SECURITY THROUGH PROCESS MANAGEMENT

Jennifer L. Bayuk
Price Waterhouse, LLP
4 Headquarters Plaza North
Morristown, NJ 07962
jennifer_bayuk@notes.pw.com

Overview

This paper describes the security management process which must be in place to implement security controls. An effective security management process comprises six subprocesses: policy, awareness, access, monitoring, compliance, and strategy.

Security management relies on policy to dictate organizational standards with respect to security. Without policy, no person in the organization is responsible for securing information or is accountable for not having done so. A fundamental component of security management is a process for the production of security policy.

However, the resulting policy has value only if it is followed. A person who is not aware of an information security policy is not necessarily accountable for violating it. In the case of a system administrator configuring system security, ignorance of policy certainly provides an excuse to use personal judgment. Effective security management relies on an awareness process to provide accountability.

The policy process dictates *what* must be done to provide an acceptable level of assurance that systems are secure. The awareness process ensures that people know what must be done. To achieve assurance that policy is being followed uniformly throughout the organization, security management must also address *how* policy is to be realized. *How-to* solutions are effected via access and monitoring processes. Access and monitoring processes constitute the daily operational activities of security management. They provide guidelines on how to securely configure information systems and how to recognize a security incident.

Once a security incident has been recognized, a security management process requires methods to ensure that known security vulnerabilities are closed and open security issues are resolved. These methods are part of a compliance process. In addition, foresighted security management will include a strategy process to ensure that security management stays abreast of changes in the information technology environment which it seeks to secure.

Hence, an effective security management process comprises six subprocesses:

- Policy
- Awareness
- Access
- Monitoring
- Compliance
- Strategy

The Policy Process

A security policy is needed to establish a framework for the development of security procedures and practices. It also provides a vehicle with which to communicate roles and responsibilities with respect to securing information. A policy framework should specify the minimum security standards to be applied to all information systems, and more stringent standards for systems which contain highly sensitive or proprietary data. A security policy should address the following:

- Scope of the policy, including the facilities, systems, and personnel to which it applies
- Objectives of the security management process and descriptions of subprocesses
- Accountability and responsibility for subprocesses at all levels of the organization
- Minimum requirements for the secure configuration of all systems within the scope[†]
- Definition of violations and consequences of noncompliance
- A user statement of responsibility with respect to the information to which he or she is granted access

A security policy is a dynamic document. Its design should be flexible to allow frequent updates as technology and/or management changes require. Security policy development is not a project with a beginning and an end. A security policy coordinator should have responsibility for maintaining a policy team which is knowledgeable in both security techniques and the target information systems operating environment. The team leader must maintain open communications channels between the policy team, the management team who approves the policy, and those to which the policy applies. An example security policy process is depicted in Figure 1.

The Awareness Process

Though security personnel are arguably the best source of information concerning an individual's responsibilities with respect to information security, there are usually not enough of them to explain those responsibilities to everyone who falls within the scope of information security policy. It is enough that each department within scope designate an individual as a *security liaison*. Security personnel should create a security awareness program that may be implemented by department liaisons. This program needs to be flexible, comprehensive, clearly communicated, and understandable by department liaisons.

[†] Minimum security requirements for system configuration may contain standards which apply to only a subset of the facilities or organizations within the scope of the policy. For example, a security policy dedicated to a PC LAN environment will not make sense to implement on an IBM Mainframe. Designating specific sections or appendices to apply only to specific platforms enables the security policy as a whole to apply equally to all facilities, systems, and personnel within its scope.

