# Global Information Assurance Certification Paper

# ISMS FOR A FIREWALL MANAGEMENT SYSTEM

MICHAEL S. ST. VINCENT

G7799 PRACTICAL ASSIGNMENT (VERSION 1.1)
SANS NETWORK SECURITY 2004



21 MARCH 2005

# ISMS FOR A FIREWALL MANAGEMENT SYSTEM

G7799 Practical Assignment (Version 1.1)

Michael S. St. Vincent

## Contents

## ABSTRACT

The ISMS is intended to assess and remediate security controls for an installed firewall management system at a large national financial services organization. The system includes a handful of servers providing the centralized control and reporting for approximately thirty firewalls located in several data centers utilizing ten differentiated rule sets through assignment of firewalls to rule collections. The system include a master console where configurations for all firewalls are established and distributed, a secondary console that operates as a hot-standby at a business continuity site, and the logging and reporting servers that collect and process the event logs from all the firewalls. While the system was initially maintained and utilized by a single team, interest in unifying all firewall systems management is now adding users for specified rule sets to allow sharing or delegation of rule set maintenance.

Several concerns drive the interest in reviewing this system as its use is expanded. First, while there has been great trust by management of the development of the system, the broader usage and the continuing increase in numbers of firewalls managed demands an appropriate rigor be applied to operational review. Second, management believes that a formal process certification (such as a SAS-70) is likely to be needed in the near future as a competitive differentiator; since the United States has not ratified a controls standard (such as the widely regarded BS7799), a representative but non-certifiable review utilizing the ISO-17799 is a valuable preparation. Finally, management believes that utilizing a review process to identify processes that lack adequate documentation or compliance will help target future staff effort more effectively.

The scope of the review will exclude the firewalls and the rules in the system except where these are directly relevant to the operational security of the management system itself.

## 1. SYSTEM DEFINITION

ACME has undertaken a proactive, structured approach to ensuring security to the benefit of its clients by developing an Information Security Management System (ISMS) for its core systems. While the company and the entities with which it interacts are constantly changing, systems security is expected to be a foundation upon which the company manages these relationships. Thus, the application of a process for protecting the enterprise firewall management system reflects the operating principles embraced by ACME.

The firewall management system is an installation of Check Point's Provider-1 system components running on Check Point's SecurePlatform (a Linux variant). The system as installed is intended to provide a redundant operating console for control of all enterprise firewall systems and a centralized and secure repository for the rule sets for all firewalls. There are currently about thirty main firewalls deployed in high-availability (HA) pairs and quadruplets in addition to about fifteen small, single firewall appliances. These firewalls are distributed in both purpose and geography. The centralized management is necessary to ensure a single operating model and to provide a single approach to activity monitoring on all firewalls in ACME.

The primary purpose of protecting the firewall management system is the control of the organization's firewall rules for creation, implementation, storage, modification and review. A breach of the rules by addition, modification or deletion would create impacts to the business of ACME ranging from a denial of service (DoS) to an exposure of other systems leading to a compromise of sensitive information or other protected content. Controls must be effective to ensure only designated firewall administrators may view, alter or implement rules or logs under appropriate authorization.

This ISMS addresses a single portion of the critical infrastructure systems of ACME and is being utilized as a practice effort in preparation for a larger assessment and implementation of a structured security practice for the organization.

