Gartner Research

Publication Date: 14 August 2009 ID Number: G00170266

Security and Risk Process Management Best Practices

Tom Scholtz, F. Christian Byrnes

This research outlines challenges, best practices and strategies for improving information security and risk process management.

Key Findings

- Formalization improves process maturity, which greatly improves the effectiveness and efficiency of information security activities and investments.
- Process management is an ongoing discipline, without which improvement in process performance would be impossible.
- Staff resistance constitutes one of the bigger challenges to process formalization.
- Formalized security processes provide a foundation for effective outsourcing relationship management.

Recommendations

- Allocate time and resources for security process formalization.
- Treat security process management as a dedicated management discipline, tasking process owners with the responsibility for improving overall security process performance.
- Guard against process formalization becoming the goal, rather than the means toward the goal.

TABLE OF CONTENTS

LIST OF TABLES

1.0 Process Formalization

A process is, in essence, a set of activities that are executed in a predefined sequence, in order to achieve a given task or objective. Process formalization, initiated by the security and risk management leadership (see "Toolkit: Formalizing Security Processes") entails:

- Prioritizing which processes to be addressed.
- Assigning process ownership.
- Documenting the process (see "Toolkit: Security Process Definition Template for Security Architecture").
- Allocating associated accountabilities and responsibilities.
- Providing the process owners with the requisite authority, budget and resources to institute, execute and improve "their" processes.
- Making any structural organization change required to improve the process execution.
- Measuring, reporting and acting on process performance.

2.0 Why Formalize Security and Risk Processes?

Processes support requirements for improved accountability, transparency and measurability in risk and security programs. Formalizing security and risk processes has a number of potential benefits:

- It highlights opportunities for improvement. The act of discussing and documenting a process often results in inefficiencies being discovered. As such, it also contributes to corporate quality management initiatives.
- It allows for metrics that enable measurement of process performance over time, thus supporting continuous improvement activities.
- It helps identify processes that are obsolete or redundant.
- It identifies areas for appropriate automation to improve productivity.
- It allows continuity of operations following staff turnover or reorganization.
- It reduces the scope of redundancy in security activities.
- It provides scalability (up or down) if workload increases or decreases.
- It provides opportunities for sharing experiences and codifying best practices within the organization.
- It helps to avoid the tendency to purchase new products for every new security threat.
- It supports the formal integration of security activities with other IT service management processes.
- It allows for improved auditability of security and risk management activities.

In addition:

- Process maturity is the foundation of security and risk program maturity (see "Security Program Maturity Timeline Update, 2009").
- A process approach is the foundation of the information security management system outlined in ISO 27001, both in terms of defining the processes used for defining and selecting controls, and as an integral part of the controls themselves (see "How to Make the Most of ISO/IEC 27001").

In summary, formalization of security processes can result in lower security and risk management costs and improved overall security.

3.0 Challenges

Despite the apparent obvious benefits of security process formalization, there are a number of realities that make it a challenging initiative.

- **Staff resistance.** Staff doesn't naturally embrace a process-based approach. If the motivation for process formalization is not communicated effectively, it can be viewed as a threat or a form of useless bureaucracy by employees. Staff typically interpret their value to the organization (and, hence, the reason for their remuneration) as being their inherent technical, procedural, and contextual knowledge and experience. Externalizing this knowledge into a formal process can be interpreted as a way for the organization to make itself less dependent on this human knowledge and to "automate" the HR costs down. In reality, processes that are properly implemented empower staff members to focus on more value-added tasks and drive continuous improvement in their contribution to the enterprise.
- **Cultural and political realities.** Existing situations can militate against process formalization. For example, trying to implement a comprehensive business continuity process in an organization in which there is no executive understanding or "appetite" for it will result in wasted resources. It would be more appropriate to focus on IT disaster recovery activities. Similarly, trying to implement a strategic security architecture process in an organization with no experience or investment in enterprise architecture will be challenging.
- **Lack of skills.** This applies to both the functional expertise (for example, does the organization have the requisite risk management skills required to formalize a risk assessment process?) as well as generic process management skills. Process management (that is, supporting the definition, formalization, maturation and continuous improvement of any given portfolio of processes) is, in itself, a discrete function and capability.
- **Temporary setbacks in process performance.** Process formalization entails change — change in responsibilities and organizations structure, new procedures and new technologies. Change impacts performance, resulting in temporary dips in overall performance. Care should be taken not to be too aggressive in interpreting short-term performance degradation as evidence that the process formalization has failed. On the other hand, be prepared to admit that midterm performance issues might be an indication that the process formalization has not been successful, so don't be scared to modify or refine the processes concerned.
- **Bureaucracy.** There is a risk that the process maturity initiatives become bogged down in bureaucracy. It is important to guard against process formalization becoming the goal,

rather than the means toward the goal. Process management is a tool for driving improved effectiveness and efficiency in the interest of the business; hence, the temptation to set process targets in isolation must be avoided. If clear benefits are not being realized by the process formalization and maturity initiatives, it is an indication that something is out of balance.

