Gartner

Research

Publication Date: 29 January 2010 **ID Number: G00173779**

Eight Practical Tips to Link Risk and Security to Corporate Performance

Paul E. Proctor

Boards of directors want to know that the organization is protected against reasonably anticipated risk. We provide case studies and tips on how to align risk and security with the business strategy, and communicate to business executives the benefits of effective risk management.

Key Findings

- The plethora of operational risk and security metrics are extremely valuable for internal operations, but they have little value to business decision makers.
- A formal program will look good to executives and makes better use of the attention that security receives following an attack before that attention inevitably fades.
- Many enterprises still take a narrow, "siloed" approach to risk assessment and management.
- Many organizations regress in their security programs' maturity practices. Reasons include lack of communication, loss of focus, too much focus on technology solutions and complacency.

Recommendations

IT risk and security organizations:

- Formalize an IT risk and security program.
- Measure your program's maturity.
- Use a risk-based approach.
- Use leading indicators of risk conditions.
- Map key risk indicators (KRIs) to key performance indicators (KPIs).
- Link risk initiatives to corporate goals.
- Don't use operational metrics in executive communications.
- Communicate to executives, emphasizing what works and what doesn't.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1.0 Introduction

The board of directors wants to know that the organization is protected against reasonably anticipated risk. CIOs, chief information security officers (CISOs), chief risk officers (CROs) and risk management officers (RMOs) struggle with how to link risk management efforts in security, privacy, business continuity and compliance to the value they provide at line-of-business and executive levels. A handful of companies have figured out how to effectively communicate to business executives the benefits. These eight practical tips can get you started in addressing this challenge at your organization:

- Tip No. 1: Formalize an IT risk and security program.
- Tip No. 2: Measure your program's maturity.
- Tip No. 3: Use a risk-based approach.
- Tip No. 4: Use leading indicators of risk conditions.
- Tip No. 5: Map key risk indicators to key performance indicators.
- Tip No. 6: Link risk initiatives to corporate goals.
- Tip No. 7: Don't use operational metrics in executive communications.
- Tip No. 8: Communicate to executives, emphasizing what works and what doesn't.

1.1 Case Study: Reporting IT Risk and Security to the Board of Directors

Since 2007, Gartner has seen an increase in the number of clients requesting guidance on how to address risk and security issues with the board of directors. Many enterprises follow a similar path. The CISO (a direct report to the CIO) receives a call requesting a short overview of risk and security for the board of directors with only a few days to prepare. This is the first such request from the board in several years. Challenges include fighting the urge to panic, sorting through the plethora of available information for the nuggets of interest to present to the board, coordinating the input of multiple direct reports, and rationalizing the results of recent risk assessments.

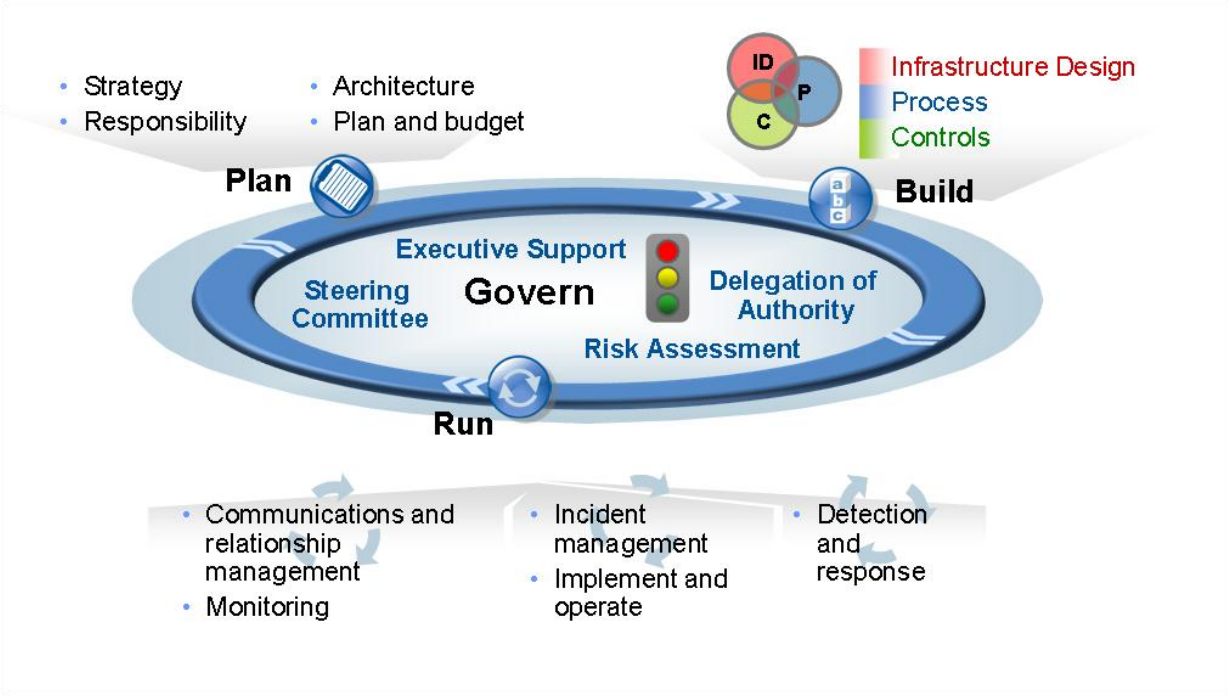
The approach that the security officers should take includes linking risk and security activities to corporate initiatives and avoiding fear, uncertainty and doubt. A four-slide deck should be created with an emphasis on what is working and what is not working in the security program. The CISO should also bring 20 backup slides that provide greater detail and operational metrics.

