The SANS Technology Institute

Fundamentals of **Information Security Policy**

How to Review and Assess Information Security Policy

The Six-Step Process

February, 2010

Ahmed Abdel-Aziz
CISSP, SANS GIAC

Table of Contents

ABSTRACT 3

INFORMATION SECURITY DRIVERS..3

THE POLICY DIMENSION & ITS RELATIONSHIP TO OTHER DIMENSIONS 4

SIX-STEP PROCESS FOR REVIEWING & ASSESSING INFORMATION SECURITY POLICY.........6

STEP1 – HAVE SOMEONE OTHER THAN THE PERSON WHO WROTE THE POLICY REVIEW IT 6
STEP 2 – ASSESSING POLICY FOR COMPLETENESS..6
Step 2.1 – Assessing Policy Framework for Completeness 7
Step 2.2 – Assessing Policy Elements for Completeness 8
STEP 3 – ENSURE POLICY STATEMENT IS CLEAR, CONCISE, AND SMART 8
STEP 4 – ENSURE POLICY ANSWERS THE 5 WS (WHO, WHAT, WHERE, WHEN, & WHY) 9
STEP 5 – ENSURE CONSISTENCY WITH LAWS, REGULATIONS, AND OTHER LEVELS OF POLICY 9
STEP 6 – CHECKING POLICY FRESHNESS AND EASY AVAILABILITY TO ORGANIZATION MEMBERS....................9

CONCLUSION 10

REFERENCES 10

Abstract

The information security policy is the foundation on which effective security is built. As with any foundation, it must be well designed, and well constructed (Weise, & Martin, 2001). All internationally accepted best practices for information security management accept the formulation of policies as the starting point to implement information security in an organization (Grobler, & von Solms, 2004).

Information security policy is one dimension of the multi-dimensional discipline of information security (Grobler, & von Solms, 2004). This paper will discuss security drivers, the relationship between the policy dimension and other information security dimensions, and then will propose a six-step process to critically review and assess information security policy.

Information Security Drivers

Before discussing information security policy and the process to assess it, it is important to know what drives information security in the first place. This is important because an organization′s security requirements, and their derived security controls such as security policy should be the result of these security drivers (ISO/IEC, 2005). According to the ISO/IEC 17799:2005 best practice information security standard *(later renumbered to ISO/IEC 27002)*, information security will function to enable the business and reduce relevant risks. The standard states that there are three main sources (drivers) of organizations′ security requirements:

Source of Security Requirements 1:

- *Security requirements derived from the legal, regulatory, and contractual requirements the organization, its trading partners, contractors, and service providers must satisfy.*

Source of Security Requirements 2:

- *Security requirements derived from assessing risks to the organization, taking into account the organization′s overall business strategy and objectives.*

Source of Security Requirements 3:

- *Security requirements derived from the particular set of objectives, and business requirements for information processing that an organization has developed to support its operations. One example could be security requirements to achieve a specific up-time for a telecom operator′s billing system.*

These three drivers for information security shape an organization′s specific security requirements (ISO/IEC, 2005). The objective of security controls, such as security policy, is to achieve those security requirements.

The Policy Dimension & Its Relationship to Other Dimensions

Information security policy sets the boundaries of behavior and empowers people to do the right thing (Northcutt, 2007). When policy is properly developed and implemented, the policy will ensure consistency and will support the organization's mission (Miles, Rogers, Fuller, Hoagberg, & Dykstra, 2004).

Security controls have been classified in multiple ways. A common taxonomy for security controls is Technology, Process, & People. We will use a derivative of this taxonomy suggested by Grobler & Von Solms in their paper: [comma in place of colon] Assessing the Policy Dimension. In this taxonomy, Process is broken up further into the following dimensions: Corporate Governance, Policies, Risk Management, and Legal & Compliance. The focus of this paper is on security policy only and will identify the relationships between the policy dimension and the other different dimensions as illustrated in Figure-1 below.