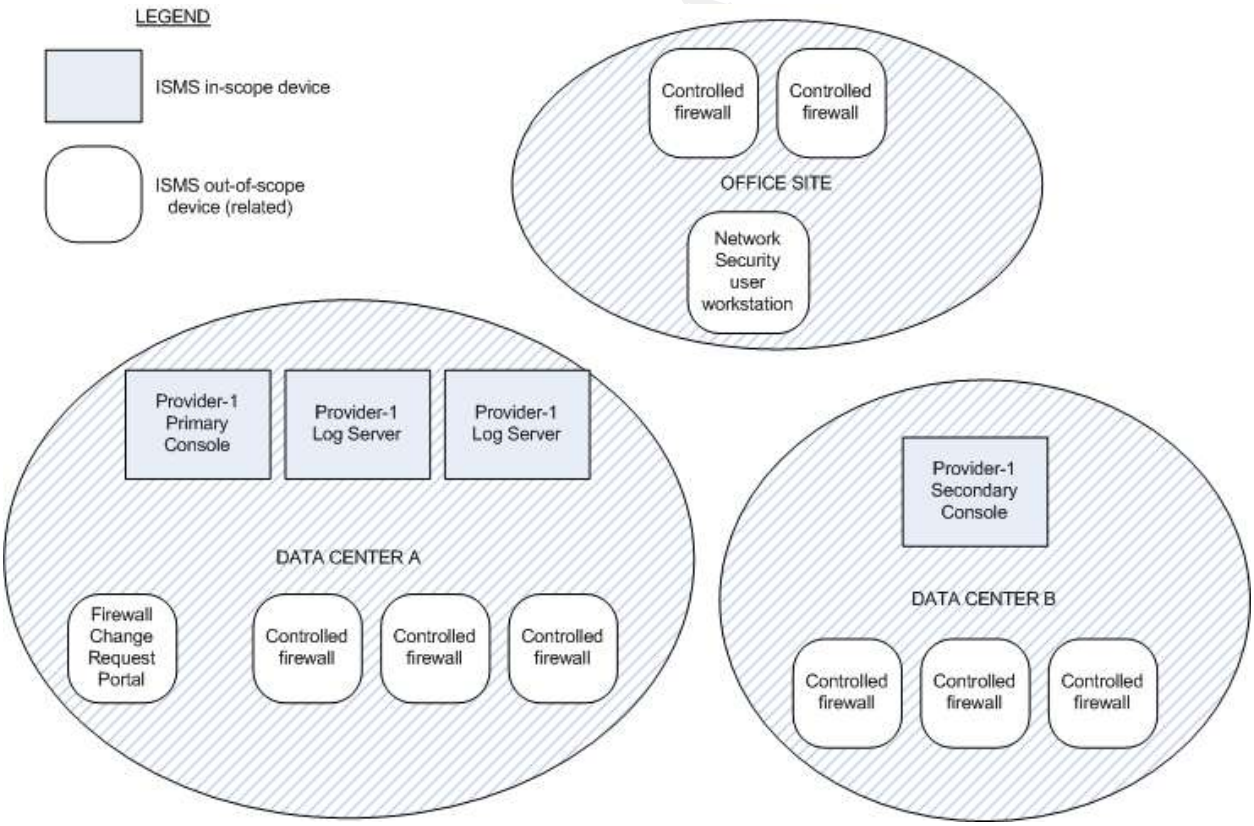
### 1.1. ACME AND ITS MARKETPLACE

ACME is a United States based enterprise of over 35,000 employees operating in several major business units performing financial services to clients from global corporations to single (wealthy) individuals. The organization is recognized as a reliable and innovative provider of expertise and one that utilizes technology to make its workforce highly mobile. Annual revenues are approximately $5 billion and the enterprise makes appropriate investments in technologies to provide redundancy and distributed presence

The information technology (IT) organizational structure is heavily centralized in one primary location in the southeastern United States with local support staff in most of over 100 local offices across the majority of the Unites States and its territories. The network security team is part of the Information Security services organization reporting to the Chief Technology Officer (a direct report of the CIO); this team has direct operational responsibility for the firewall management system, the firewall platforms (hardware and software) and the firewall change request process utilized by other teams within IT.

### 1.2. ISMS SCOPE

This plan is limited to the system which is defined as the centralized consoles, logging servers, and associated restricted networks. At the boundary of the system are the logical interfaces to the enterprise backup system, the routing point to access networks of the enterprise in general, and the physical confines of the computing platform cases. The image below provides a general identification of devices referenced in this document and their status as in- or out-of-scope.



The vendor-provided software utilized by users of the system to interact with it is at the boundary of the system and reviewed in its role in operating the system, but is presumed to be operating on a secured system which is out of scope of this review. Relevant security-impacting aspects of the client software is noted where appropriate as part of the interface to the system.

The environment in which the system operates is generally outside the scope of the system itself, but is recognized in the system review as an important part of the overall security of the system.

The managed firewalls are also outside the scope of the system, but do interact with the system in significant ways. Due to the interaction, the firewalls are included in so far as the interaction has a security ramification.

The web-based firewall change request portal utilized by requesters, the network security team (implementors) and Information Security management (approvers) is a separate system and is considered outside the scope of the firewall management system. While recognized as a tool utilized in some of the control processes, the security management practices for the portal system is managed by a different group than the network security workers. Use of the portal as augmenting or supporting controls is within the scope of the review.