Boards value transparency. Effective reporting delivers visibility into the organization's risk posture so that it can make more-effective business decisions.

2.0 Tip No. 1: Formalize an IT Risk and Security Program

Organizations must formalize their IT risk and security programs to develop business relevance. A formalized program is one that is repeatable and measurable. Figure 1 shows the Gartner Security and Risk Management Activity Cycle. The activity cycle is a representation of a formal program organized around the govern, plan, build and run phases (see "Activity Cycle Overview: Security and Risk Management Professionals").

Figure 1. Gartner Security and Risk Management Activity Cycle



Source: Gartner (January 2010)

- **Govern phase:** Governance defines the decision-making authority and accountability for encouraging desirable behavior. This phase is composed of governance, risk and compliance processes that establish a link between the business and the risk it accepts through an effective delegation of authority, and the execution of program maturity assessment. Governance, risk and compliance requirements cross all risk-based functional roles and include executive reporting and support, delegation of authority, program maturity assessment, steering committee reporting, charter creation, risk assessment, communications, remediation, and testing.

- **Plan phase:** A consistent strategic and organizational model will drive effective tactical planning and annual planning. Risk and security professionals must develop a long-term vision for their programs, ensure that all roles and responsibilities are assigned and accepted, and create an annual plan with quarterly objectives. Annual planning should precede the annual budget proposal process, and the annual plans for the different components of risk and security should be related to the enterprise's risk management strategy. Architecture provides the guiding principles for the implementation of controls, formalizes traceability between the business strategy and security decisions, and facilitates interoperability.

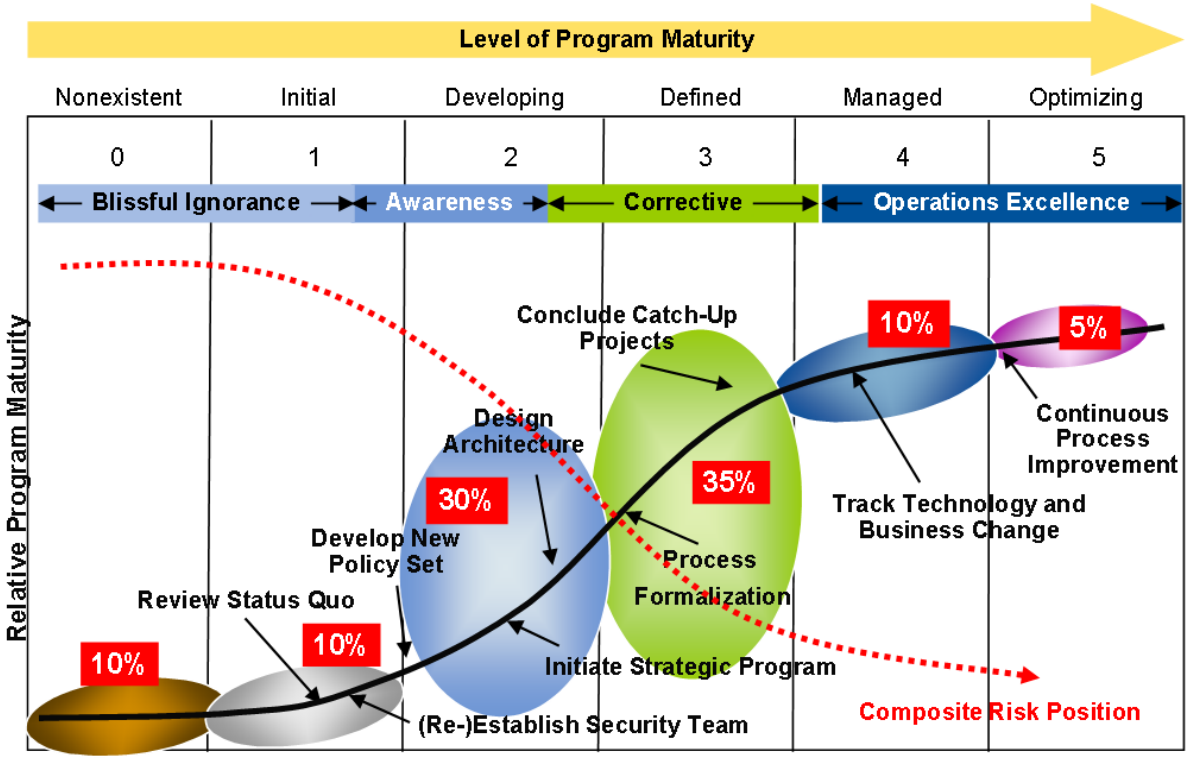
- **Build phase:** In the build phase of the Gartner Activity Cycle, the common strategic initiatives are controls, policy, infrastructure design and process formalization. At the same time, each functional role has its own unique requirements. Controls are elements that are implemented to protect the organization from a reasonably anticipated risk; examples include firewalls, acceptable-use policies, financial close processes and password aging. Process formalization drives the maturity of any program. The build phase also encompasses infrastructure design and technology selection.

