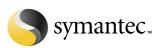# 8 Key Requirements of an IT Governance, Risk and Compliance Solution

Confidence in a connected world.   ✸ symantec™

8 Key Requirements of an IT Governance, Risk and Compliance Solution

Contents

Introduction

Today IT security teams must contend with a dizzying array of challenges, from cyber-crime and government regulation to the ever increasing complexity of the IT environment itself. For organizations that handle large volumes of customer and employee information, the risk of a data breach is now higher than ever before. Driven by the rising tide of organized cyber-crime, targeted attacks are increasingly aimed at stealing information for the purpose of identity theft. More than 90 percent of records breached in 2008 involved groups identified by law enforcement as organized crime.[1]

At the same time, the growing number of government regulations, industry standards and internal mandates make compliance a difficult and expensive undertaking. According to a recent survey by the IT Policy Compliance Group, 70 percent of respondents are now subject to multiple regulations, standards and mandates required by contractual obligations. In addition, IT infrastructures have reached such a level of scale and complexity that it is now difficult to control deviations from technical standards. There is constant tendency toward *configuration drift* that can lead to breakdowns in the security, availability and reliability of data and systems.

Given these IT governance, risk and compliance challenges, it is essential to establish strong security policies to protect both assets and information. But putting policies in place is only a first step. It is also necessary to ensure that these policies are effectively enforced. To meet strategic management objectives, IT must continuously monitor and remediate any deviations from established standards and do so in a manner that is efficient and cost-effective.

Fortunately, many solutions are available to solve these challenges, each offering its own set of features and functionality. But what criteria should a company use in evaluating these solutions? This paper answers that question by exploring the eight key requirements of an IT Governance, Risk and Compliance (IT GRC) solution.

Common approaches to the problem

For many organizations today, policy compliance is still managed manually with checklists, spreadsheets and paper-based questionnaires. This tends to be an expensive process since it typically involves redundant efforts as different groups develop and manage their own procedures involving common controls across multiple mandates. It also leads to a lack of visibility into policy enforcement both within the business unit and across interrelated IT applications and environments. This manual approach to managing compliance makes it relatively easy for auditors to find discrepancies between policies, procedures, controls and documentation. The ensuing confusion leads to higher business risks, more audit deficiencies and higher audit fees.

Some organizations expand on existing practices using best of breed, point products to solve IT risk and compliance challenges. However, this piecemeal approach tends to be quite costly due to additional expenses for hardware, software, maintenance, integration and vendor management.

1-Verizon Business Risk Team, 2009 Data Breach Investigations Report

Key requirements of an IT Governance, Risk and Compliance solution

Balancing today's requirements for better IT security and policy enforcement with the growing need to control the cost and complexity of compliance, organizations are starting to look for a more comprehensive approach to solving the IT GRC problem. To help you find the right solution for your organization, the following set of key requirements provides a sound basis for evaluation and planning:

- Policy and controls mapping
- Policy distribution and attestation
- Automated assessment of procedural controls
- Automated assessment of technical controls
- IT asset repository
- IT risk evaluation
- Remediation management
- Flexible reporting and analytics

This list of requirements is consistent with the recommendations of industry analysts at Gartner.[2] In addition, research by the IT Policy Compliance Group reveals that organizations with the lowest risks and fewest audit problems are three times more likely to have adopted solutions that meet all eight of these key requirements.

1 - Policy and controls mapping

Whether IT policies are designed to meet industry regulations, best-practice frameworks or internal directives, policy management is at the heart of an effective IT GRC solution. Defining and managing policies is a complex task. To ensure the secure operation of business processes throughout the enterprise, IT policies must be mapped to both technical controls that protect IT assets and data as well as procedural controls that drive specific employee behaviors. This can be costly and time-consuming. For example, the IT Policy Compliance Group notes that simply mapping control statements to policies from PCI, ISO or CobiT averages one-person day per control statement. Such efforts place organizations in the business of managing content that adds little value, while reducing the value of IT's overall contribution to the business.

By leveraging an IT GRC solution which automates the compliance process, you can greatly reduce the number of employees required to help manage policies. Automation allows your organization to define a superset of control requirements across multiple regulations, frameworks and internal mandates so you can test a given control once and apply the result to multiple mandates. These capabilities are critical to saving time and resources by eliminating redundant efforts.

Some IT GRC solutions can also help by providing up-to-date policy content, including customizable sample policies and policy templates for all relevant regulations and standards. When the vendor monitors any changes in regulations, such as the recent update from PCI version 1.1 to PCI version 1.2, and updates policy content and control statements accordingly, your organization is relieved of the burden of expertise.

2-Gartner Research, Mark Nicolett, Paul E. Proctor, "Critical Capabilities for IT Governance, Risk and Compliance Management, 2009," 16 April 2009

2 - Policy distribution and attestation

Not only do organizations need to define polices, they also need to manage every stage of the policy lifecycle, following repeatable steps to review, publish and distribute policies to the appropriate individuals and groups. By adopting a solution with automated workflow you can simplify this process by automatically tracking policy acceptance, exceptions and comments. This data can then be used to provide proof of policy enforcement for audit purposes.

Taking this a step further, some IT GRC solutions enable you to automatically trigger policy expirations or force annual policy reviews as required by many regulations. For organizations still using manual processes to manage policies, these measures can be especially challenging to implement.

3 - Automated assessment of procedural controls

Procedural controls governing employee behavior can be difficult to assess. For example, how do you verify in a cost-effective manner that your employees have actually read and understood your corporate security policy? Similarly, how do you verify that the right processes are being followed with respect to employee hiring and termination?