### 1.3. OVERALL STATE OF SECURITY IN ACME

ACME has taken an continual improvement approach to systems protection over the past five years with the establishment and development of an Information Security department chartered to identify, measure and, as possible, mitigate and remediate information risks in the organization. This effort has resulted in a formalization of operational security practices and centralization of various security activities (including the firewall management).

Management has determined that the marketplace has increased in awareness of security certifications of operating facilities as a differentiating factor between vendors. In ACME's own procurement of services, vendor assessments have included review of completed SAS-70 or similar certifications; this has led to the presumption that lacking a certification may become a liability in competing for clients. This ISMS and anticipated subsequent certification through other processes is the next step in the continual improvement of operations and information security practices across the enterprise.

### 1.4. APPLICABLE PROCEDURES & PROCESSES

Procedures for processing firewall changes have been established for several years with reviews performed annually to ensure that any changes in practice are included. These are posted on a nationally-available intranet site along with other security procedures. The procedures imply de-facto policies, but policies do not exist in a formal manner.

In support of the procedures, a web-based firewall change request portal is on the intranet. The portal has access control and workflow to enforce the procedures utilizing the user's account and the assigned role. Briefly, the portal provides for the entire process: request creation (by an authorized requester), submission (requester), review (firewall team), advancement for approval (team), management approval or rejection (management), implementation (team), and change acceptance (requester). In addition to the enforcement of actions based on role, the portal provides restrictions on view of requests so that one requester is unable to view or alter a different requester's submission, even if in possession of the appropriate record locater information. This portal was developed in Autumn 2004 and has proven to be a major improvement in communication, workflow and role-enforcement from the prior paper-based request method.

The firewall management system also provides some granularity of control for users. Each user has a separate account and each computer system communicating with the console must come from a pre-registered IP address and must utilize a system-signed digital certificate to provide encryption of the session. Firewalls are grouped into logical collections or “containers” that share common rules for ease of management; the system provides access control roles so that users may be provided different levels of access (full, read-only, or no access) to different containers. Finally, the access to the log servers is also separate from access to the management of the rules so that read-only access to the logs without access to the rule containers (or vice versa) may be configured. While accounts and their access have been restricted following the principle of least-privilege, policies and procedures regarding system account provisioning are not documented.

Provider-1 also utilizes its certificate-issuance to provide encrypted communications between the system and the managed firewalls. Firewalls are brought under control of the Provider-1 system through an enrollment process that licenses the firewall software from the authorized pool of licenses and downloads the firewall's unique certificate for all control and logging communications.

### 1.5. OBSERVATIONS OUTSIDE THE SCOPE OF THIS ISMS

General data processing activities and requirements are handled following standard practices for ACME's data centers, but documentation lacks for these. Much of this falls outside the scope of this ISMS, but management of the appropriate areas will be reminded of the importance of reviewing the need for documentation that may benefit all groups with equipment in the data centers. This would support future ISMS reviews for other systems.

## 2. PLAN PHASE

### 2.1. IMPROVEMENTS RECOMMENDED

The initial review committee was selected as two members of the network security team, a member of another security team (for an outsider's view) and the manager over the the technical security teams (with responsibility for the firewall management system). This group was chartered to perform the following major efforts to establish a baseline ISMS:

- Gather all identifiable policies, procedures and standards already documented
- Identify major gaps in policies, procedures and standards that could be reasonably addressed in the first review cycle (three months) by existing staff in the network security team
- Analyze, rate and rank the identified gaps with regard to risk
- Provide guidance to staff in remediation for the first cycle with recognition that the reviews would recur to obtain incremental improvements over time

The overall effort for the ISMS was determined to be approximately one hundred (100) hours of effort, with about one-half the time spent in committee and audit meetings and the remainder on ISMS documentation, policy development, and implementation of new processed and/or procedures. This will take place during a compressed time line of six weeks so that the initial effort is completed on a quarterly boundary; thus, the first regular review cycle will have the normal three-month period to perform review and further improvement. Given that the scope of policies and procedures is very localized (impacting, in general, only one team), the management approval cycles are presumed to be short (weeks at most) and will not require review above the senior manager level.

The identification of risks by the committee began with a table-top audit of the practices and systems; staff familiar with the configuration and operation of the firewall management system were interviewed by the panel utilizing a combination of the BS 7799.2:2002 standard and an internally-developed vendor assessment questionnaire. Identified concerns were then grouped and those perceived to potentially carry the greatest risk were analyzed utilizing a modified version[1] of the Risk Dynamics method.