- **Run phase:** The run phase of the Gartner Activity Cycle represents the operating elements of the program, and it includes incident management, operations, implementation, enforcement and monitoring. The run phase is where most of the budget is spent, while the other three phases ensure that the budget is spent appropriately.

3.0 Tip No. 2: Measure Your Program's Maturity

A formal program can be measured using a maturity scale. Figure 2 illustrates the Gartner analysis of the aggregate maturity position achieved by Global 2000-type organizations through 2009. This illustration uses the Gartner maturity timeline representation as the basis, integrating traditional maturity phases with the Gartner-defined maturity levels. The black arrows represent the milestones an organization meets as it matures; the large colored bubbles represent the maturity of organizations in the Gartner client base.

Figure 2. Security Program Maturity Timeline, 2009



Note: Population distributions represent typical, large, Global 2000-type organizations.

Source: Gartner (January 2010)

Not all organizations complete the maturity journey. Many organizations regress in their practices. Reasons for falling back in maturity include:

- The progress and value of the program are not effectively communicated, resulting in premature budget cuts.
- Organizations lose focus, with projects going down the wrong tracks, resulting in rework.
- Leadership changes, resulting in new managers wanting to establish their own, new regimes.

- There is too much focus on technology solutions at the expense of the "softer" issues, such as process, policy, awareness, governance and culture.
- There is a general return to complacency, resulting from reduced pressure that comes from less publicity about security incidents and compliance issues.

These factors result in many organizations bouncing back and forth between the awareness and corrective phases (see "Security Program Maturity Timeline Update, 2009").

3.1 Case Study: General Dynamics

General Dynamics is an extremely diverse, highly decentralized global conglomerate with more than 80,000 employees. The company's decentralized structure and the sensitivity of its position as a defense contractor have made it extremely challenging to design effective enterprisewide information security policies and practices (see "General Dynamics' ISRB Sets a New Standard for Enterprise Security Governance").

In March 2005, General Dynamics' systems came under a severe, sustained attack that was highly sophisticated and very well-organized. In April, its newly appointed CIO, Tommy Augustsson, established a "red team" — a multidisciplinary, cross-organization group of business leaders, technical specialists and others who were tasked with assessing the entire company's state of security readiness, identifying weaknesses, determining acceptable levels of risk and proposing necessary changes.

Following the review, General Dynamics significantly altered its governance processes for information security. It established the information security review board (ISRB), which reports directly to the CEO and has enterprisewide responsibility for security policies and practices. The ISRB ensures that information security governance efforts have commitment at the highest levels. It involves stakeholders from many different business units, disciplines and skill sets. It also establishes clear accountability for security practices and decisions.

The efforts of the ISRB have resulted in an overwhelming majority of the company's business units and internal organizations now having green rankings. The ISRB has also become an enterprisewide clearinghouse for security problems and issues. Information security practices are standardized and repeatable, even in a complex technology environment, reducing the time and cost associated with security decisions.

The company's information security practices have reached such a level of maturity that people, not processes or technology, are the primary security concern. For this reason, employee awareness communications have become a more important focus for the ISRB.

While most organizations will not need to reach this level of maturity in their governance processes, they should not ignore the importance of executive involvement in their security decisions. Many organizations are moved to action when they suffer loss from security lapses, but security departments should not wait for such focused attention from executives to move forward in formalizing their programs. A formal program will look good to executives and makes better use of the attention that security receives following an attack before that attention inevitably fades.