- **Scope creep.** No security or risk process lives in isolation — it is typically interdependent and integrated with a number of other security, risk, IT and business processes. It is important to stick with the original scope specification of any given process definition, reconciling overlaps and conflicts via RACI charts and integration maps (see "Toolkit: Security Process Definition Template for Security Architecture").

- **Inappropriate automation.** Not all processes lend themselves to the same level of automation. For example, a risk assessment process, while potentially benefiting from workflow and document management technology, is largely dependent on actions, interactions and decisions among human stakeholders. On the other hand, security event monitoring, correlation and reporting lend themselves to comparatively high-level automation. Inappropriate automation results in process performance degradation.

- **Getting started.** As the challenges are overcome, there remains the difficulty in creating an initial draft of a process catalog that employees can follow. This is particularly challenging in environments with no experience in process formalization. The early iterations can be very rough, and it is hard for those working on the formalization and the process owners to reach consensus on a draft catalog that is sufficient for everyone's needs.

4.0 Planning a Process Maturity Project

Improving process maturity is a key strategy for improving the overall effectiveness and efficiency of the information security program (see "Toolkit Best Practices: Assessing Security and Risk Management Process Maturity"). A process maturity project would incorporate the following steps:

- **Identify and assess the current maturity levels.** Identify the processes that will be included in the maturity initiative. Assess the maturity of each of these processes. This typically requires an assessment of the current maturity level, using the Capability Maturity Model Integration (CMMI) scale to express the current levels. For example, the vulnerability assessment process is currently at CMMI Level 2.

- **Formalize informal processes.** The maturity assessment will often identify some security and risk processes that are so immature (CMMI Level 0 or 1) that they first need to be formalized before any meaningful maturity work can be performed on them.

- **Define the desired state.** Make a decision about the desired level of maturity for the respective processes, including an estimation of the time frame within which the desired maturity level should be reached. For example, the desired maturity level of the vulnerability assessment process is CMMI Level 4, and it should preferably be reached within two years.

- **Develop a maturity plan for each process.** Identify specific actions for improving the maturity of each process. The maturity criteria outlined in "Toolkit Best Practices: Assessing Security and Risk Management Process Maturity" can be used as a framework for identifying maturity actions. See Table 1 for an example of a maturity plan for the vulnerability assessment process.

Table 1. Illustrative Maturity Plan for Vulnerability Assessment Process

Maturity Criteria	Actions to Reach Level 3	Actions to Reach Level 4
Integration	Integrate with risk assessment and security monitoring processes.	Integrate with change and configuration management processes.
Automation	Evaluate and implement application, system and network assessment tools and/or services.	Integrate selected tools/services with risk reporting system.
Stability	Standardize process across all business units.	
Metrics	Develop effectiveness and service-level metrics.	Develop efficiency/productivity metrics and risk-expression metrics.
Performance	Set and track effectiveness and service-level performance targets.	Set and track efficiency/productivity performance targets.

Source: Gartner (August 2009)

Clearly assign resources and responsibilities for executing on the maturity plan and actions for each process. Prioritize the maturity projects based on potential risk impact, resource availability and expected time to value. Document and track all the actions taken in order to report back to governance stakeholders, and to allow leverage of lessons learned.

5.0 General Best Practices

Don't attempt the process management initiative in isolation. In most organizations, the IT operations and service management functions have extensive experience in process formalization and maturity management. Reach out to them, and find out about the potential pitfalls and how to avoid them.

Then, use the relationship to get a better understanding of the interdependencies and potential integration points with IT service and operations management processes. If your IT service management colleagues use the IT Infrastructure Library (ITIL), spend time to get an understanding of how that framework can be used to improve the interrelationships between service and security management processes (see "Preparing for the Impact of ITIL v.3 on GRC Strategies").

Utilize metrics to measure and report on process effectiveness and efficiency. Ensure that meaningful metrics are integrated into the process design. For example, measuring, logging and reporting on the number of different types of security vulnerabilities must be an integral component of the vulnerability assessment process. Consolidate process metrics and include them in executive reporting to substantiate improvement in the overall security program performance (see "The Do's and Don'ts of Information Security Metrics").