1 The Risk Dynamics analysis methodology was utilized with the following modifications: cost to deploy was considered a sunk cost by management; vulnerability, consequences, and recovery time were separately considered but combined for the report; and detection and response times were factored into the likelihood of occurrence which was of significant interest. The FMECA severity scale was used to measure the vulnerability/consequences as it was deemed most descriptive by management.

It is the belief of management and senior staff that the process of examination will result in improvements in several ways. A verified and verifiable level of operations discipline will be achieved; knowledge transfer and on-the-job training will occur within the team in the course of completing process documentation; efficiencies are likely to be identified; and, overall security for the system will be improved. In each of these there is an improvement in readiness for a future data-center scoped assessment that is anticipated within the next few years.

### 2.2. ISMS MANAGEMENT APPROACH

After the initial review by the committee described in section 2.1, it is recommended that a permanent committee be formed to continue the work of the quarterly reviews.

Due to the limited scope of this ISMS, a single management committee with an approving sponsor will be used. The committee includes no less than four and no more than six participants to ensure the group is sized to accomplish the task but not difficult to guide. The makeup of the committee is as follows:

- Manager of technical security[2] teams (chairman) – overall responsibility for ISMS report compilation and coordination of documentation and corrective actions
- Two members from network security team (including technical lead) – responsible for procedures, configuration of system and ensuring that changes in policy/procedure/standards are both realistic and communicated effectively to the other staff members
- One or more members from other Information Security teams – responsible to provide objective but interested development of policies and review of procedures to ensure alignment to policies
- Others outside Information Security as deemed beneficial[3] -- responsible to provide an outsider's objective review of the policies, the verification processes and the impact of such policies and procedures on firewall change requesters.

Providing oversight, guidance and support to the management committee is the director of Information Security. The director also has executive responsibility for the outcome of the ISMS.

2 Including network security

3 These will generally be either interested stakeholders in the processes and/or will be those from teams preparing to attempt similar ISMS activities whose participation is to learn the ISMS process used by ACME.

The firewall management system will be reviewed quarterly to allow implementation of identified changes in smaller steps without losing focus on the improvement of the system over time. Both the management and staff are committed to improving the security of this system as a model for other efforts and as a responsibility to ensure the systems that the information security staff are an example of proper systems management to other groups.

Since this ISMS is an early adoption of the process life cycle for improving security practices and there is an anticipation for extending such reviews to portions or all of the major data centers, it is likely that this committee will become subordinate to a larger ISMS committee with focus on Information Security systems. The makeup of an overall ISMS committee is not yet being discussed.

## 2.3. POLICIES TO BE IMPROVED/DEVELOPED

### 2.3.1. INFORMATION SECURITY PASSWORD POLICY

**Policy name:** Information Security Department Passwords

**Purpose:** In recognition of the sensitivity associated with user accounts of the members of the network security team, the policy states requirements for Information Security Staff utilization, creation and maintenance of strong and frequently changed passwords for Information Security managed resources. This practice also preserves the confidentiality and integrity of the ACME's data by only allowing authorized users to access protected information.

**Audience:** All members of the Information Security department, with special emphasis on those staff members with administrative or otherwise highly-sensitive access credentials.

**Areas of standard that will be addressed:** Standard 9.3.1 addresses user responsibility for password management and the issue of whether ACME has supplied written procedures to appropriate staff. While recognized as an appropriate requirement, ACME currently lacks an Information Security staff policy document. The policy document is recognized as and important document to create, providing staff with guidelines for maintenance and creation of passwords.

### 2.3.2. ANNUAL RULE REVIEW

**Policy name:** Firewall Rules Review

**Purpose:** Due to the operational risk of rules being present in the firewalls to permit access after the appropriate business reasons are past, a review policy and procedure is required to support the staff's informal review process with more structure and authority. The policy will state the need to review and will authorize the removal of any rules lacking current need or continuing sponsor.

**Audience:** The Policy will serve two purposes. First, the policy will provide authorization and instruction to the network security staff to regularly perform the reviews and properly process any obsolete rules out of the system. Second, the policy will inform all rule change requesters of their responsibility to annually re-confirm the business and technical requirements for the access granted.

**Areas of standard that will be addressed:** The standard 12.2.1 requires regular reviews of systems to ensure compliance is not compromised by lack of proactive checking; this will ensure that the firewall management system is not indirectly compromised through lack of review.