4.0 Tip No. 3: Use a Risk-Based Approach

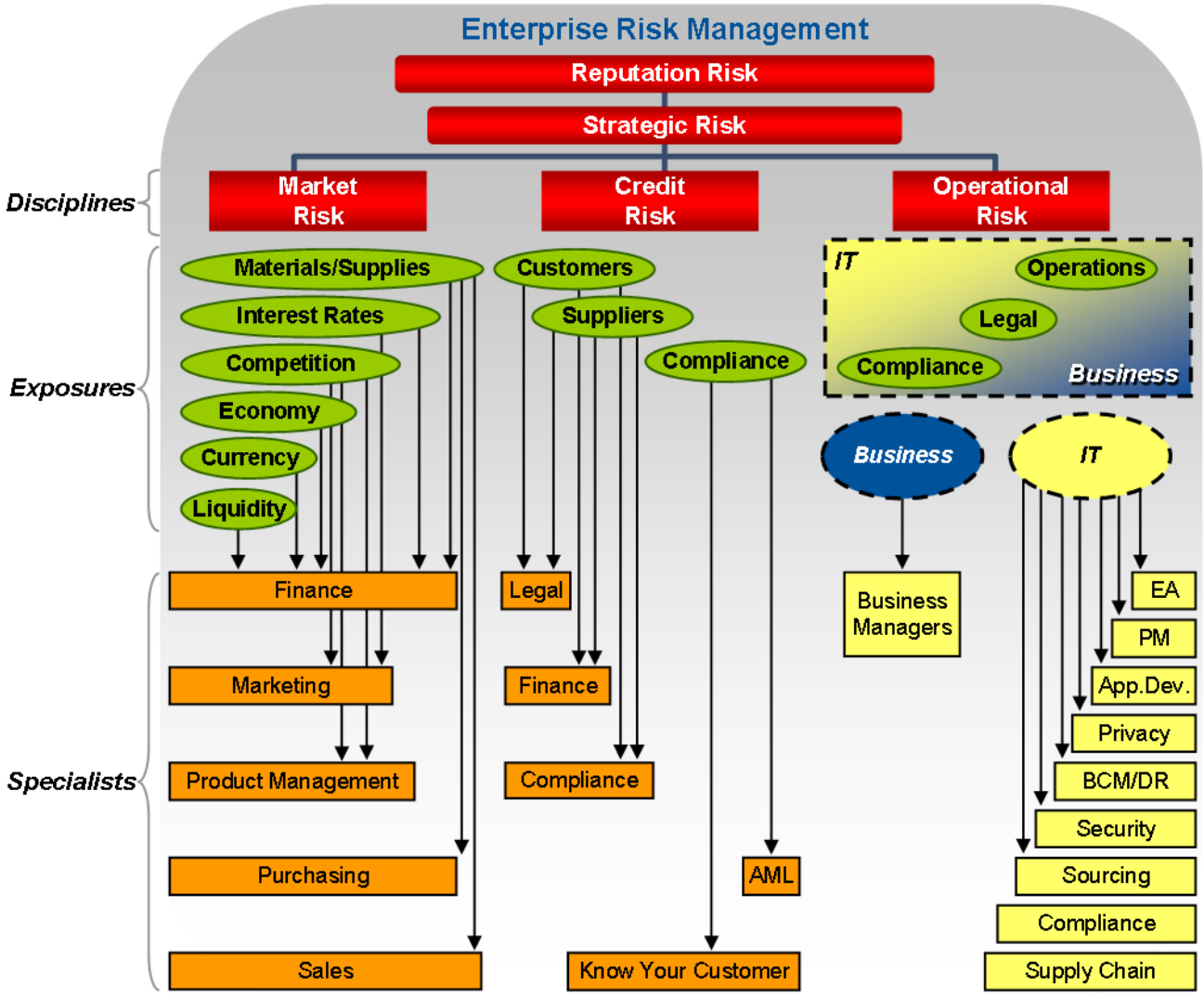
Many enterprises still take a narrow, siloed approach to risk assessment and management. Enterprise managers and IT managers who have risk-related responsibilities can use Gartner's guidance to develop risk practices that are effective and appropriate to their specific needs. There

is no single definition of risk that is appropriate for all enterprises or organizations within enterprises (see "An Overview of IT and Enterprise Risk Management").

Risk and the accountability for risk acceptance are, and should be, owned by the businesses that are creating and managing those risks. IT tools can automate effective risk management processes, but the results delivered by these tools will be only as good as the underlying frameworks, processes and data structures. Risk managers should develop enterprise-specific definitions of risk, as well as an organizational structure that eliminates conflicts and overlaps in responsibilities among all risk-related specialists.

Risk managers should create an overarching risk framework to address the entire enterprise, and they must ensure that staff members at all levels clearly understand their risk-related responsibilities (see Figure 3 and "A Risk Hierarchy for Enterprise and IT Risk Managers"). Risk managers must take a proactive approach to risk assessment and management, so that they are managing risk, not being managed by it. They should also make line-of-business managers, not IT managers or auditors, explicitly accountable for residual risk. By involving operational managers in assessing the effects of risk events on operational performance, the organization will gain a better understanding of and commitment to risk management.

Figure 3. The Gartner Risk Hierarchy for Enterprise and IT Risk Managers



AML = anti-money-laundering; BCM = business continuity management; DR = disaster recovery; EA = enterprise architecture; PM = portfolio management

Source: Gartner (January 2010)

5.0 Tip No 4: Use Leading Indicators of Risk Conditions

A common practice of many operational risk assessment approaches is to consider the likelihood or probability of various risk categories and then determine their financial impacts. Many of these approaches provide limited insight, because broad assumptions are required to make them work. Often, these assessments are generated in a bottom-up fashion and then aggregated into an overall organizationwide risk profile. These assessments require (among other things) a clear and consistent understanding of how operational performance affects financial performance. It is important that the assumptions associated with these cause-and-effect relationships be consistent across the various individual risk event assessments. Furthermore, there must be clear visibility into the "mechanics" of these cause-and-effect relationships.

Most people gravitate toward the use of financial metrics as the primary measure of performance, but these metrics have limited use for our purpose. Financial metrics do not enable businesses to understand and measure how value is created in their organizations. Although financial metrics remain a fundamental measure of value, they represent only the outcomes of business activity: They are lagging indicators of performance. Business managers need a better understanding of the drivers of their business and the nonfinancial metrics that are the leading indicators of financial outcomes.

Gartner has defined and organized a catalog of nonfinancial business performance metrics in the Gartner Business Value Model (see "The Gartner Business Value Model: A Framework for Measuring Business Performance"). These nonfinancial performance metrics will enhance IT-to-business communication by enabling greater precision and meaning in addressing increasingly complex business issues.

Every manager of a risk domain (security, business continuity management, privacy and so on) can look out across his or her business to identify the key business processes and applications that would be negatively impacted by the identified risks. Risk managers should not focus exclusively on IT-centric KPIs. Doing so perpetuates the notion that IT risks relate only to IT. Table 1 describes examples of leading and trailing indicators.

