Gartner

ITScore Overview for Security and Risk Management

Analyst: *Paul E. Proctor*

Summary

Good security and risk management requires mature business continuity management, compliance, identity and access management, information security management, privacy, and risk management practices. Enterprises should periodically assess and improve their maturity in all these areas.

Overview

A program maturity assessment is crucial to identifying gaps and risk across six security and risk management domains. IT and business professionals in these areas can use the Gartner-developed ITScore methodology and its accompanying diagnostic tool to make crucial advances in the maturity of their programs and practices.

Key Findings

- Improvements in maturity across six security and risk management domains means moving beyond a technology-centric approach to one that takes into account the enterprise's business requirements and associated risks.
- Reaching the highest level of program maturity may not be possible, but continuous process improvement to advance maturity levels is possible and necessary.
- As maturity improves in each of these risk-related programs, the risk posture of the organization also improves, leading to reduced costs and improved performance.

Recommendations

- Use the Gartner-developed ITScore methodology to evaluate and improve program and process maturity across six key security and risk management domains.
- Work to extend activities in these areas beyond a narrow IT-centric focus to align with key business needs and associated risks.

Analysis

Gartner developed the ITScore maturity assessment framework to enable IT professionals and business leaders to assess the maturity of a wide range of enterprise roles, domains and functions. The ITScore system has been applied to six domains that are specific to the security and risk management role, including business continuity management (BCM), compliance, identity and access management (IAM), information security, and risk management. The ITScore methodology and the accompanying diagnostic toolkits — which are presented in six separate domain-specific research documents — can be used to determine current and desired maturity levels in each of these domains, as well as improve the maturity of the programs and practices.

The ITScore methodology is consistently applied across all roles and domains, but the dimensions measured for each are, inevitably, diverse and specific to the requirements of each role and domain. For example, the characteristics of a given maturity level for compliance are very different from those for risk management, and the recommendations for improvements — the actions that need to be taken to the next level of maturity — are very different for privacy and BCM. Nonetheless, certain broad, common themes can be identified across all these domains. One of these common themes is the need to move beyond traditional IT-centric approaches, and in fact, beyond the IT organization, to reach the entire enterprise. Another is the need to formalize programs and practices. Still, another — perhaps the most important of all — is to align practices in these areas with the identified requirements of the business.

An ITScore-based methodology assessment represents an evaluation of a risk and security program compared against key indicators of maturity, which encompass management processes, personnel and organization, technology and

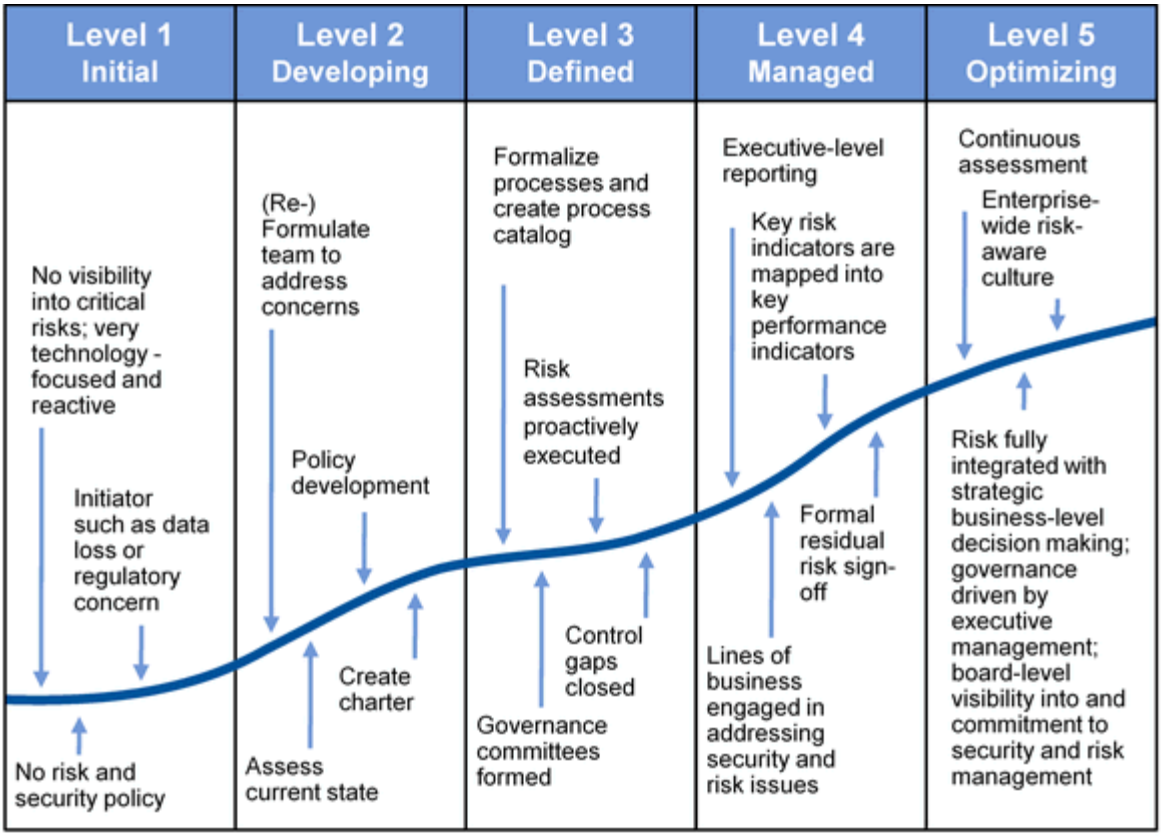
tools, and business culture. Gartner has identified five maturity levels — aligned with our established maturity levels — that represent increasing capabilities. It is important to note that the highest levels of compliance maturity may not necessarily be attainable — or even desirable — for all enterprises. However, the process of continuous improvement that ITScore makes possible can deliver significant improvements in each of these domains, can significantly reduce enterprises' risk exposure and, in some cases, may also deliver improvements in the effectiveness and efficiency of related business processes.