### 2.3.3. FIREWALL CHANGE POLICY

**Policy name:** Firewall Change Requests

**Purpose:** Since changes to the firewalls have critical impact on perimeter security, this policy establishes a formal and structured methodology for those changes. Having a single method for requesting firewall changes reduces the potential for errors.

**Audience:** The policy addresses anyone who would request a firewall change. Generally, this would be information technology staff.

**Areas of standard that will be addressed:** Standard 8.1.4 requires that processes exist to segregate duties to avoid unauthorized changes; this policy requires that the requester, the processor (network security staff) and the approver be different parties to reduce the risk (by review) of inappropriate changes being implemented. Additionally, standard 9.4.1 requires that network

services use is controlled; this applies in that the firewalls managed by the system enforce restrictions and, thus, the procedures for making changes is a control over network services utilization.

### 2.4. CURRENT MAIN RISKS APPROACHED

Following is the summary from each of three “high” risks identified during the “table top” audit of the system.

#### 2.4.1. PASSWORD POLICY ENFORCEMENT

Given that individuals tend to (manually) synchronize disparate system passwords and choose poor passwords unless forced through controls to do better, the compromise of another system's password store or exchange could compromise the firewall management system through the unauthorized use of stolen credentials. Considering that the system does not age passwords, weak passwords can remain indefinitely. The identified risk is lack of both policy and mechanisms to prevent these scenarios.

**Nature of threat:** Serious – Use of weak passwords that are also used for other systems creates an easy-to-compromise entry point through the authentication mechanism protecting system access. Due to other systems' password hashes being sent over the general network frequently, likelihood is high that a “targeted” system user may have their other system's password hashes captured and decoded.

**Vulnerability:** Catastrophic – The system must be protected from unauthorized user access, but authentication currently is through the use of passwords as a single factor form of authentication combined a loosely-coupled second factor.[4] Contributing vulnerability factors include lack of enforced password complexity; lack of policy or procedural-based approach to password creation; lack of password audits; and lack of enforced password aging. Successful password compromise would allow an attacker to make any desired changes within the system.

4 The IP address originating the session must be in a table of approved addresses to connect to the Provider-1 console server. This “second factor”, however, is not coupled to the user login information: any authorized account may login from any authorized IP address. This is a modest additional control factor.

**Likelihood of occurrence:** Moderate – For an interested insider attacker, the access to other systems' authentication traffic is easily obtained. While all users of the system should be aware of the risk of reusing passwords and of the need to avoid weak passwords, the likelihood of recycled passwords is still moderate to high.

**Risk level:** High

**Control selected:** Policy regarding network security team password practices; establishment of strong password technical controls[5] (enforcement) – standard 9.3.1 “Password Use”

**Reasoning:** Policy requirements will more clearly define the expectation that users with access to the system are required to utilize unique passwords that are appropriately complex to protect the system from unauthorized use. Technical enforcement (data validation on the password for complexity) will help reinforce the requirement by rejecting poor passwords.

**Risk level after implementing control:** Moderate – Password complexity is easily achieved when appropriate policy requirements and automated enforcement mechanisms are placed as demonstrated with other systems in the organization already.

### 2.4.2. ANNUAL RULES REVIEW

While the stated policy is that all firewall rules are subject to an annual review for continued need and the requirement that the requester re-assert the continuing business requirement, a review process is not formalized. Due to inheriting the original rulebase[6] from the telecommunications group, efforts have been spent over the course of two years to slowly and methodically identify traffic (via log review), classify it and use the data to build new rules for legitimate legacy traffic. The completion of the informal cleanup effort provided a base from which to begin review of approved rules on record, but the process has not begun.

5 The manual control that will be used is a password complexity enforcement mechanism in Active Directory (“AD”). The Provider-1 system allows for external authentication via secure LDAP and other methods. Since the AD system is also separately audited, there will be checks outside of the firewall management system that enforce this control.

6 The original rulebase was actually a set of network routes that allowed data to pass across a border router.

**Nature of threat:** Moderate – If rules are not reviewed on a regular (annual) basis, the possibility of having obsolete access in or out of the network increases dramatically. While some rules have specific end dates at creation and others are indeterminate, project access requirements change over time. Regardless of how the obsolescence is determined, rules should be removed when no longer needed.

**Vulnerability:** Catastrophic – If a rule has allowed access to a machine that is no longer performing a given task, unexpected access may exist. Alternately, another machine may re-utilize the same IP address to which an obsolete rule allows access; the access would then expose the new server. Allowing unforeseen access to a server may lead to a compromise of it and its contents or may allow an attacker to use the server as an entry point into the network.

