Leveraging a Maturity Model to Achieve Proactive Compliance
Leveraging a Maturity Model to Achieve Proactive Compliance

Contents

Introduction ......................................................................................................................... 1
Characteristics of Companies with Mature Processes .................................................. 2
Compliance Challenges.................................................................................................... 3
Capability Maturity Model as a Framework .................................................................. 3
The Path to Maturity ......................................................................................................... 4
Leveraging the Maturity Model to Achieve Audit Cost Savings ................................. 7
Conclusion ..................................................................................................................... 8
Appendix 1 ...................................................................................................................... 9
Introduction
Traditionally IT has been evaluated based on its ability to support business processes and applications that directly impact customer retention, sales, revenues and profits. Although valid, this point of view is now under siege as most organizations today face significant risks to their business stemming from loss or theft of confidential data, disruptions caused by IT downtime and potential compliance deficiencies. Whether it is a matter of protecting information, assuring system availability or responding to audits, in today's interconnected world IT must simultaneously manage both opportunity and risk.

Given this situation, mature organizations now view compliance within the context of their overall risk profile. This view necessitates a shift from a tactical, reactive mindset to a more strategic, proactive approach to compliance.

Proactive compliance describes an innovative new way of thinking about how to demonstrate compliance with industry regulations and standards, achieve IT best practices and meet internal audit requirements. Rather than focusing exclusively on the immediate need to pass an audit, proactive compliance entails looking beyond the audit and leveraging compliance efforts to drive IT operational excellence. By deploying the right mix of planning, tools and resources, a program of proactive compliance enables organizations to spend less on compliance, reduce audit deficiencies, improve system availability and strengthen data security.

Unfortunately, for most organizations the reality is quite different. Facing an increasing number of regulatory requirements, tight budgets and limited resources, many companies adopt a highly reactive approach to compliance. They resort to checklists and struggle to deploy ad hoc controls in response to regulatory gaps with little or no formal oversight of IT. According to recent research, these organizations typically experience higher compliance costs, more audit deficiencies, more business downtime due to IT failures and greater risk of confidential data loss.

This paper examines how organizations can use a Capability Maturity Model to help achieve proactive compliance. It explores how an organization can move from the lower levels of the model, where the focus is typically on process alignment and mechanisms for assessing risk, to the higher levels where the needs of CIOs, CISOs and Compliance Managers are met through a combined focus on system availability, data security and compliance. Drawing on recent research from the IT Policy Compliance Group, the benefits of such operational excellence are quantified. Each level of the Capability Maturity Model is described, including recommendations for moving up to the next level. Guidelines are also provided for solutions to be adopted at each level in support of these recommendations. Finally, this paper highlights how one Fortune 500 company realized significant cost-savings in the areas of audit scoping, preparation and testing as it moved towards adopting a truly proactive approach to compliance.
Characteristics of Companies with Mature Processes

Not surprisingly, research from the IT Policy Compliance Group confirms that companies with mature compliance practices have become successful at passing audits by establishing a focus on operational excellence. These companies have learned that improvements to system availability and data protection not only facilitates compliance but can also pay big dividends:

1. **Less spent on compliance:** Most companies spend too much on the wrong compliance practices and not enough on the right ones. As a result, their overall cost of compliance is relatively high. By contrast, companies who reach compliance maturity have aligned spending with practices that are delivering results. They realize an average 52 percent annual reduction in audit expenses and 38 percent annual reductions in overall spend (i.e. audit expenses and security).¹

2. **Fewer audit deficiencies:** Audit deficiencies decline significantly as compliance capabilities mature. For example, organizations operating at an *ad hoc* level typically face 12 audit deficiencies.² Firms who achieve compliance maturity average two or less.³

3. **Lower financial impact from IT disruptions:** Companies with a mature compliance practice experience reduced financial impact from business disruptions caused by IT downtime. Companies operating at the lowest level may experience a 1 to 9 percent loss of revenue, depending on the operational impact of the disruption. By comparison, companies operating at the highest level experience only a 0.03—0.3% loss of revenue.⁴

