Transform Governance, Risk and Compliance to Integrated Risk Management

Published: 6 October 2016

Analyst(s): John A. Wheeler

Integrated risk management enables simplification, automation and integration of strategic, operational and IT risk management processes and data. Risk and security leaders should use Gartner’s definition for IRM to structure risk management processes, functions and technology requirements.

Key Challenges

■ Seventy-four percent of global risk management executives state that their ability to forecast critical risks will be more difficult in three years. The leading obstacle to forecasting critical risks noted by these executives is the continued lack of cross-organization collaboration.

■ The governance, risk and compliance (GRC) software market has evolved and segmented. Risk and security leaders must understand this segmentation as well as the evolving need to provide an integrated view of strategic, operational and IT risk management processes and data.

■ Risk management solutions and related processes are typically focused on individual functions across an organization, which inhibits collaboration and understanding of risk at an enterprise level.

■ Many organizations employ a "technology-first" mindset when trying to solve their most pressing risk management challenges. This leads to a highly fragmented risk management technology architecture that cannot meet the needs of the senior executive management team and the board of directors.

Recommendations

■ Use the Gartner definition of integrated risk management (IRM) to structure risk management processes, functions and technology requirements to make better-informed decisions and develop comprehensive, enterprisewide IRM requirements.

■ Develop comprehensive, enterprise-specific IRM requirements to align current and future IRM initiatives and investments.
Assign accountability for addressing the gaps, issues and findings provided by well-executed risk management.

Table of Contents

Introduction............................................................................................................................................ 2
Analysis..................................................................................................................................................3
Use Gartner’s IRM Definition to Structure Risk Management Goals, Functions and Requirements to Make Better-Informed Decisions.......................................................................................................3
Operational Risk Management............................................................................................................4
IT Risk Management............................................................................................................................4
IT Vendor Risk Management...............................................................................................................5
Business Continuity Management Planning........................................................................................5
Audit Management..............................................................................................................................5
Corporate Compliance and Oversight..................................................................................................5
Enterprise Legal Management............................................................................................................6
A Coordinated System Is Needed.......................................................................................................6
Gartner Recommended Reading............................................................................................................6

List of Figures

Figure 1. Gartner IRMS Market Segments..............................................................................................4

Introduction

IRM is a set of practices and processes supported by a risk-aware culture and enabling technologies, that improves decision making and performance through an integrated view of how well an organization manages its unique set of risks.

Under the Gartner definition, IRM has certain attributes:

- **Strategy:** Enablement and implementation of a framework, including performance improvement through effective governance and risk ownership
- **Assessment:** Identification, evaluation and prioritization of risks
- **Response:** Identification and implementation of mechanisms to mitigate risk
- **Communication and reporting:** Provision of the best or most appropriate means to track and inform stakeholders of an enterprise's risk response
- **Monitoring:** Identification and implementation of processes that methodically track governance objectives, risk ownership/accountability, compliance with policies and decisions that are set through the governance process, risks to those objectives and the effectiveness of risk mitigation and controls

- **Technology:** Design and implementation of an IRM solution (IRMS) architecture

To understand the full scope of risk, organizations require a comprehensive view across all business units and risk and compliance functions, as well as key business partners, suppliers and outsourced entities. Developing this understanding requires risk and security leaders to address all six IRM attributes.

**Analysis**

**Use Gartner's IRM Definition to Structure Risk Management Goals, Functions and Requirements to Make Better-Informed Decisions**

Risk management solutions are an increasing area of focus for most organizations, as risk profile complexity and interconnected relationships grow explosively. In fact, according to a 2016 survey of risk executives by the Risk and Insurance Management Society, 74% of respondents state that their ability to forecast critical risks will be more difficult in three years. Moreover, the leading obstacle to forecasting critical risks noted by these executives is the continued lack of cross-organization collaboration.

To understand the full scope of risk, organizations require a comprehensive view across all business units and risk and compliance functions, as well as key business partners, suppliers and outsourced entities. As a result, new technology solutions are emerging to increase the collaborative nature of risk management, both within and external to an organization.