Table 1. Leading and Trailing Indicators

Outcomes	First-Order Derivative	Second-Order Derivative	Third-Order Derivative	Fourth-Order Derivative
Financial measures	Internal indicators	Key risk indicators	External indicators	Weak signals
• Profit • Cash • Company value	• Time to market • Client retention • Cash-to-cash cycle time	• Reputation index • Availability • Unanticipated exception response times	• The Conference Board Leading Economic Index • Industry-specific indicators • Competitors • Supply chain vulnerabilities (key suppliers and key customers)	• Political ticker • Culture • Social patterns • Emerging technology
Trailing indicators	Leading indicators	Leading indicators	Leading indicators	Leading indicators

Source: Gartner (January 2010)

Trailing indicators tell an organization what happened, while leading indicators provide visibility into future outcomes. For example, quarterly financial results indicate only how well the company performed in the previous quarter. A leading indicator, such as the health of the supply chain, is predictive of how the organization will perform in current and future quarters. Organizations need to define new leading indicators of business performance that include both KPIs and KRIs. Knowledge of, and skill in, applying leading indicators of desired outcomes are necessary to manage risk.

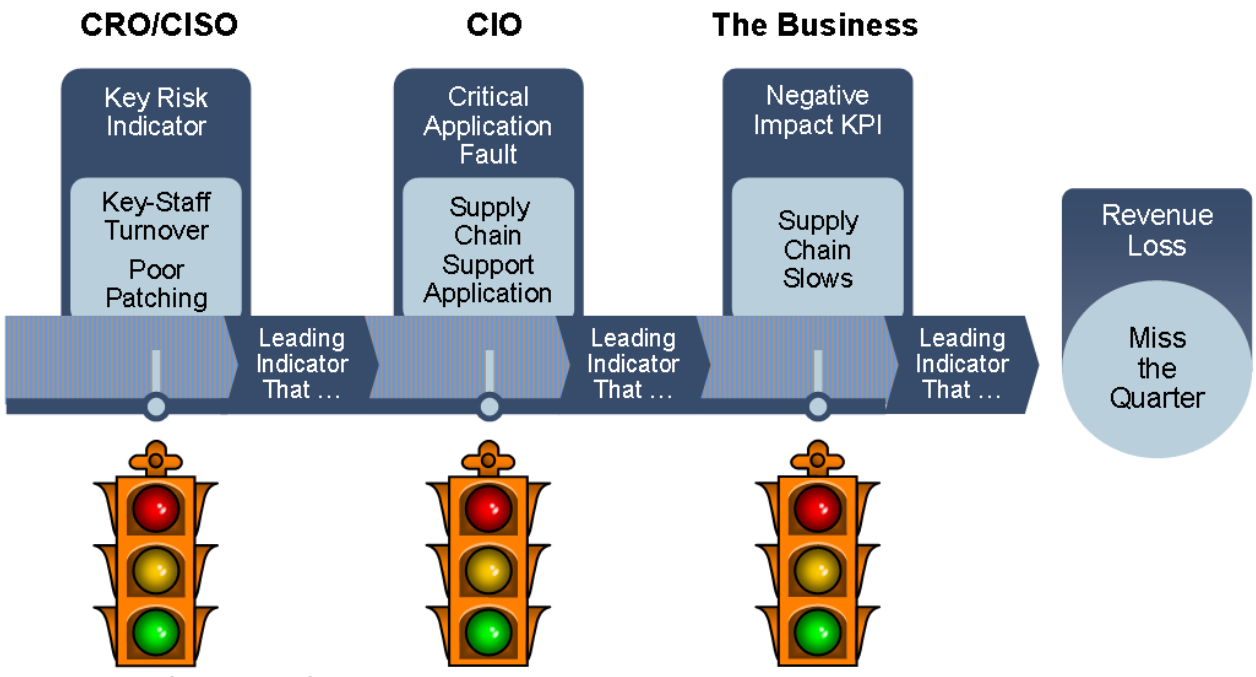
6.0 Tip No. 5: Map Key Risk Indicators to Key Performance Indicators

The relationship between risk management and corporate performance should be conceptually and intuitively obvious, because improperly managed risk can lead to business failures and poor business performance. However, making this relationship measurable has eluded most organizations. As a result, the benefits of many operational risk management activities are not clear to the business people who are most at risk. In addition, they often fail to take advantage of the risk information that is available when making critical business decisions.

To address these issues, enterprises should develop credible, discrete business performance measures, and risk management efforts should produce credible, discrete risk indicators that directly impact those business performance measures. A deeper and common understanding of how risk events affect business performance is needed. KRIs are leading indicators of when business performance is at risk.

A simple example is illustrated in Figure 4. An organization has a KRI that measures patching levels on critical systems, which host supply chain support applications. It also has a KPI that measures the operation of the supply chain. It's important to note that the supply chain KPI is a business metric — not an IT metric. When the patching KRI turns from green to yellow or red, it is a leading indicator that the supply chain may suffer failures or slowdowns. This, in turn, would impact the supply chain KPI, which is a leading indicator that the company may miss a revenue target. This relationship and mapping can demonstrate to business executives why they need to heed KRIs and can help them make better business decisions based on those KRIs.

Figure 4. An Example of Leading Indicators



Source: Gartner (January 2010)

Good key risk indicators are simple and measurable and have a direct impact on multiple key performance indicators. An example of a good KRI is key-personnel turnover. Loss of key

personnel raises risk from the loss of knowledge and the need to replace these people. It raises the risk of accidental loss, lost efficiency and potential segregation-of-duties issues. These risks, in turn, may result in critical-system downtime or failure, failing to meet service-level agreements (SLAs), and/or compliance issues. Any of these could, in turn, impact KPIs such as on-time delivery.