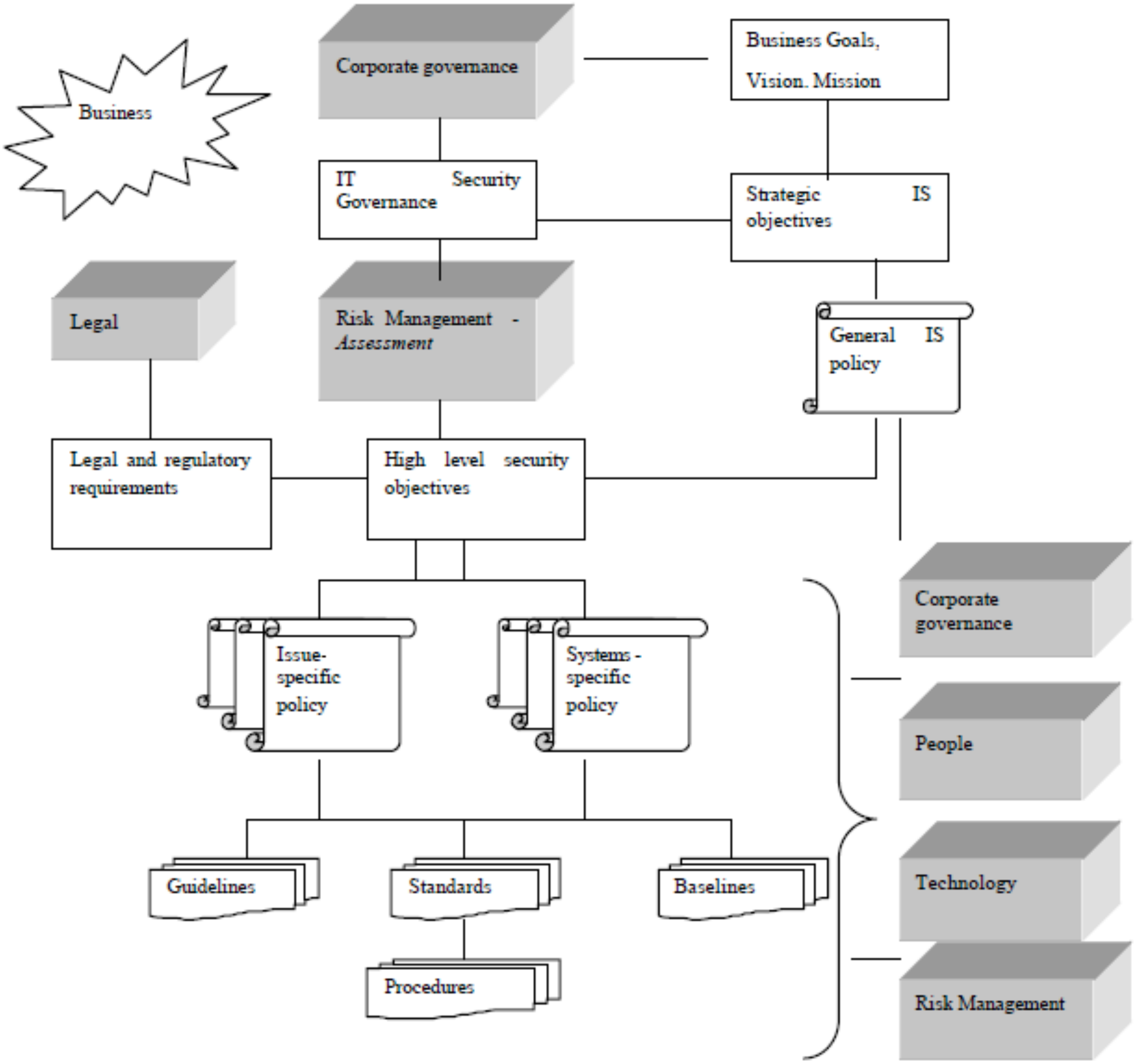

Figure 1: Policy Dimension Relationships (Grobler, & Von Solms, 2004)

Notice how the high-level security objectives in the figure are derived from the three security drivers listed in the previous section of the paper: **Information Security Drivers**. The high-level security objectives in the figure come from: 1-Legal & Regulatory Requirements, 2- Risk Assessment, 3- The Strategic Objectives and Strategic Security Objectives of the Organization. These high-level security objectives should fulfill the organization's specific security requirements.

With that background information of security drivers and security policy, I believe assessing and reviewing security policy will be more effective. The next section explains a six-step process to follow when reviewing and assessing information security policy.

Six-Step Process for Reviewing & Assessing Information Security Policy

The following are six important steps to take when evaluating information security policy (Northcutt, 2007).