There are a growing number of IRMS vendors (see "Market Guide for Integrated Risk Management Solutions") that automate various workflows in support of cross-organization collaboration for risk management. Through common functions such as an asset repository, regulatory mapping, survey capabilities, workflow functions and data import, IRMS vendors address multiple market segments defined by Gartner. The seven defined Gartner IRMS (formerly known as GRC) software market segments are as follows (see Figure 1; for more information and context, see Note 1):

- Operational risk management (ORM)
- IT risk management (ITRM)
- IT vendor risk management (VRM)
- Business continuity management planning (BCMP)
- Audit management (AM)
- Corporate compliance and oversight (CCO)
Operational Risk Management

The linchpin for the seven market segments is ORM (see Figure 1) since it is most broadly focused on those risks that "relate to the uncertainty of daily tactical business activities, as well as risk events resulting from inadequate or failed internal processes, people or systems, or from external events" (see "Magic Quadrant for Operational Risk Management Solutions"). ORM software applications allow organizations to aggregate and normalize data from multiple data sources, including operational and financial systems, as well as from external sources such as regulatory alerts and loss-event databases.

IT Risk Management

IT risks are those within the scope and responsibility of IT, the IT department or IT dependencies that create uncertainty in business activity. ITRM solutions automate IT risk assessments, policy management, control mapping and reporting, security operations analysis and reporting, and incident management (see "Magic Quadrant for IT Risk Management Solutions").
IT Vendor Risk Management

Vendor risk management programs help organizations manage the risks of third parties with adequate controls for business continuity management, vendor performance, vendor viability security and data protection. Failure to comply with these mandates can have significant audit-related, and, for some industries, regulatory repercussions, which can undermine shareholder value and corporate viability. The IT VRM market addresses risks related to regulatory compliance, information security and vendor performance that arose from enterprises' increased use of, and reliance on, service providers and IT vendors. Solutions in this market have capabilities ranging from risk assessment to risk monitoring and risk rating (see "Magic Quadrant for IT Vendor Risk Management").

Business Continuity Management Planning

Business continuity management (BCM) is the practice of coordinating, facilitating and executing activities that ensure an enterprise’s effectiveness in identifying risks that can lead to business disruptions, implementing disaster recovery solutions and recovery plans, responding to disruptive events and recovering mission-critical business operations. BCMP software automates processes such as risk assessment, business impact analysis (BIA), and recovery plan development, exercising and invocation. BCMP tools can greatly benefit organizations by jump-starting their BCM programs and quickly improving their overall continuity capability (see "Magic Quadrant for Business Continuity Management Planning Software, Worldwide").

Audit Management

Internal auditors have three roles: auditing, providing advice to middle and senior management, and providing consultation to business process stakeholders. When risk owners and management do not identify risk or adequately mitigate the risk, it is imperative for the internal auditors to provide independent and objective insight on risk. The audit management solution market caters to this need by automating internal audit operations. These solutions automate audit planning, scheduling, work paper management, time and expense management, reporting and issue management (see "Market Guide for Audit Management Solutions").

Corporate Compliance and Oversight

The scope of compliance management programs continues to increase. Regulatory compliance and change management gets more and more complicated. The recent increase in focus on commercial compliance (increasingly required by business partners) and organizational compliance requirements (such as ethics and corporate social responsibility) has made the compliance manager’s role ever more challenging. Corporate compliance and oversight software supports the goals and activities of compliance leaders, providing automated policy development and management, compliance risk assessment, control rationalization, assessment and attestation, regulatory change management and investigative case management (see "Market Guide for Corporate Compliance and Oversight Solutions").
Enterprise Legal Management

Enterprise legal management software applications are focused on supporting legal and compliance departments, corporate secretaries, boards of directors and senior management. They provide support through better documentation, spend management, information availability and collaboration via an integrated set of applications that include matter management, e-billing, financial/spend management, legal document management and business process management (see "Market Guide for Enterprise Legal Management Solutions").