A key step is to replace paper-based surveys that require manual distribution and collection with Web-based survey tools that allow you to poll business owners on the completion of required procedures. Some IT GRC solutions supply sample customizable surveys that encompass IT administrative processes, use of assets, and security incident response procedures. Survey responses are then collected in a central repository for analysis and reporting.

For added value, these solutions typically allow you to attach supporting documentation or links to relevant web sites to further educate employees. Such survey tools may be used for security awareness training, allowing you to easily educate your user community, evaluate their understanding of security topics, and provide evidentiary support for auditing purposes.

Automating the assessment of these procedural controls also allows you to assess them more frequently thus improving your overall IT risk and compliance posture without incurring higher costs.

4 - Automated assessment of technical controls

Many organizations face major challenges managing technical controls. According to the IT Policy Compliance Group, 63 percent of organizations fail audits due to problems found with user and application access controls. Other common technical control failures include IT policies and standards (63 percent), IT configurations and change management (63 percent), and controls for application development and maintenance (50 percent).

Given the number and diversity of technical controls that organizations must monitor for security and compliance reasons, it is neither cost-effective nor practical to evaluate them all without automation. By leveraging an automated IT GRC solution, the status of technical controls can be evaluated on a programmatic basis using best-in-class pre-packaged content, such as sample control statements mapped to technical controls. With such a solution, deviations from technical standards (or configuration drift) across servers, desktops, databases and directories can be identified automatically. Automation also allows organizations to increase the frequency of controls assessments to improve their overall security posture without incurring higher costs.

In order to evaluate technical controls across the entire enterprise, it may be necessary to deploy both agentless and agent-based data gathering options. Larger organizations also require a solution that provides broad hardware and software platform support for multiple operating systems, databases and applications.

5 - IT asset repository

A consolidated view of your IT assets—one that provides a clear understanding of which assets support which business processes—is essential to improving both your security posture and your compliance results. For example, to enforce data security you need to know which servers in your environment house confidential data and ensure those servers are patched and configured correctly to prevent any breaches. For purposes of compliance and risk management, being able to prioritize controls and remediation based on asset classifications, such as confidentiality, integrity, and availability, allows you to focus your resources on areas of greatest risk.

While most organizations recognize the benefits of a centralized view, due to the heterogeneous and dynamic nature of most IT environments, the IT asset repository can be difficult to implement. Even those organizations who have found a way to create such a repository have frequently had challenges classifying their assets in a meaningful way and keeping the repository current. Smart organizations are adopting IT GRC solutions that help them automate the discovery and classifications of assets. These tools discover new assets in the environment, including data feeds from other asset systems, and automatically classify assets by their properties. They enable organizations to benefit from a centralized view of assets in terms of security and compliance, without adding additional IT overhead.

6 - IT risk evaluation

It is impossible to completely eliminate risk in today's challenging IT environment. The best approach therefore is to adopt a risk-reduction strategy by implementing a solution that allows your organization to prioritize security and compliance efforts based on risk level. For example, by using an industry-standard risk scoring algorithm (Common Vulnerability Scoring System) you can assign an externally facing Web server or a PCI server a higher risk value than a print server so that deficiencies or problems on these high-risk assets are given priority status in terms of remediation efforts. You may even decide that to improve the overall security posture of your environment you need to have tighter configuration controls on these high risk assets.

For procedural controls, it should be possible to conduct risk-weighted surveys following the distribution of new policies and rate responses based on risk. Ultimately, your IT GRC solution should help you to focus on high-priority controls in order to meet risk and compliance goals on time, and within budget.

7 - Remediation management

Finding and fixing deficiencies in a timely manner is often one of the most challenging issues facing IT security teams. An IT GRC solution should be enabled for automated integration with third party ticketing systems (such as Remedy, HP® Service Desk or Altiris™ Service Desk from Symantec). Such integration will help ensure that problems with vulnerabilities, patches, and configurations are quickly corrected. For example, when a deviation from technical standards is detected it would initiate an automated remediation ticketing process. Automating these procedures based on risks and policies leads to higher levels of IT service, lower costs and improved customer service.

8 - Flexible reporting and analytics

IT GRC solutions with flexible reporting options can offer a clear view of your IT risk and compliance posture, from a top-level view to the most granular of details based on your unique business needs. For example, executive dashboards may show high-level trend and status views providing data for effective business and financial decision-making. Whereas technical reports may include detailed, actionable information on specific controls to drive remediation efforts. These reports should combine checks on technical controls such as password renewals, and patch updates with procedural assessment responses, such as those confirming employee awareness of security policies. In addition, it should be possible to pull relevant third party data into reports to provide a more comprehensive view of your IT environment, including asset and controls data from other devices and applications, such as firewall logs or vulnerability assessment data.

By automating the reporting process, you can trim significant labor and consulting costs from your IT budget. Comprehensive reports can also serve as auditable evidence of your compliance posture.

Conclusion

As you evaluate IT Governance, Risk and Compliance solutions, bear in mind that only a holistic, integrated approach will allow you to manage *all* aspects of your IT risk and compliance challenges. By evaluating potential solutions against the eight requirements outlined in this paper, you can better enforce your IT policies and improve your overall security posture, while controlling costs.

About Symantec

Symantec is a global leader in providing security,
storage and systems management solutions to help
consumers and organizations secure and manage
their information-driven world. Our software and
services protect against more risks at more points,
more completely and efficiently, enabling
confidence wherever information is used or stored.

For specific country offices
and contact numbers, please
visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com