- Step 1 – Have Someone other than the Person who Wrote the Policy Review It
- Step 2 – Assessing Policy for Completeness
- Step 3 – Ensure Policy Statement is Clear, Concise, and SMART
- Step 4 – Ensure Policy Answers the 5 Ws (Who, What, Where, When, & Why)
- Step 5 – Ensure Consistency with Laws, Regulations, and Other Levels of Policy
- Step 6 – Checking Policy Freshness and Easy Availability to Organization Members

Step1 – Have Someone other than the Person who Wrote the Policy Review It

People tend to spot their own errors a small percentage of the time. Therefore, someone other than the person who wrote the policy should review and assess it for mistakes or omissions. That person needs to know the organization, fundamentals of information security, and be detail-oriented for best results. The person must have enough technical knowledge because the policy must be reviewed for technical accuracy (Scarfone, Souppaya, Cody, & Orebaugh, 2008).To assess the specificity of the policy, it is good to have a person that is not familiar with the exact topic do the assessment, so that auto-correction and mentally filling in any errors or omissions does not take place.

Information security policy should have an owner who has approved management responsibility for the development, review, and evaluation of the security policy (ISO/IEC, 2005). Although the policy owner is responsible for the policy review, this does not mean they have to do the review themselves. Another person or team should be assigned that task to increase the opportunity for improvement of the security policy.

Step 2 – Assessing Policy for Completeness

The second step in assessing policy is quite large and so is divided into two sub-steps:

1- Assessing Policy Framework for Completeness
2- Assessing Policy Elements for Completeness

Step 2.1 – Assessing Policy Framework for Completeness

Every organization should set up a policy framework to represent all the policies, standards, procedures (Grobler, & von Solms, 2004). According to many literature sources, three general types of policies exist:

- General/Corporate policy providing general direction
- Issue-specific policies such as electronic mail, Internet use, etc.
- System-specific policies used when configuring and maintaining systems

The relationships between the policy framework components are illustrated in Figure-2 below.

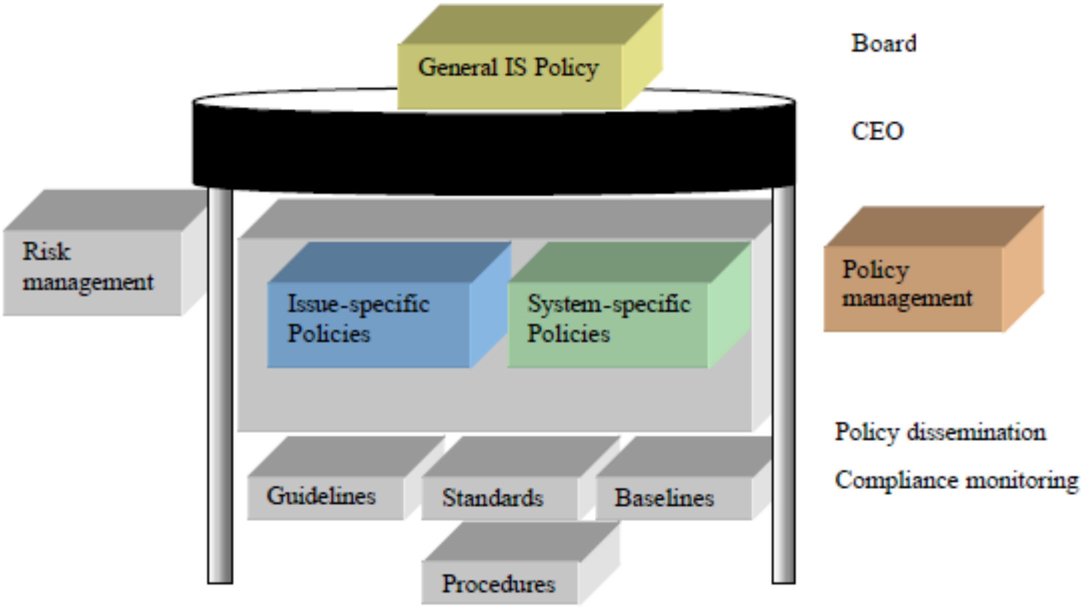

Figure 2: Policy Framework (Mohan, 2003)

When assessing the policy framework for completeness, it is necessary to check that the policy set covers the risks and high-level security objectives defined earlier in Figure-1 (Grobler, & von Solms, 2004). If an organization′s security requirements are not defined, then it is difficult to assess how good or bad the policy set is for the organization. The ISO/IEC 17799 standard recommends conducting a risk assessment to define security requirements before policy development takes place. Using the same logic when policies have already been developed in the absence of defined security requirements, a risk assessment should be conducted first before policy assessment takes place. During policy assessment, it is necessary to check for the existence of standards and procedures supporting the policy set; however, evaluating the content of these standards and procedures would typically be out of the policy assessment′s scope (Grobler, & von Solms, 2004).