The typical reaction of technology staff is to reach for technology solutions to solve process problems. It is important to remember that technology is primarily used to automate components of processes (see "Critical Capabilities for IT Governance, Risk and Compliance Management, 2009"). The level to which a specific process can successfully be automated depends on:

- The nature of the process itself — e.g., event monitoring and consolidation lend themselves more to automation than policy management.

- The maturity and efficiency of the process within the organization, as well as within the industry as a whole.
- The stability (i.e., rate of change) of the process.

Consider including process principles, models, templates and high-level definitions as artifacts in the security architecture to leverage reuse and consistency in process management throughout the organization (see "The Structure and Content of an Information Security Architecture Framework" and "Toolkit: "Security Process Definition Template for Security Architecture").

Process maturity is a key building block of overall program maturity. But not all processes need to aspire to Level 5. The highest levels of process maturity are generally achieved by large enterprises whose core products and services, not just their financials, are regulated. These enterprises have many processes going on all the time, and they are comfortable adding security and risk management processes to the stack. However, in many organizations, the incremental cost of reaching Levels 4 and 5 for all processes typically outweighs the incremental benefits. Be realistic in rationalizing the target maturity levels of individual processes.

Moving up the maturity scale is an incremental process. Maturity plans should focus on improving maturity one level at a time. Avoid the temptation to "skip" a level.

Process maturity can also be used as a vehicle to communicate effectively with executive management. The concept of funding improvement in an existing process to gain efficiencies and a better risk posture resonates with business management better than operational metrics (see "Toolkit Tutorial: Assessing Risk Posture and Setting Priorities Using a Process Maturity Tutorial").

6.0 Security Process Management in an Outsourced Environment

A process-based view of security responsibilities and activities provides a good foundation for developing an organizational strategy for information security in outsourced environments. In other environments, it will simplify any future outsourcing initiatives. Indeed, a well-defined set of security roles and its associated strategic and operational processes provide a framework against which respective responsibilities can be allocated (see Table 2). Although the service provider will be responsible for performing these processes, never forget that accountability for information security cannot be outsourced. Ownership for all processes and functions remains within the client organization.

Table 2. Example Security Responsibilities in an Outsourced Environment

Role	Process/Function	Client Organization	Outsourcer/Service Provider
Leadership	Relationship Management	Own and Execute	Ad Hoc Support
	Strategy/Architecture	Own and Execute	Ad Hoc Support and Third Party
Analysis/Design	Policy Management	Own and Execute	Participate
	Risk Management	Own and Execute	Participate
	Trust/Domain Management	Own and Execute	Participate

Role	Process/Function	Client Organization	Outsourcer/Service Provider
	Technology Domain Specialists	Coordinate	Own and Execute
	Project Management	Own and Execute	Participate
	Quality Assurance	Own and Execute	Participate
Awareness	Awareness Communication	Own	Execute
	Local Coordinator	Own and Execute	Liaise
Security Operations	Monitoring	Own	Execute by Third Party
	Response	Own and Execute	Participate
	Forensics	Own and Execute	Participate; Ad Hoc Support by Third Party
	Vulnerability Research	Own	Execute by Third Party
	Configuration Management	Own	Execute by third Party
Administration	User Life Cycle Management	Own and Execute	Liaise

Source: Gartner (August 2009)

Process alignment between client and outsourcer is a prerequisite for outsourcing success. This predicates a review of the tools and processes used by both parties, and an agreement to use one or the other or an integration of the two sets.

In addition to providing a model for allocating responsibilities between client and outsourcer, security processes also enable specific associated metrics. These metrics potentially form the foundation for effective security service levels to be negotiated and instituted as part of the outsourcing relationship. Furthermore, effective security auditing is crucial in an outsourced environment, and the nature of processes (i.e., a predefined set of actions executed in a predefined sequence, with consistent decision points) enables improved auditability.

RECOMMENDED READING

"Toolkit: Formalizing Security Processes"

"Toolkit: Security Process Definition Template for Security Architecture"

"Security Program Maturity Timeline Update, 2009"

"Toolkit Best Practices: Assessing Security and Risk Management Process Maturity"

"Preparing for the Impact of ITIL v.3 on GRC Strategies"

"The Structure and Content of an Information Security Architecture Framework"

"The Do's and Don'ts of Information Security Metrics"

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

"How to Make the Most of ISO/IEC 27001"

Acronym Key and Glossary Terms

ad hoc support	Perform steps/activities on an "as needed" basis
coordinate	Ensure steps and activities are aligned
execute	Primary process/function execution responsibility — i.e., perform most steps/activities
liaise	Maintain communications relationship
own	Process ownership and accountability
participate	Some process/function execution responsibility — i.e., perform some steps/activities
third party	Other external consulting or service support

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

Gartner