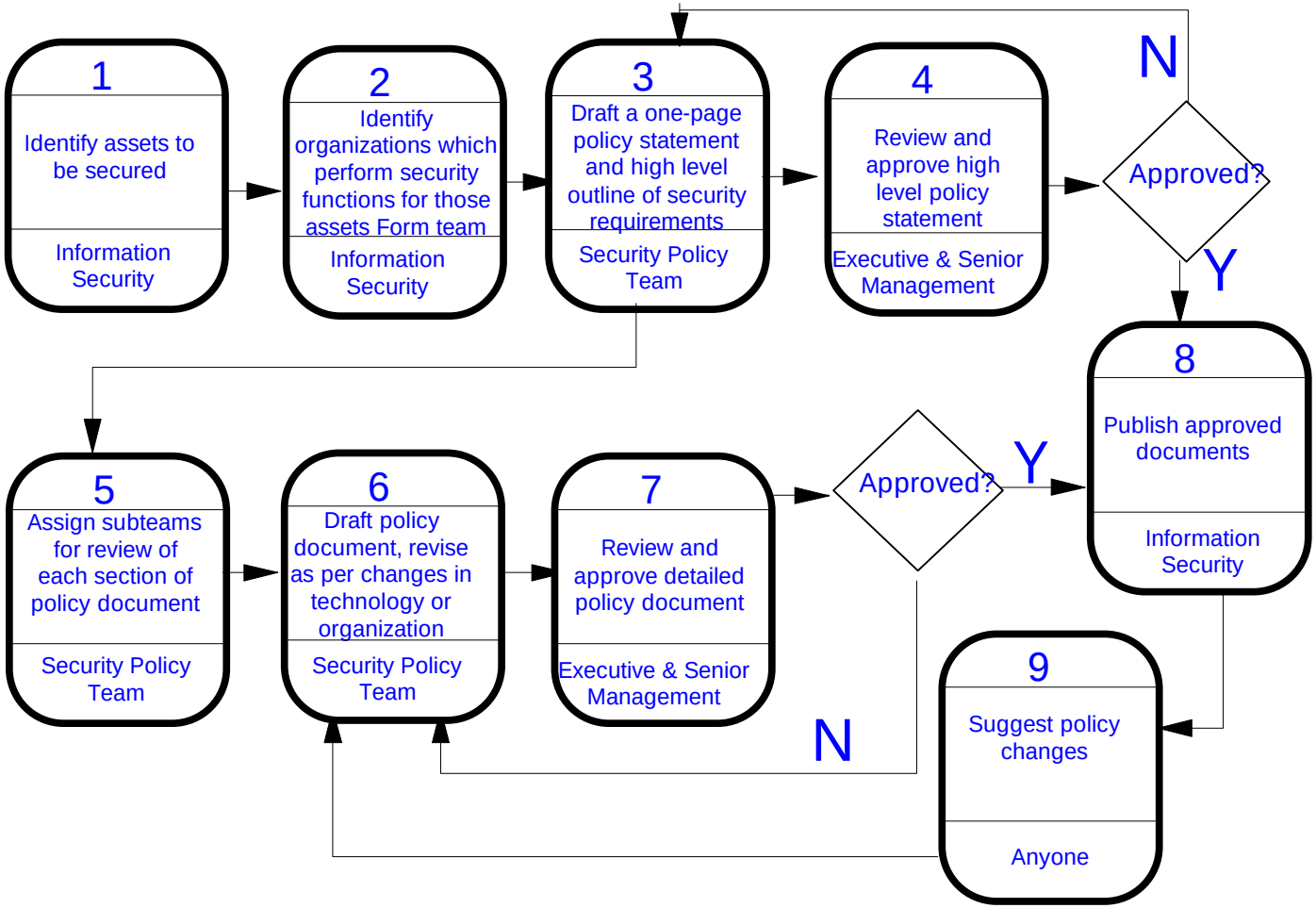

Figure 1: Example Policy Process

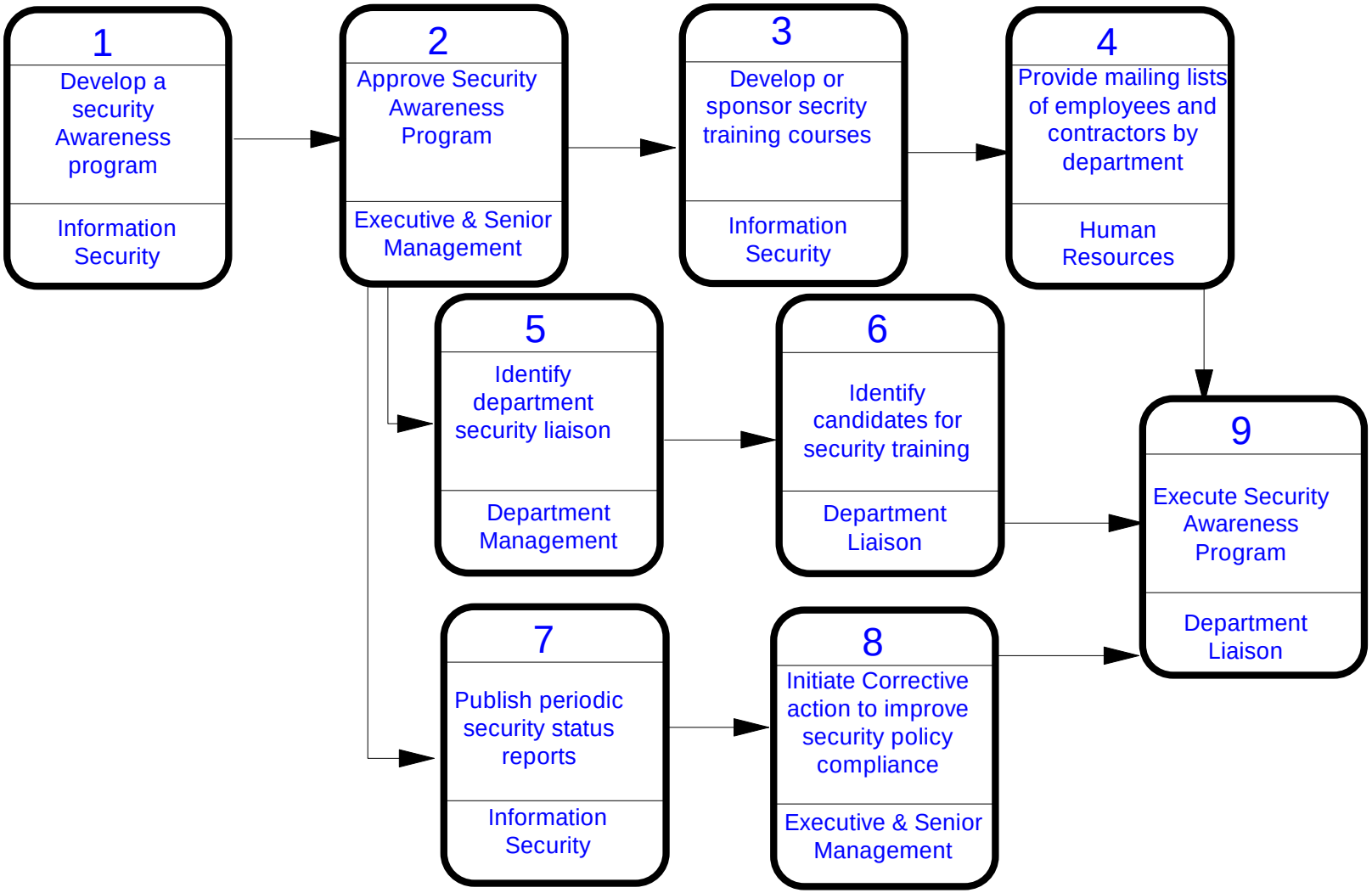

Figure 2: Example Awareness Process

The awareness program must clearly specify the actions required of employees and contractors and the seriousness of the actions that will be taken for non-compliance or violation of security policy. The awareness program should address the following key issues:

- Display high-level support
- Teach people how to obtain and comply with policy
- Point out the business risks in security policy violations
- Address the widest possible audience
- Allocate responsibility

An effective security awareness process will have executive and senior management play a formal role in improving security awareness by endorsing the security awareness program and by setting high priorities for security compliance. It will be integrated with personnel hiring and contracting practices to ensure completeness of coverage. The expected level of participation is evident in the example of a security awareness process depicted in Figure 2.

The Access Process

A security access process helps ensure that access decisions are made in a controlled manner, and that information concerning access is securely communicated between those that have a need to know. An access process should address:

- Identification of those who require access
- Authorization procedures for system access
- Automatic authentication of those identified and authorized for access
- Separation of duties between authorization and authentication
- Separation of access environments for distinct job responsibilities

Though security policy may dictate the details of how access should be administered, decisions concerning who should have access to production systems must rest solely with department managers responsible for the systems' smooth operation. In many organizations, the Information Security department facilitates the actual creation and maintenance of access, but it may be performed by anyone as long as it is done in accordance with policy and a separation of duties between authorization and authentication is maintained. An example access process is depicted in Figure 3.