Step 2.2 – Assessing Policy Elements for Completeness

According to the NIST SP800-26 *(Security Self-Assessment Guide for Information Technology Systems)*, the three key components of security policy are:

- Purpose & Scope
- Responsibilities
- And Compliance (consequences and penalties for not following policy)

Security policies exist at different levels and policy elements may not be the same at each level, however the above three components must exist in the policy set. Corporate policy provides general direction to be implemented at lower levels in the enterprise, while a system-specific policy is much more detailed; therefore, their policy elements will likely differ. The most common elements of issue-specific policy include the following:

- Purpose: The reason for the policy
- Related Documents: Any documents affecting contents of this policy
- Cancellation: Any existing policy that is cancelled when this policy is effective
- Background: Amplifying information on the need for the policy
- Scope: The range of coverage for the policy
- Policy Statement: The actual guiding principles of what is to be done and when.

The most common elements of general or corporate security policy include the following (Grobler, & von Solms, 2004):

- Need for/scope of information security
- Objectives of information security
- Management′s commitment
- Roles and Responsibilities
- Policy violations and disciplinary actions
- Monitoring and review
- User declaration and acknowledgement
- Risk management

Since policies differ, and not all policies have all of the elements, the important issue in this step is to ensure the policy is not badly flawed due to a lack of an element.

Step 3 – Ensure Policy Statement is Clear, Concise, and SMART

The policy statement, or body of the policy, identifies the actual guiding principles of what is to be done. The statement is designed to influence and determine actions within the scope of coverage. Therefore, it needs to be clear and use simple language that is easily understood by everyone. The statement also needs to be brief and express a lot in a few words. This is important because readers are busy; reading through multiple paragraphs without finding pertinent information creates discomfort (Lindley, 2001). Finally, the policy statement needs to be SMART

*(**S**pecific, **M**easurable, **A**chievable, **R**ealistic, and **T**ime-Bound)*. The rule for evaluating specificity in policy is that the policy must be sufficiently detailed to allow procedures and checklists to be evaluated against the policy (Northcutt, 2007). If this is not possible, the policy is not specific enough.

Step 4 – Ensure Policy Answers the 5 Ws (Who, What, Where, When, & Why)

Security policy needs to answer who, probably by job function not by name, is responsible for what. It also needs to make clear when those actions need to be accomplished. Policy needs to explain why the policy exists through the following policy elements: Purpose, Background, or Policy Statement. If you cannot explain why the policy exists, it is very difficult for organization members to understand or follow it (McConnell, 2002). If the "why" cannot be answered, then the policy is probably not needed. Answering the "where" question may be more appropriately included in procedures instead of policy; however, it still needs to be considered in policy (Lindley, 2001).

Step 5 – Ensure Consistency with Laws, Regulations, and other Levels of Policy

Security policy must be consistent with various laws and regulations; otherwise the organization may face lawsuits. Laws and regulations will change from country-to-country and from industry-to-industry; therefore, policy assessment needs to consider the location and industry of the organization to ensure consistency with laws and regulations. Security policy exists at various levels and supports the organization to achieve its mission. When a policy is assessed, checking consistency with lower-level and high-level policies needs to be done. If you discover any discrepancies or contradictions, they should be noted and resolved. If possible, priority should be given to higher-level policy when it contradicts lower-level policy. This is because higher-level policy provides direction and guidance for compliance with industry regulations and laws, and also because higher-level policy should be aligned with the strategic objectives of the organization (Weise, & Martin, 2001).

Step 6 – Checking Policy Freshness and Easy Availability to Organization Members

Security policy needs to be examined for provisions to keep it current. This is important because an outdated policy could cause more damage than good. Consider an example of policy stating wireless traffic needs to be encrypted using the WEP protocol. This would provide a false sense of security for users, and is one reason why policy should not be technology-specific since technology is outdated quickly. Regularly reviewed policy should reflect lessons learned from recent incidents and new threats to the organization's security. Common business practice suggests that organizations should update their policies on a yearly basis. Policy can be refreshed off-schedule due to an update trigger such as a new regulation compliance requirement. The ISO/IEC 17799 standard recommends having defined management review procedures for security policy, including a schedule of the review. The review of information security policy should take into account the results of management reviews. Management sees the big picture and knows if the approach to information security should change for the organization; this change in approach should be reflected in the security policy. Finally, management approval should be obtained for the revised policy. As part of the last step in the six-step process, it is necessary to check whether the security policy is readily available. The target audience for the policy needs to know the policy exists, be able to easily access it, and be required to do so. The best policy will be no good if people do not know it exists, can't find it, or had no time to read it (McConnell, 2002).