4. **Less risk from loss or theft of sensitive information:** Finally, compliance maturity is also associated with dramatically lower financial risks and capital losses caused by the loss or theft of customer data. Companies operating at Level 1 experience losses amounting to 8 percent of revenue due to loss or theft of data compared with losses of 0.5 percent of revenue for companies operating at Level 5.⁵

¹ IT Policy Compliance Group; http://www.itpolicycompliance.com/
³ Ibid.
⁴ Ibid., p. 63.
⁵ Ibid., p. 63.
Compliance Challenges
Compliance today represents a more difficult and various set of challenges than ever before. While facing an increasing number of requirements, most organizations spend more than they should on compliance, and reap less than optimal results.

- **Complex, competing demands.** Multiple, often overlapping regulatory requirements make it hard to keep up and can lead to costly duplication of efforts. In a recent survey by IT Policy Compliance Group, 70 percent of all respondents reported being subject to multiple compliance mandates as well as contractual obligations and industry standards. The adoption of industry-standard best-practice frameworks and the trend towards more frequent internal audits further complicate the already difficult task of staying ahead of the compliance curve.

- **Costly manual processes.** The manual compliance methods used by many organizations pose significant problems in terms of cost, scalability and reliability. Yet, according to the IT Policy Compliance Group, most companies have not yet replaced the bulk of their manual processes with automation. In fact, 52 percent of large enterprises and 62 percent of enterprises automate less than 50 percent of their controls. At the same time, these organizations are generally overspending on compliance due to their high investment in manual procedures in an effort to pass audits.

- **High risk of compliance deficiencies.** Many companies are at high risk of compliance deficiencies due to a lack of visibility into their IT environments. With multiple systems for different platforms, regions and business units, they are often unable to identify and measure the relevant IT information, much less prioritize compliance risks. The problem is compounded by the fact that audits firms themselves are often stretched thin, and many projects are now run by auditors with relatively little experience of the audit process. These novice auditors may interpret regulations too literally, commit rookie errors or respond to initial setbacks by probing deeply, making it even more difficult to demonstrate compliance. Organizations lacking clear visibility into their IT controls often find themselves at the mercy of these auditors-in-training—and run a proportionately higher risk of compliance deficiencies.

By taking a more proactive approach to compliance, companies can arm themselves with detailed knowledge of policies and controls and prepare themselves to confront any audit issues that may arise. In the following section we will examine how this can be achieved by following a Capability Maturity Model to help organizations move from an ad hoc to a proactive compliance posture.

**Capability Maturity Model as a Framework**
The Capability Maturity Model used in this paper is designed specifically to help companies to gauge their security and compliance practices not just in terms of passing an audit, but in the larger context of achieving IT best practices. Primary benchmark research conducted by the IT Policy Compliance Group during the past two years has resulted in a Governance, Risk and Compliance Capability Maturity Model (GRC CMM) with specific practices associated with each maturity level.

The scale employed for the GRC CMM borrows from prior research, including significant contributions made by ISACA and the IT Governance Institute. Against this scale, the business results, financial losses, financial risks, business disruptions,
and regulatory compliance experience of more than 2,600 firms have been mapped, from worst (Level 1) to best (Level 5) results.

**Figure 1:** Illustrates the model’s five levels. Moving from left to right, an organization progresses from ad hoc audit practices at Level 1 through increasingly well defined processes and procedures to Level 5, where compliance practices are automated and optimized. Progress is always accompanied by learning. As organizations progress from level to level, practices that improve results are reinforced, while those that do not are discarded or de-emphasized.

---

**The Path to Maturity**

No company magically morphs from Level 1 to Level 5. Indeed the path to maturity requires commitment, knowledge, tools and resources. In this section, we will explore how organizations can successfully move through the maturation process. For each level, we will examine how an organization typically views and handles the audit process. We will also highlight what needs to be done to move up to the next level.