Overview of ITScore Maturity Levels

- **Level 1: Initial.** Whatever processes exist are likely to be ad hoc, disconnected, disorganized and IT-centric. There may be general awareness of the need for improvements, but no formal responsibilities have been assigned and no formal program is in place.
- **Level 2: Developing.** There is limited but increasing recognition of the need for a formal program, and management commitment has likely been secured. Requirements are being assessed, responsibilities are being assigned, and an implementation plan is being developed. Communication and awareness efforts are beginning.
- **Level 3: Defined.** The scope and objectives of an enterprisewide program have been established, and processes and performance metrics have been defined. A formal program is now in place, with an identified leader and clear commitment from senior management and other key stakeholders (for example, line-of-business managers).
- **Level 4: Managed.** Most identified gaps have been closed. Decisions about program activities are based on input from stakeholders enterprisewide and are designed to address the clearly identified needs of the business and, particularly, risks associated with those activities.
- **Level 5: Optimizing.** The program is now recognized as a strategic business imperative enterprisewide. Accountability for associated risks rests with line-of-business owners, who explicitly accept ownership of residual risk.

Figure 1 gives an overview of the five security and risk management maturity levels.

Figure 1. Overview of ITScore Maturity Levels for Security and Risk Management



Source: Gartner (August 2010)

How to Use This Assessment

The ITScore diagnostic tool can be used to perform an initial compliance maturity assessment and then — on a quarterly or at least annual basis — to track improvements in maturity. The results can be used in:

- Improving the enterprise's visibility into the program and its associated risks
- Identifying gaps in the program and related controls
- Demonstrating, to senior management and other stakeholders (who may be either internal or external), the value of maturity improvements and justifying the costs of the program
- Making necessary changes in organization structure to support maturity improvements
- Communicating with different target audiences inside and outside the enterprise
- Identifying potential areas where improved maturity can enable more-efficient, more-effective business processes

Risk Management Maturity

The maturity of an enterprise's IT risk management program is a key indicator of the effectiveness and efficiency of its overall risk posture. Improving risk management maturity is fundamental to improving the cost-effectiveness and business alignment of the enterprise's risk activities, but these improvements require different actions, depending on the current maturity level of the risk management program. In the absence of a realistic and actionable understanding of the current state of its IT risk management program, the enterprise cannot identify business-critical risks to its processes and operations, identify and close gaps in its risk controls, improve its program maturity, and justify the not-inconsiderable costs of IT risk management.

Privacy Maturity

Enterprises worldwide increasingly recognize the critical importance of privacy protection as a business discipline. The failure to protect personal information (such as name, address, date of birth and telephone numbers) and, especially, sensitive information (for example, health data, religious affiliation and political opinions) from misuse or exposure can expose the enterprise to profoundly damaging consequences, whether the failure is caused with malicious intent or only accidentally. The consequences range from regulatory action to legal liability to reputational damage resulting in the loss of customers, partners or employee confidence. The level of privacy protection and overall privacy maturity varies widely from enterprise to enterprise, from industry to industry, and from region to region.

Compliance Maturity

Enterprises, their business leaders and their IT organizations have historically seen compliance as a comparatively simple "checklist" function — a matter of ensuring that applicable regulatory requirements have been met. Regulatory mandates, and, particularly, the financial reporting requirements of the U.S. Sarbanes-Oxley Act, have certainly focused intense attention on compliance in recent years. Many enterprises have found Sarbanes-Oxley compliance alone to be an overwhelming undertaking. However, this narrow focus on regulatory mandates, understandable though it may be, has caused many enterprises to neglect other critical components of compliance. And no enterprise can achieve an acceptable level of compliance maturity until it recognizes all the critical components of compliance — regulatory, commercial and organizational — and addresses them in an enterprise-specific manner.

Security Maturity

Most enterprise leaders recognize the benefit of information security maturity. The growing awareness of the need for robust, mature security practices to protect business-critical IT systems and data is constantly reinforced by media reports about security, by regulatory or other compliance requirements, or by a damaging data breach affecting the enterprise itself. Another important driver of growing concern about information security maturity is enterprises' ongoing search for better forms of management — and, specifically, better alignment between what the business needs and what the IT organization does.

Identity and Access Management Maturity

Managing users' identities and entitlements has become increasingly complex as systems, applications, and endpoint access programs multiply and as enterprises allow employees, contractors, partners, suppliers, and customers greater access to their systems and data. At the same time, enterprises face increasing pressure to ensure that they manage users' identities and access in compliance with new legislation and regulations — and to be able to demonstrate that they are doing so. Many large enterprises have tried to reduce this complexity and address compliance issues through

a variety of technology projects. These projects are often disjointed and poorly aligned, and the enterprise finds itself struggling with another layer of complexity without realizing any clear business value.

Business Continuity Management Maturity

BCM is increasingly recognized as a mission-critical function for most enterprises. There are three main drivers for this broad awareness of the importance of BCM — 24/7 service delivery requirements, globalization, and increasing natural and man-made risk — and they are expanding the scope of BCM well beyond its roots in IT digital rights management (DRM). Enterprises must concern themselves with much more than the need to restore their data centers following a natural disaster such as a hurricane or an earthquake. They must also take into account regulatory and other compliance requirements, reputational damage, and maintaining the confidence of customers, business partners and the financial markets. They must also ensure that their BCM efforts are cost-effective and sustainable. For all these reasons, virtually every enterprise needs to make a serious, sustained effort to advance its BCM maturity level.