Most organizations have a plethora of operational risk and security metrics. While these metrics are extremely valuable for internal operations, they have little value to business decision makers. Many security and risk management organizations are wasting their time seeking an appropriate presentation of these technical and operational metrics to report up. The only way to succeed is to organize these into a coherent minimal set of credible KRIs that can be mapped to KPIs.

KRIs should reflect the domain of risk for which the group developing the indicator is responsible. Organizations with broad operational or enterprise risk efforts should select and roll up KRIs from individual silos.

The purpose of this mapping is to facilitate conversations and arrive on an agreement on the most relevant measures and their impacts. The mapping should evolve through discussions with risk subject matter experts and appropriate people from the business. This will have the immediate benefit of raising the relevance and awareness of risk management work to the business.

Organizations may be tempted to overemphasize the impact of availability on KPIs. Where possible, balance should be created to reflect other aspects of risk, including threats to confidentiality, integrity, SLAs, the organization and other types of threats. Annex C of ISO 27005 provides a good starter list of threats from physical damage to natural events and the compromise of information that can be used to map the impacts of KRIs to KPIs.

7.0 Tip No. 6: Link Risk Initiatives to Corporate Goals

Using fear, uncertainty and doubt to get executive support does not work. Executives do not want to hear about how bad everything will be if they don't invest in risk management and security. It is equally useless to cite the return on security investments, because investing a dollar/euro in risk and security does not tangibly return a dollar/euro. Demonstrating business value is required, and this can be accomplished by directly linking corporate goals to security initiatives and then reporting progress. Security professionals should seek out sources that discuss stated corporate goals and use them liberally throughout their board communications. Security professionals should use the exact wording in the initiatives, so it is obvious that risk and security efforts are linked to specific initiatives. The higher the importance of the initiative is, the more value it will show to the executives.

7.1 Case Study: A Power Utility Aligns Security Risk With Business Strategy

The security officer of a large power utility company used corporate initiatives and statements of direction to directly link risk and security efforts to the business context. The utility's executives had already created a five-year strategic plan that was rich with guidance and specific terminology. This, in turn, had been used by the CIO to create the IT strategic plan and echoed many of the important business themes from an IT perspective. It was a relatively straightforward exercise to extend those themes and specific initiatives through to the risk and security team's charter, five-year strategic plan and budgeting requests.

The security officer used executive sign-off of the charter to drive executive visibility. This exercise resulted in increased budget and staffing. It also supported major internal initiatives to improve risk and security program maturity.

8.0 Tip No. 7: Don't Use Operational Metrics in Executive Communications

Organizations in Gartner's client base struggle with defining the right metrics to share at the business executive and board levels. Each seems to be seeking the "right" view of operational metrics that will resonate with a business audience. Operational metrics are not appropriate for use at the business executive level, because business people lack the context and training to understand the meaning of operational metrics in a business context.

Operational metrics work well to operate a program, but they will not resonate with business people. Operational metrics should be used with peers and subordinates to manage the effectiveness of a program. Business executives who demand this level of detail without having an understanding of how to apply it are wasting their time and security professionals' time. Certainly, security professionals should provide detail when it is requested, but they should beware of wasting time trying to educate business executives on the relevance of detailed metrics. They should try to provide business executives with information already packaged in a business context.

9.0 Tip No. 8: Communicate to Executives, Emphasizing What Works and What Doesn't

Risk management and security groups face more-aggressive reporting requirements for an audience with increasing levels of sophistication. In a risk-based world, a business-oriented audience wants to know: How protected are we? How much risk are we accepting? What is our risk posture? There are few credible risk posture metrics that resonate with a business-oriented audience. Process maturity is a well-understood discipline in many organizations, so process maturity metrics can provide a foundation to effectively communicate a company's risk posture.

Process maturity can be used as an indirect indicator of risk posture, and the resulting analysis can be used to set project priorities during strategic and tactical planning. This method provides only one view of risk. It provides a credible overview of the risk posture for the enterprise in terms that a high-level audience can grasp. This is a blunt instrument that is complementary to, but does not replace, formalized risk assessments (see "Toolkit Tutorial: Assessing Risk Posture and Setting Priorities Using a Process Maturity Tutorial"). The following sections describe eight steps to use process maturity as an indirect indicator of risk posture.

9.1 Step 1: Develop a Process Catalog

To put each of these steps in context, we'll follow a single key process — incident response — through each of the five steps. First, a process catalog should be developed. In Step 1, incident response would be called out as a key tactical process and formalized. A document would be created that includes a description of the process, a flow chart, an integration matrix, skill and staffing requirements, and definition of roles and responsibilities (see "Security and Risk Process Management Best Practices").

9.2 Step 2: Assess Process Maturity

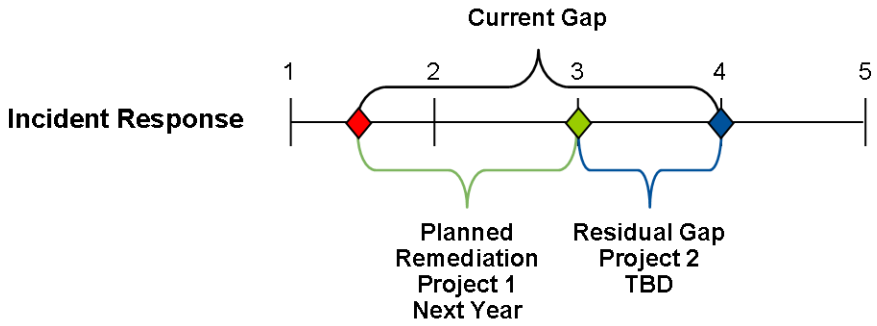
For our incident response process example, an analysis shows a process in disarray that was developed when the organization was much smaller. Although written down, the process is no longer followed. It lacks accountability, and the metrics are not being recorded any longer, so there is little visibility into its effectiveness. It also lacks any automation, so it is entirely manual. Based on these factors, the incident response process is determined to be at Maturity Level 1 (see "Toolkit Best Practices: Assessing Security and Risk Management Process Maturity").