**Level 1—Initial (Ad Hoc)**

At Level 1, IT initiatives are based on the changing needs of the business, and problems are resolved on a project basis with teams formed and dissolved as needed. Much time and energy is spent trying to identify issues, assess specific risks and make information available to address gaps in understanding or support audit escalations. Routine governance activities do not take place. Compliance processes are not documented. In fact, no one realizes that more formalized oversight of IT is required.

To move on from this level, the focus must be on minimizing exposure and reducing audit risks. According to research conducted by the IT Policy Compliance Group, the number one cause of audit failure within organizations is lack of
employee awareness. To reduce audit risks, clearly it is crucial to ensure that everybody within the organization fully understands what is included in an audit scope and what their individual responsibilities are.

**Recommendations for Level 1:**

- Compare existing policies already in place with a comprehensive list of industry-specific policies to identify potential policy gaps
- Establish and communicate any new policies to comply with industry regulations or standards
- Track policy acceptance to ensure users have read the policies and acknowledged accountability
- Conduct formalized training on what is included in the audit scope
- Gather attestation evidence to show that those who needed to complete audit scope training have done so and are fully aware of their responsibilities

**Level 2—Repeatable**

For organizations operating at Level 2, audit requirements are typically managed on a case-by-case basis using repeatable but intuitive procedures and practices with limited involvement from business stakeholders. This is reflected in the typical audit response, which can be characterized by a costly and inefficient cycle of testing, failing, fixing and retesting.

To progress beyond this level, organizations must identify assets that are in scope for the audit process and begin to focus on **standardization**. Standardization requires enforcing unified data protection policies across servers, networks and endpoints. By standardizing controls for their assets and monitoring their IT environment, these organizations will be able to handle audit requests more efficiently.

**Recommendations for Level 2:**

- Standardize on how endpoints (laptops, desktops and servers) are protected from network, web and other forms of malware attacks
- Provide a means of identifying endpoints which are missing patches or have security vulnerabilities (e.g. weak passwords) so that they can be flagged for remediation efforts
- Identify critical servers that may need higher levels of protection such as those containing proprietary or highly confidential information (e.g. PCI-regulated servers housing customer credit card data)
- Standardize on how these critical servers are protected and monitor them on a daily basis to identify systems that should be locked down in response to malicious activity or unplanned changes

**Level 3—Defined**

Significant progress has already been made by organizations that reach Level 3. The focus has now moved beyond standardizing configuration settings to finding an effective means of gathering the necessary information to test against these standards and gather audit evidence. This is where **automation** comes into play.
Companies who automate their compliance processes not only significantly reduce audit costs and test time; they also have easy access to data needed to generate audit reports. Auditors are generally more favorably disposed towards automation as a means of gathering data since it eliminates inevitable errors incurred through manual processes.

**Recommendations for Level 3:**

- Automate the process of mapping technical and procedural controls to policies
- Automate the distribution of patch updates for known vulnerabilities in operating systems and applications
- Automate the archival of emails in compliance with company policies. Provide an easy means of classifying, organizing and managing this electronic data so that in the event of a legal liability issue, email archives can easily be searched and evidence gathered as proof of compliance. This reduces both organizational risk and the cost of incident responses.
- Automate the process of server backups to ensure they are being managed in a consistent manner and in accordance with compliance controls
- Provide the ability to automatically enforce data security policies and notify employees of violations in order to change behavior and pinpoint compliance gaps in existing business processes
- Gain visibility into who has access to this exposed data and automatically check whether the machines housing the data are adequately protected (i.e. have strong passwords and the latest patch updates)

**Level 4—Managed**

At Level 4, organizations turn their attention towards creating a managed network. This involves monitoring the network to keep systems constantly available and fully operational. A managed network requires real-time visibility into the latest security threats and the ability to prioritize necessary remediation efforts.

Benefitting from the standardization and automation applied at previous levels, organizations at Level 4 can easily access data to demonstrate how they are not only complying with audits but also protecting their networks. The challenge is to figure out how this information can be delivered in comprehensive reports for multiple audiences from executive-level dashboards to detailed IT reports on control deficiencies.