**Likelihood of occurrence:** Moderate – The likelihood that a rule is obsolete depends upon the total number of rules in the rulebase and the period that the rules have been in place. With a rulebase that has over 150 rules and has been in use over a year, it is very likely that at least one rule is no longer authorized or is no longer needed.

**Risk level:** High

**Control selected:** Monthly review of expiring rules against business requirement to retain access – standards 9.4.6 “Segregation in networks” (perimeter security mechanisms); 12.2.1 “Compliance with security policy” (regular review); and 9.4.2 “Enforced path”

**Reasoning:** The controls are directly related to the issue; the need for restricted access to/from the server/data is a necessity. If there is a clear need to restrict access to only authorized access, it is necessary to ensure that rules in place are still relevant and accurate.

**Risk level after implementing control:** Low to Moderate – Risk is reduced based on guarantee of detection occurring within a single year for any given rule, rather than a constantly compounding risk of obsolete rules building in the rulebase.

### 2.4.3. FIREWALL CHANGE REQUEST REVIEW GUIDELINES

The information security analysts on the network security team perform a review of each firewall change request before advancing the request for management approval. General instruction has been provided to staff regarding verification that the request

meets technical requirements[7], but staff has expressed concern that they are uncertain what additional factors lead to approval or rejection; there is an apparent inconsistency (from the staff perspective) in the management review process regarding qualifiers. No documentation outlines business requirements to guide staff in better pre-screening requests.

**Nature of threat:** Serious – Staff lacks the procedural documentation to assist and ensure correct analysis is made. To compensate, staff often invokes management for input or additional guidance in making review decisions before requests are advanced for final management approval.

**Vulnerability:** Critical – Improper or high-risk rules are added to the rulebase due to inadequate review for risk and impact by analyst staff. If the data presented to management is incomplete, under-represents or varies in stating the operational risks, management judgment is indirectly impaired in being the business units' defense against excessive risk.

**Likelihood of occurrence:** High – A review of recent requests indicates that there is very likely a variety of staff interpretations of what should be considered in the technical risk review of a rule before presentation to management for implementation approval.

**Risk level:** High

**Control selected:** Creation and provision of a reasonably short checklist to aide analysts in reviewing and rating key risk factors for presentation to management during request approval cycles – standards 8.1.1 “Documented Operating Procedures - Communications and Operations Management”, and 8.1.2 “Operational Change Control”

**Reasoning:** ACME does not have a detailed procedural document that staff can utilize during the firewall change process.

**Risk level after implementing control:** Moderate – Improving the focus of information collected for change requests will support the network security analysts in being consistent and complete during the information gathering process.

7 Technical requirements include hostname matching given IP address, servers meeting configuration standard review cycle requirements and similar easily verified elements of a request.

## 3. DO PHASE (IMPLEMENTATION)

### 3.1. REMEDIATION PLANS

#### 3.1.1. PASSWORD STRENGTH REMEDIATION

**Problem & obstacles:** Some staff have suggested that the passwords in use have been unchanged for long periods of time and/or are not strong passwords. As security professionals, however, there is recognition that this is simply based out of a lack of enforcement leading to a lack of attentiveness to this issue.

**Actions required to resolve:** A publication of a policy with specific standards and sample passwords to emphasize proper password construction is needed. Also, the Provider-1 system will be configured to utilize the centralized authorization source of Active Directory which has automated enforcement mechanisms. Instruction to staff and an announced follow-up password review (informal) will strengthen the indication of management's intent to have this practice followed.

**Action plan:**

- Create review policy and obtain manager approval – estimated time: one week
- Instruct staff on new policy and notify of conversion date for authentication source – estimated time: one day
- Configure Provider-1 to utilize Active Directory authentication via RADIUS – estimated time: one week

#### 3.1.2. RULES REVIEW IMPLEMENTATION

**Problem & obstacles:** The work practices of the network security team do not include a formal rule review due to a lack of organization and reporting support. No reporting script exists to identify the rules that are expired (per original request time) or are due for annual recertification. Without an automated approach to identifying the target rules, it will be difficult to arrange staff to identify what to review given the hundred of rules in the system.