9.3 Step 3: Develop a Process-Maturity-Based Risk Report

To assess the risk posture of the poor incident response process, the organization convenes a group, including representatives from IT, security and the business. The group models the significance of the incident response process through scenarios describing likely events and unlikely events with high impact. The group looks at the current state of the control, and it qualitatively assesses the ramifications of the process's relatively low maturity. One finding is that the lack of accountability results in a process that will break down in the midst of difficult circumstances, such as a substantial loss. Another finding is that the lack of automation will prevent the process from scaling to the new organization. The overall conclusion in the wake of increasing pressure to report breaches in a timely fashion is that the incident response process has materially increased the risk of the organization. It is determined that the process should be at Maturity Level 3 to put the organization's risk posture where it wants to be for this process.

In Figure 5, the red diamond (Maturity Level 1.5) represents the current state, the blue diamond (Maturity Level 4) represents the desired state, and the green diamond (Maturity Level 3) represents an intermediate state following a remediation project.

Figure 5. Process Maturity Diagram



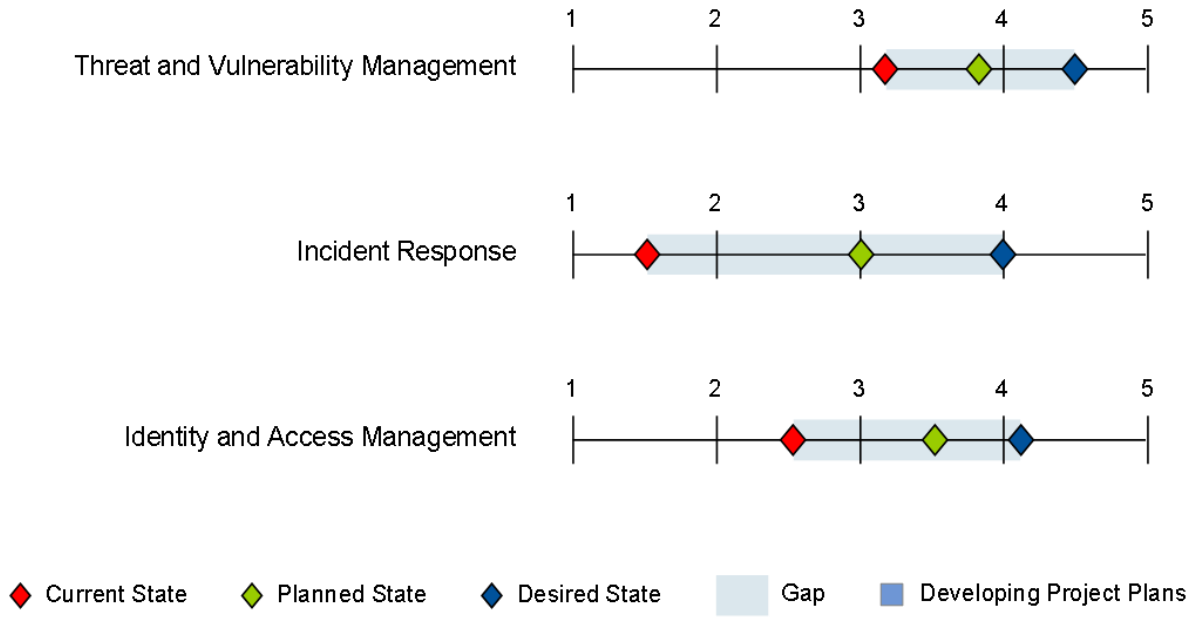
TBD = to be determined

Source: Gartner (January 2010)

9.4 Step 4: Decompose the Gaps Into Projects

The findings from the risk report should be used to develop a set of projects to address gaps. Each project should materially improve the maturity of the process it impacts. Project management people should be involved during all steps of this process, but they should lead this step so that proposed projects are in the required form and that all the organizational-specific requirements necessary for approval are addressed (see Figure 6).

Figure 6. Decompose the Gaps Into Projects



Source: Gartner (January 2010)

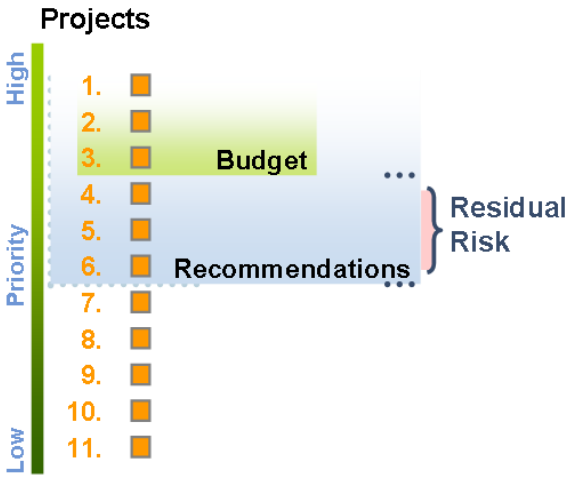
In our example, two findings were determined to materially impact the maturity of incident response, so project plans are developed — one to assign accountability for bringing the process back online, and one to automate the process using the company ticketing system with a formalized escalation process. This and other improvements in the first project will bring the maturity up to Level 3, and the second project would further bring it up to Level 4, where the company has determined it should be.