The Monitoring Process

Security monitoring is required to detect both unauthorized system access and attempts at unauthorized system access. Left unmonitored, unauthorized access attempts may become unauthorized access. A security monitoring process includes three basic activities:

- configuring system security profiles and frequently reviewing system security logs
- identifying the root cause of security alerts

using the information derived from the first two activities to devise ever more meaningful system security profiles

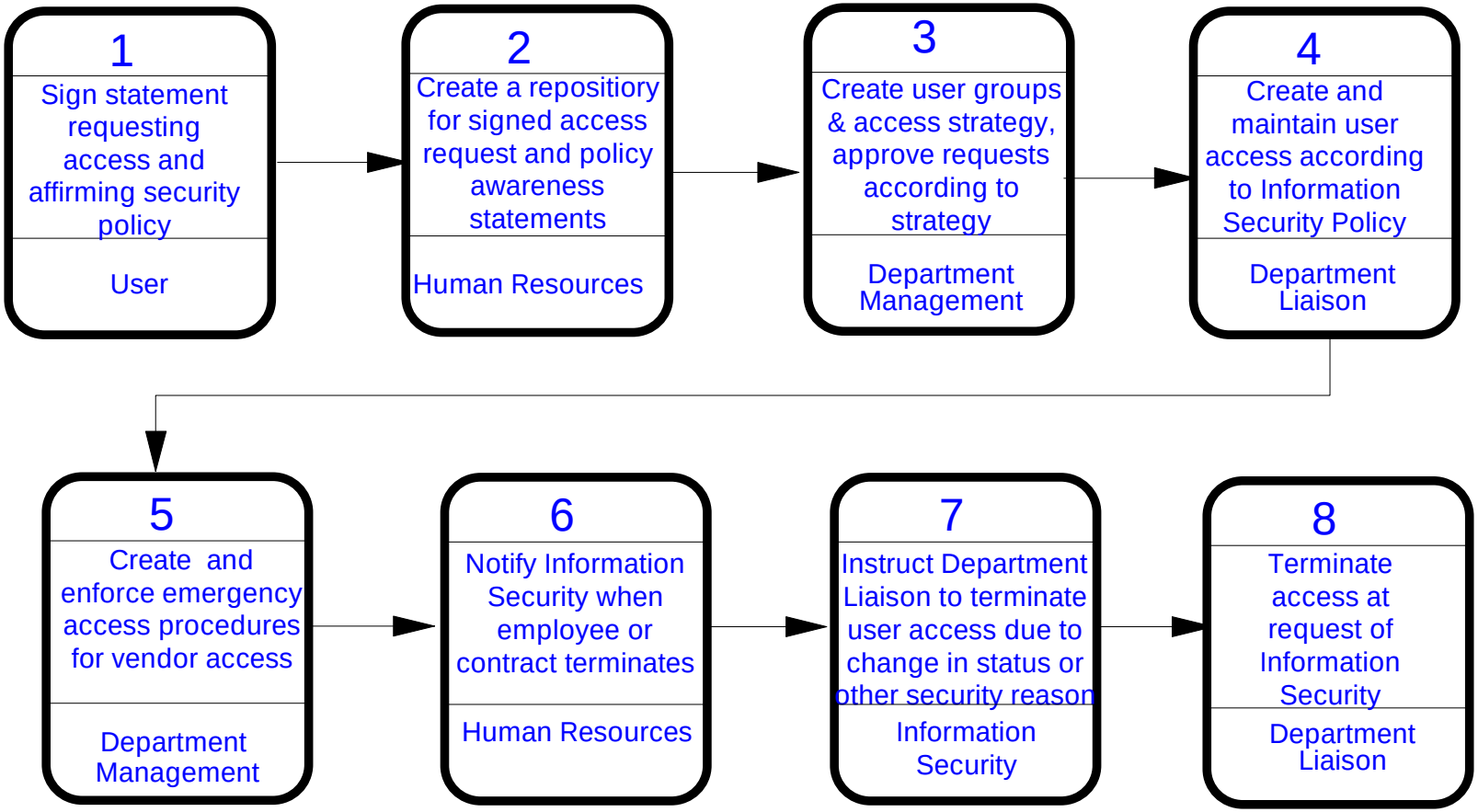

Figure 3: Example Access Process

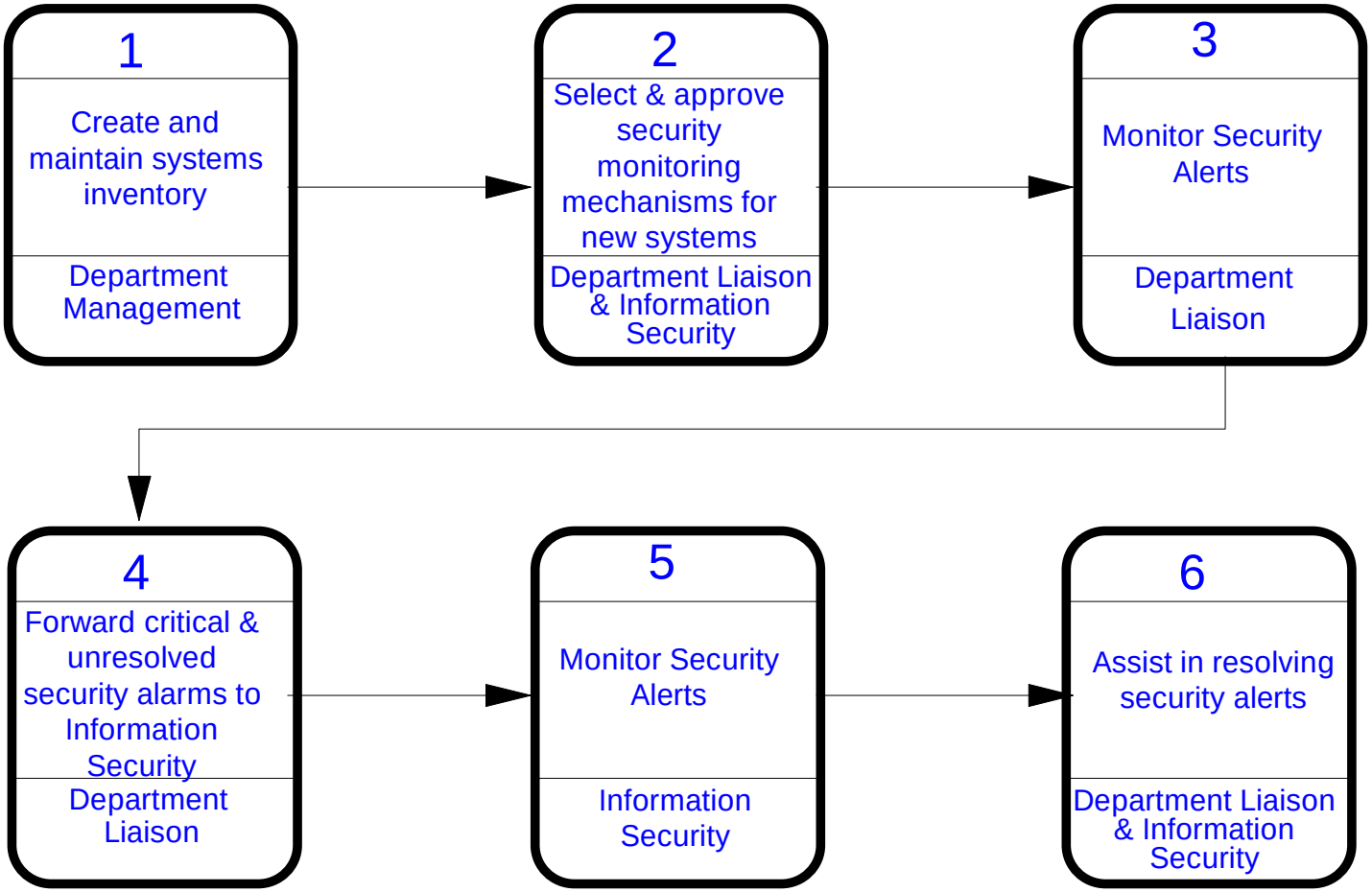

Figure 4: Example Monitoring Process

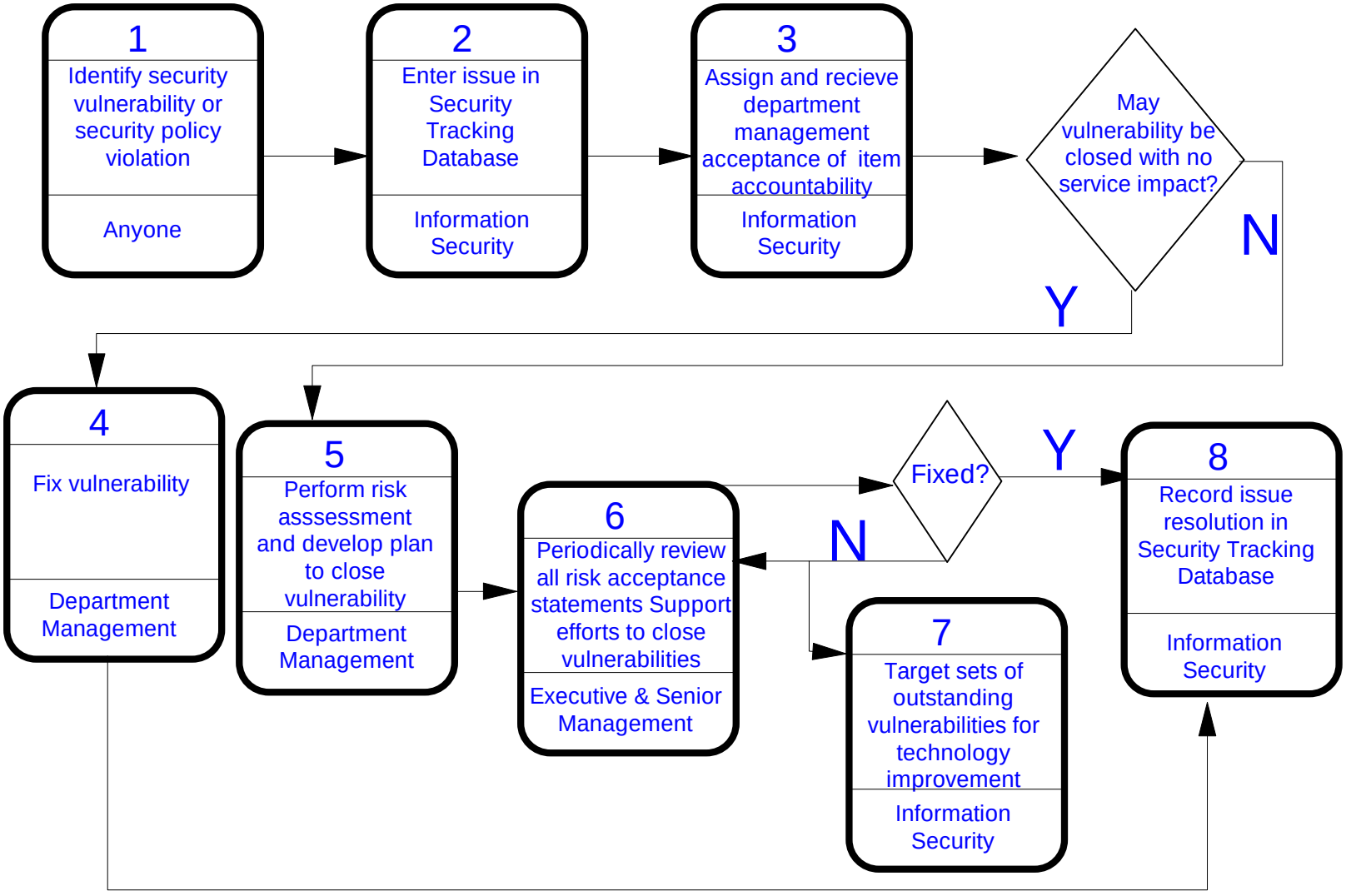

Figure 5: Example Compliance Process

Security monitoring is most cost-effective when merged with other monitoring processes such as performance or activity monitoring. However, where the root cause of a security alert cannot be determined or is determined to be a computer intrusion, system monitoring responsibilities should be shared with Information Security. Information Security should help ensure that all necessary operational and legal requirements for intrusion containment are met. Information Security should also track security alerts over time to determine if there are patterns. An example security monitoring process is depicted in Figure 4.

The Compliance Process

The extent to which there exists a formal compliance process is the extent to which security management efforts are effective in establishing a uniform level of security controls. Because compliance activities must be distributed among those who are responsible for the secure operation of information systems, departmental management must manage with reference to policies established by Information Security. However, there will be instances of non-compliance for many reasons, including:

- the technical architecture of a system does not support a required security function
- resources required to maintain compliance are unavailable
- a security incident reveals a security vulnerability which is not yet addressed by policy
- routine security audits or security reviews reveal previously unnoticed risks

In any case, the instance of noncompliance must be:

- reported to the Information Security
- assigned to appropriate management
- supported by a risk acceptance until resolved

The security compliance process must track all such security issues to ensure that steady progress is made toward their resolution. An example of a compliance process is depicted in Figure 5.