Conclusion

This paper explained security drivers, the security policy dimension, its relationship to other dimensions, and how to review and assess security policy by following six important steps. Before assessing and reviewing security policy, it is valuable to understand the security drivers, and how the policy dimension relates to other information security dimensions. The six-step process starts by having a person other than the person who wrote the policy review it for the completeness of policy framework and policy elements; a clear, concise, and SMART policy statement; answering the 5 Ws; consistency with laws, regulations, and other policy levels; and finally for policy freshness and easy availability.

In the end, it is crucial to remember that Good Policy Beats No Policy. We must be practical and not spend months or years trying to get a perfect policy in place (Northcutt, 2007). Good policy is a good start, and hopefully this policy will be improved to become great policy – a strong foundation on which effective security is built.

References

[1] Standards Direct, (2007). ISO 27002 - The Information Security Standard. Retrieved January 16, 2008, from The Standards Direct Electronic Shop Web site: http://www.standardsdirect.org/iso17799.htm

[2] ISO/IEC 27002. (2007). In *Wikipedia* [Web]. Wikimedia Foundation. Retrieved January 16, 2008, from http://en.wikipedia.org/wiki/ISO_17799

[3] Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. U.S. Department of

Commerce, National Institute of Standards & Technology. (2008). *Technical Guide to Information Security Testing and Assessment* (Special Publication 800-115). Gaithersburg, MD

[4] Northcutt, Stephen (2007). *Fundamentals of Information Security Policy.* SANS.

[5] Biermann, E., & Mlangeni, SA. (2009). Assessment of Information Security Policies within the Polokwane Region. Tshwane University of Technology.

[6] Grobler, T., & von Solms, SH. (2004). Assessing the Policy Dimension. Johannesburg, South Africa: Technikon Witwatersrand.

[7] Guel, M. (2007). A Short Primer for Developing Security Policies. Retrieved February 2, 2010, from SANS: Information Security Policy Templates Web site: http://www.sans.org/security-resources/policies/#primer

[8] McConnell, K. (2002). How to Develop Good Security Policies and Tips on Assessment and Enforcement. Retrieved February 2, 2010, from GIAC Practicals Web site: http://www.giac.org/practical/kerry_mcconnell_gsec.doc

[9] Kee, C. (2001). Security Policy Roadmap – Process for Creating Security Policies. Retrieved February 2, 2010, from SANS Reading Room Web site: http://www.sans.org/reading_room/whitepapers/policyissues/security_policy_roadmap_process_for_creating_security_policies_494?show=494.php&cat=policyissues

[10] Lindley, J. (2001). Technical Writing for IT Security Policies in Five Easy Steps. Retrieved February 2, 2010, from SANS Reading Room Web site: http://www.sans.org/reading_room/whitepapers/policyissues/technical_writing_for_it_security_policies_in_five_easy_steps_492?show=492.php&cat=policyissues

[11] Weise, J., & Martin, C. (2001). Developing a Security Policy. Retrieved February 16, 2010, from SUN BluePrints Web site: http://www.sun.com/blueprints/1201/secpolicy.pdf

[12] Weise, J., & Martin, C. (2001). Data Security Policy – Structure and Guidelines. Retrieved February 16, 2010, from SUN BluePrints Web site:

http://www.sun.com/blueprints/tools/samp_sec_pol.pdf

[13] Miles, G., Rogers, R., Fuller, E., Hoagberg, M., & Dykstra, T. (2004). *Security Assessment: Case Studies for Implementing the NSA IAM*. Rockland, MA: Syngress Publishing Inc.

[14] Swanson, M. U.S. Department of Commerce, National Institute of Standards & Technology. (2001). *Security Self-Assessment Guide for Information Technology Systems* (Special Publication 800-26). Washington, DC

[15] Etsebeth, V. (2003). Implementing information security governance. *Legal Implications of Information Security Governance* Johannesburg: University of Johannesburg.

[16] Mohan, F. (2003). Policing System Assets through Information Security Policies. Retrieved Feb 9, 2010, from SecureSynergy web site:http://www.securesynergy.com