9.5 Step 5: Develop a Strategic Plan

Once the impact of each project is known in terms of the process's maturity level and the organization's risk posture, then the projects can be prioritized based on budget, schedule and impact. All of this can be conveyed to the business-oriented audience, who owns the risk and the budget, using the process maturity metrics.

In our example, because of budget and resource concerns, the company decides to execute on the first project and use the knowledge learned while fixing the process to refine the requirements for automation. The organization accepts the continued residual risk by bringing the process up to only Level 3. The remaining gap is signed off as an exception that expires in 12 months, with the intent that the subject will be revisited at that time. The project is then prioritized, along with other risk mitigation projects, into a comprehensive strategic plan that forms the foundation for the budget request (see Figure 7).

Figure 7. Stack-Ranking Projects and Addressing Residual Risk



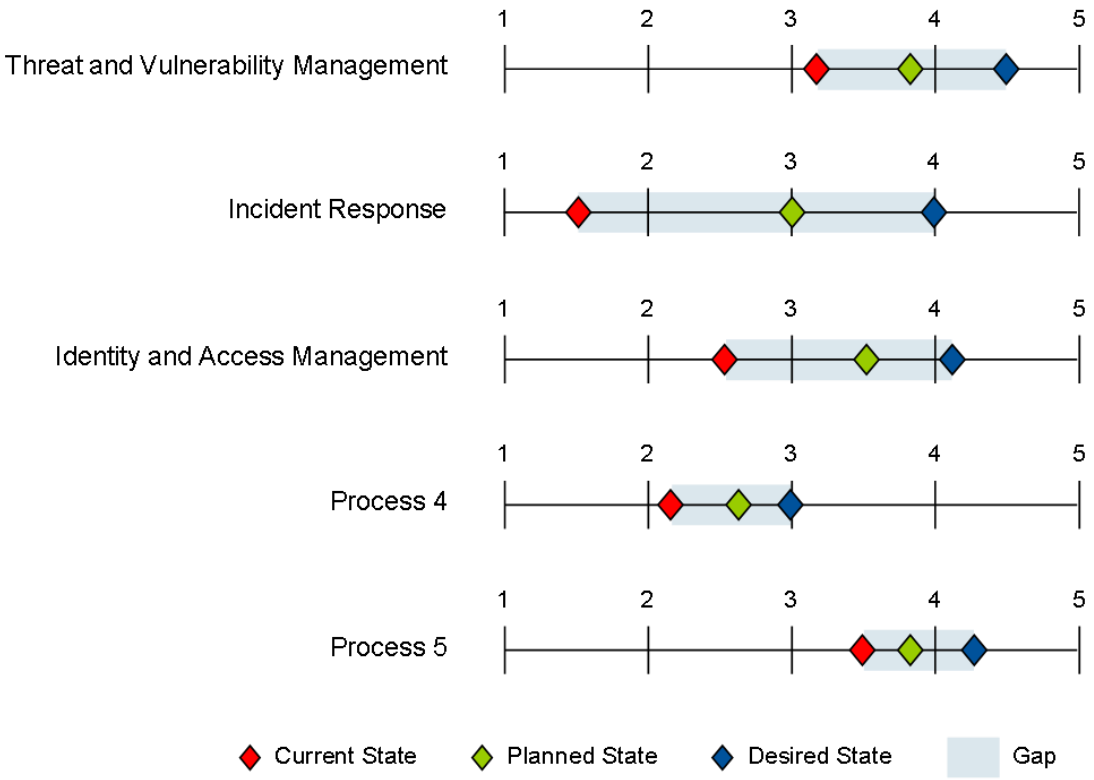
- Develop a strategic plan:
  - Prioritize projects based on budget, impact and schedule.
  - Draw a line and make a recommendation for an annual project plan based on program improvement and lower risk.
  - Use accountability for risk-based decisions to address push-back against recommendations.
- This changes the fundamental budget justification conversation away from the traditional (failed) models.

Source: Gartner (January 2010)

9.6 Step 6: Issue Quarterly Reports

The key to continued executive interest is ongoing engagement through quarterly reports that demonstrate improvements as projects progress. The reports will also serve as an early warning mechanism for failing or neglected projects (see Figure 8). Most of all, they will answer that pressing question for most executives today: How secure are we?

Figure 8. Quarterly Reports for Projects



Source: Gartner (January 2010)

RECOMMENDED READING

"Map Key Risk Indicators to Key Performance Indicators to Support IT and Enterprise Risk Management"

"Toolkit Tutorial: Assessing Risk Posture and Setting Priorities Using a Process Maturity Tutorial"

"Transparency Provides Opportunities and Threats in the 21st Century"

"The Gartner Business Value Model: A Framework for Measuring Business Performance"

"A Risk Hierarchy for Enterprise and IT Risk Managers"

"Q&A: How to Close the Gap Between Information Security and IT Risk Management"

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509