**Actions required to resolve:** The informal attempts to keep the rulebase “clean” indicate that the staff is ready and willing to perform the task. A policy for staff reference (to defend against uncooperative requesters) and a report to identify which rules to

review must be created. Once available, staff will need to be instructed on the new process and supported by management with adequate time to process the list each month.[8]

**Action plan:**

- Create report providing rule record number, review type (annual or rule-expiry), and review due date – estimated time: one week
- Create review policy and obtain manager approval – estimated time: one week
- Create review procedure for staff, including verification by staff that it is practical to execute – estimated time: two weeks
- Send policy announcement to all requesters of record and respond to initial concerns – estimated time: two weeks
- Instruct staff on new procedure and set enforcement start date – estimated time: one week

### 3.1.3. REVISED FIREWALL REQUEST REVIEW PROCESS

**Problem & obstacles:** The current review process for firewall change requests is structured around the procedure for requesters rather than an internal procedure focused on risk identification and analysis. Lacking a structured approach, staff makes best-effort reviews based on individual personal methods for determining risk rather than using an objective standard.

**Actions required to resolve:** A procedure and a simplified risks-review checklist are required to provide the structured and repeatable review of requests. Also, during the initial application of such a process, additional training (and tuning of the checklist) will be required.

**Action plan:**

- Review, at minimum, ten requests where management sent questions back to staff for risk clarification or identification; summarize results to identify common elements for checklist – estimated time: one week
- Provide draft checklist to management for review and comment – estimated time: one week

8 A monthly review appears to be appropriate in that it offers both flexibility in scheduling over a period of time without being so long that the task is not addressed.

- Provide revised checklist to staff for review and comment – estimated time: one week
- Create final review procedure and checklist and obtain manager approval – estimated time: one week
- Instruct staff on new procedure and set enforcement start date – estimated time: one week

## 3.2. CONTROLS & STATEMENTS OF APPLICABILITY

### 3.2.1. ESTABLISHMENT OF TECHNICAL PASSWORD COMPLEXITY CONTROLS (ENFORCEMENT) – STANDARD 9.3.1 "PASSWORD USE"

A careful review of the available password control mechanisms in the firewall management system identified both strengths and drawbacks. As with many security management products, it appears that built-in security controls (such as strong password enforcement) is missing in the base product. Provider-1 does provide, however, optional external authentication methods. This provided the ability to utilize the implemented password-complexity enforcement of ACME's Windows Active Directory structure.

The Active Directory system, as implemented at ACME, enforces password complexity and expiry. Current standards force password change after ninety (90) days. Current password complexity enforce the requirement of three of four character types being present in passwords, but dictionary-word use (with symbol substitution) is not enforced. Since the Active Directory provides greater enforcement that the Provider-1 system and is already subject to periodic audit and logging, it has been chosen as an appropriate enforcement mechanism to support the password policy and standard published.

An additional benefit is that this aligns the firewall management system with a more general drive towards a reduced sign-on ("RSO") initiative. This RSO effort is reducing the number of independent authentication systems/sources and, as a side benefit, is resulting in a greater number of systems being compatible with a single sign-on ("SSO") effort.[9]

### 3.2.2. RESTRICTING ROUTE BETWEEN WORKSTATION AND FIREWALL MANAGEMENT SYSTEM – STANDARD 9.4.2 "ENFORCED PATH"

During the initial review, the committee identified the need to limit the route between the workstations running the firewall management system console software (users) and the core system. This was based on the ability of Provider-1 to limit from which IP

9 RSO is the concept that the same username and password tuple, as maintained in a single authentication system, is utilized by various systems for login. SSO takes the concept further such that once a user logs into a workstation, applications launched (such as web sites) automatically recognize the workstation-verification of the authenticated user and do not challenge again. Under RSO, authentication is obvious each time is occurs; under SSO it is transparent to the user.

address user workstations connections would be accepted. After further review, it was determined that there are a number of other controls that provide enforcement that make rote control both excessively burdensome and unnecessary.

First, all communications between the workstations and the core system are encrypted with asymmetrically-keys channels. This enforcement is enforced by the design of the Provider-1 software and cannot be undermined. This feature was one of the supporting controls identified during the procurement of the system, but committee members were unaware of this important nuance.

Second, routing is controlled by other teams and may be subject to compromise without warning to the staff or management of the firewall change management system. Thus, it is not a reliable control and cannot achieve complete mediation.

Finally, some of the routes necessary to support the communication between the primary components and the secondary (business continuity site) components of the system are shared with many other systems due to cost constraints. As all communications are encrypted by default, further data segregation is not necessary.

While this control was determined to not be applicable, the discussions held regarding the need provided the committee greater understanding of controls already extant.

