external mandates while managing the delicate risk versus return balance. Compliance process automation is the key to meeting these requirements in a cost-effective and sustainable manner.

By combining IT risk assessment and compliance capabilities into an integrated solution, Symantec helps customers improve alignment between IT compliance and business risks. Control Compliance Suite lets customers implement end-to-end coverage of the IT compliance lifecycle strengthening its IT GRC practices – from defining appropriate policies based on regulatory mandates to assessing IT controls to remediating deficiencies and finally generating detailed reports.

Symantec Control Compliance Suite offers flexible and scalable deployment options for the largest and most complex IT infrastructures in the world. It provides global coverage for regulatory content, frameworks and best-practice standards. The newest version of

Control Compliance Suite will support assessment of IT controls for a broad range of IT platforms as well as risk assessment capabilities that enable quick identification and remediation of information assets at highest risk in the organization.

Organizations with mature IT GRC practices such as frequent auditing of their IT environment against company policies and standards often benefit from increased revenue, higher customer satisfaction, less data loss and lower compliance costs.

Control Compliance Suite newest module lets organizations collect, store and analyze log data as well as monitor, prioritize and respond to security incidents. As a result, security teams can proactively monitor risk to their IT assets in real time and meet compliance requirements around incident response and log management.

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information and interactions by delivering software and services that address risks to security, availability, compliance and performance. Headquartered in Cupertino, CA, Symantec has operations in more than 40 countries. More information is available at [www.symantec.com](http://www.symantec.com)