**Recommendations for Level 4:**

- Provide the ability to view security incidents in real-time across the entire IT environment and correlate security events to discover root causes and prioritize remediation efforts
- Combine data from multiple places in the network and deliver role-based dashboard reports to demonstrate proactive compliance and drive necessary remediation efforts

**Level 5—Optimized**

By Level 5, an organization has effectively developed a self-healing system. This system is characterized by an ability to automatically identify security and compliance risks as they arise and correct them in real-time.
Symantec offers a full portfolio of solutions and services that enable organizations to move through these different stages of the Capability Maturity Model towards a truly proactive compliance posture (see appendix 1).

**Leveraging the Maturity Model to Achieve Audit Cost Savings**

The path from Level 1 through Level 5 in the Capability Maturity Model is a continuum. At each new level, an organization can dramatically improve its IT processes, leading to greater success in passing audits and significant cost savings. These savings can be experienced in all three key stages of the audit process—scoping, preparation and test of design and execution.

**Figure 2:** Maps the progress made by one Fortune 500 company (Company X) as it moved through the Capability Maturity Model refining its audit processes accordingly. The data is based on findings produced by the company’s auditing firm.

Audit Scoping

Auditing firms typically find that their customers spend 25-30 percent of year-one compliance budgets on audit scoping. Scoping involves figuring out what needs to be audited, who the stakeholders are and what technology supports the key processes. Each year, effort spent to revisit the scope for new audits is often the most time-consuming and yet wasteful part of the audit because previous year’s efforts are rarely leveraged.

Company X successfully managed its audit scoping costs by formalizing user accountability at the start of the audit process through policy awareness, training and communication. Additionally, prior year scoping efforts were fully leveraged and improved, leading to a 50 percent reduction in the overall costs of audit scoping.

Audit Preparation Time
Once the scope has been determined, gathering the necessary evidence can also be very time-consuming. During the first year of compliance activities, auditing firms typically find that customers dedicate about 50 percent of their effort to producing the documentation necessary to pass an audit.

By standardizing control output and implementing ongoing control assessments and reports, Company X was able to realize a 50 percent reduction in audit preparation time, saving both money and resources.

**Audit Test of Design and Execution**

Finally testing for adequate design and execution of the key controls typically makes up the final 20-25 percent of audit efforts. As organizations move through the maturity model, testing of controls becomes more formalized and in some cases is automated. This allows them to quickly identify measures that need to be taken to achieve regulatory compliance and reduce IT risks.

Company X was able to achieve this status, resulting in a 60 percent reduction in test of design and execution and 100 percent elimination of additional test rounds.

**Conclusion**

Done properly, proactive compliance will result in an ongoing continuum of well-documented, well-planned security. This can be achieved by using the Capability Maturity Model as a framework and leveraging the powerful Symantec portfolio of security and compliance solutions. Organizations that attain this level of maturity can benefit from reduced audit costs and risks, improved overall security posture and the ability to operate with greater confidence in the digital world.

For additional information on Symantec products and security offerings, please call 1 (800) 721 3934 or +1 (408) 517 8000 outside the U.S.
## Appendix 1

<table>
<thead>
<tr>
<th>Maturity Model Levels</th>
<th>Symantec Solutions and Services</th>
</tr>
</thead>
</table>
| **Level 1**           | • Symantec™ Control Compliance Suite  
                        | • Symantec Security Awareness Training |
| **Level 2**           | • Symantec™ Endpoint Protection  
                        | • Symantec™ Control Compliance Suite  
                        | • Symantec™ Network Access Control  
                        | • Symantec™ Critical Systems Protection |
| **Level 3**           | • Symantec Control Compliance Suite  
                        | • Altiris™ Patch Management  
                        | • Symantec Enterprise Vault™  
                        | • Symantec NetBackup™  
                        | • Symantec™ Data Loss Prevention |
| **Level 4**           | • Symantec™ Security Information Manager |
| **Level 5**           | • All of the above solutions |
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

Copyright © 2009 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

NO WARRANTY. The information in this document is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the information contained herein is at the risk of the user. This document may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.
11/2009 20700020