A Coordinated System Is Needed

Enterprises that can coordinate their risk management activities better often do so through an enterprisewide operational risk management program and collaboration between the risk management, corporate compliance functions, and business unit leaders who are accountable for risks. Risk and security leaders must also assign clear accountability for action to be taken based on findings from risk management activities. A central system for tracking deficiencies, analysis of correlation of deficiencies between risk management silos and the impact on business outcomes, and prioritization of remediation should be maintained. This type of approach supports the collaboration of multiple stakeholders (including IT, legal, finance, risk, compliance, audit, strategy and business unit leaders) in pursuit of greater risk awareness, accountability and, ultimately, better decision-making capabilities.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Magic Quadrant for Operational Risk Management Solutions"
"Magic Quadrant for IT Risk Management Solutions"
"Magic Quadrant for IT Vendor Risk Management"
"Magic Quadrant for Business Continuity Management Planning Software, Worldwide"
"Market Guide for Audit Management Solutions"
"Market Guide for Corporate Compliance and Oversight Solutions"
"Market Guide for Enterprise Legal Management Solutions"
"Hype Cycle for Risk Management Solutions, 2016"
"Market Guide for Integrated Risk Management Solutions"
"Special Report: Cybersecurity at the Speed of Digital Business"
"2015 CEO Survey: Committing to Digital"
Note 1 Shift From GRC Software to IRMS Market Focus

In 2013, Gartner embarked on a process to renovate its coverage of the GRC software market. This process involved nine analysts who collectively took more than 1,000 inquiry calls a year on GRC requirements. Supported by survey research of both Gartner and non-Gartner clients, the analyst team determined that the predominant use of GRC software focused on seven primary market segments (see IRMS market segment definitions above).

In late 2015, Gartner conducted a survey of Gartner clients to better understand the use of GRC software to support the ever-growing importance of risk management across the enterprise. In that survey, 63% of survey respondents who are not currently using GRC software reported that the effort to provide consolidated risk management information to the senior executive team and board of directors requires either a "fully" or "extensive level" of manual effort. In addition, of the nearly 40% of clients who are not using GRC software, 65% are not familiar with the term "GRC." However, in a 2015 Gartner CEO survey, 65% of global CEOs and senior executives view that the level of investment in risk management tools and practices are falling behind (see "2015 CEO Survey: Committing to Digital").

Also, Gartner has noted a shift away from compliance-focused imperatives related to GRC software deployments to greater investment in risk-based approaches designed to respond more effectively to the growing cybersecurity and related digital business demands facing organizations today (see "Special Report: Cybersecurity at the Speed of Digital Business"). As a result, Gartner is now focusing its research on the more aptly termed IRMS market, seven market segments and related key stakeholder roles shown in Figure 2.
Figure 2. Gartner IRMS Research and Related Key Stakeholder Roles

<table>
<thead>
<tr>
<th>Hype Cycle for Risk Management Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Financial Officer</td>
</tr>
<tr>
<td>Magic Quadrant for Business Continuity Management Planning</td>
</tr>
<tr>
<td>Chief Procurement Officer</td>
</tr>
<tr>
<td>Magic Quadrant &amp; Critical Capabilities for Operational Risk Management</td>
</tr>
<tr>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>Magic Quadrant for IT Vendor Risk Management</td>
</tr>
<tr>
<td>Chief Legal Officer/General Counsel</td>
</tr>
<tr>
<td>Market Guide for Audit Management</td>
</tr>
<tr>
<td>Chief Operating Officer</td>
</tr>
<tr>
<td>Magic Quadrant for IT Risk Management</td>
</tr>
<tr>
<td>Chief Risk Officer</td>
</tr>
<tr>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td>Market Guide for Corporate Compliance &amp; Oversight</td>
</tr>
<tr>
<td>Chief Audit Executive</td>
</tr>
<tr>
<td>Market Guide for Enterprise Legal Management</td>
</tr>
<tr>
<td>Chief Compliance Officer</td>
</tr>
</tbody>
</table>

Source: Gartner (October 2016)

Evidence