The Strategy Process

The security of information services is a reflection of the quality of information services. Developers of new products must recognize the strategic importance of integrating security mechanisms into the product itself. The security strategy process should aim to bring security expertise into long-range systems planning. The security strategy process may facilitate the integration of security into system design by:

- Developing risk assessment methods that quantify levels of operational risks in new products
- Contributing to business cases for including security mechanisms in architecture budgets
- Reviewing and testing new security features and products

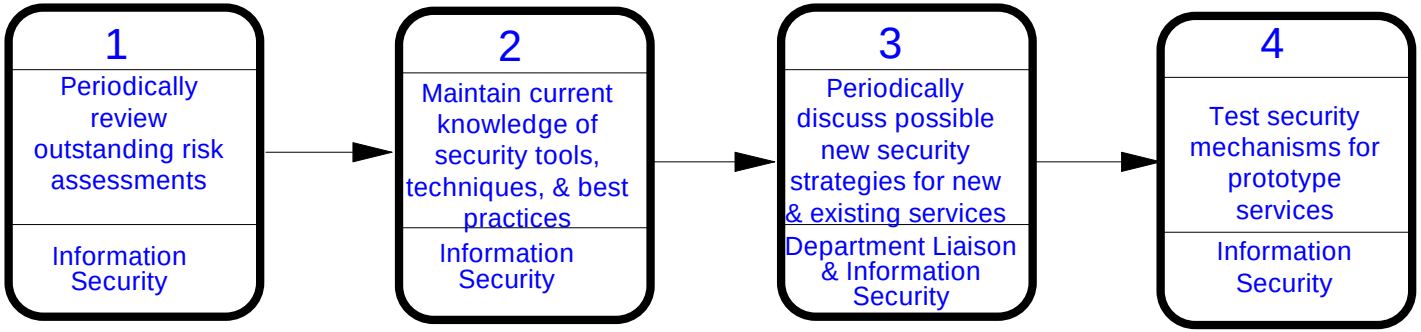

Figure 6: Example Strategy Process

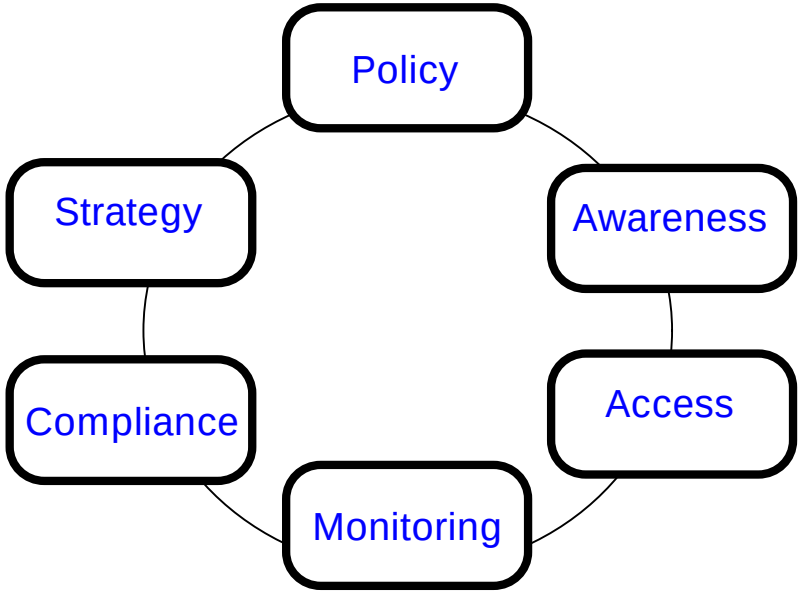

Figure 7: The Security Management Process

To facilitate the secure deployment of new and prototype services, the technical sophistication of the security department must equal that of the new service or prototype developer. Information Security must be an equal partner at every stage in the planning of services which require the use new technology. An example security strategy process is depicted in Figure 6.

Summary

This document describes the security management process which must be in place to implement security controls. The security management process includes six functions, each of which may be viewed as a distinct sub-process:

Policy:	to establish a framework for the development of organizational standards with respect to security
Awareness:	to educate those affected by security policy on their roles and responsibilities
Access:	to limit dissemination and modification of customer data and other sensitive information
Monitoring:	to detect policy violations and other security vulnerabilities
Compliance:	to track security issues and help ensure that resources facilitate the resolution of security issues
Strategy:	to meet the security challenges presented by new information technologies

Taken together, these six processes form one high-level security management process, displayed in Figure 7.