### 3.2.3. DEVELOPMENT OF OPERATING PROCEDURE DOCUMENTS FOR STAFF – STANDARD 8.1.1

The need for operational procedure documentation was identified by management during an informal review of all data center systems, but it was believed that the basic documents for business continuity and firewall change requests addressed most needs. Upon more careful review it was determined some aspects of daily system operations needed more attention.

The review of change requests was inconsistent and lacking the important guidance necessary to ensure the protection to the firewalls management by the system. This is being addressed by the development of a set of review standards (a “checklist” of common risks) for staff to utilize in presenting request evaluations to management. This will ensure that all staff are reporting on the same risks in a consistent manner and management will have a basis for assuming that the presentation of risk is consistent.

A discussion of password usage also indicated that a statement be developed regarding the responsibilities of information security staff that exceeds that of others in utilizing best practices for passwords. In addition to the technical controls, raising awareness and stating/documenting policy (rather than assuming it is known) is part of the documentation for operations on the firewall management system.

The audit cycles for the operational documentation should confirm both the existence and the regular familiarity and use of it. Several operational activities (backup and restore, system build standards and so on) are documented under the standing business continuity plan. While quarterly verification of the plan being current is already mandated through other programs, these should be audited to ensure that the process is working.

The review of documentation controls has been very positive in improving the practices by raising management's awareness of the inconsistent standard used to measure risk and the true interest from staff to remedy this shortcoming. In addition, the perception of an audit being utilized for positive change (rather than strictly for "punishment") has grown among staff. Several of the network security are interested in continuing to improve the practices utilizing the audit checklist as a starting point for examination.

## 4. CHECK PHASE

The committee worked individually and as a team to develop checklists relative to the standard 8.1.1 regarding documented operating procedures. Several of the first round actions identified as improvements to the system involved documentation, so this control was clearly indicated as requiring a solid checklist to ensure that the effort was not diluted through lack of adequate audit.

The checklists are organized by documented procedure and the associated activities that the procedure is intended to enforce.

### 4.1. GENERAL SYSTEM DOCUMENTATION CHECKLIST

This checklist will verify that all the major procedures are documented and reviewed for currency (as appropriate). This addresses both the concern for having actual accurate documentation (rather than all processes being “in people's heads”) and the concern that the procedures that are less frequently used (such as disaster recovery steps) still reflect the actual operating environment.

1. Is there general firewall management system operations documentation for staff?

   1.a. Obtain a copy of the firewall management system operations guide (s) from management. Verify with staff that the documentation is generally available and known to them.

   1.b. Identify a single daily operational process (such as adding a rule to the rulebase) in the documentation. Review the process with a staff member to ensure that the documented process is accurate with current practice. Note significant discrepancies.

   1.c. Verify through interview with management that there is a feedback process and owner for the document or for all subsections of the document.

   1.d. Verify through interview with management that there is a process to ensure documentation is reviewed and updated (as needed) during each major version upgrade of system components.

2. Is there requester instructions for making firewall change requests?

   2.a. Request a copy of the Firewall Rule Change Procedure from management.

2.b. Identify and interview a requester who has made multiple requests within recent periods. Determine whether the person is familiar with and can easily access the procedure from a location that is available to all requesters.

2.c. Verify through interview and, if practical, an actual request being performed, that the process the requester follows is not significantly different than the documented procedure.

3. Is there a change request verification checklist used by staff to ensure consistency in request validation?

   3.a. Request a copy of the checklist or procedure used by staff to prepare a request for presentation to management for approval.

   3.b. Interview a network security staff member to determine whether the checklist is utilized regularly. Determine whether there are frequent occurrences of information requests from management that wuold suggest that the list is not complete or is not properly focused on relevant issues for staff review.

4. Is there a documented procedure for annual review of all rule base changes?

   4.a. Follow the audit checklist (see below) for “Annual rule review”.

5. Is there a patching process document in use?

   5.a. Request a copy of the patching policy or procedure(s) from management that apply to the system.

   5.b. Interview staff to determine whether the policy/procedure is being followed. Verify that staff has familiarity and access to the patching documentation.

   5.c. Verify through interview and guided inspection of audit trails and/or code in production that patching is current as required by the documented policy/procedure.

6. Is there business continuity and/or disaster recovery procedure documentation?

   6.a. Obtain from management a copy of the recovery procedure(s).

   6.b. Determine whether the documentation addresses: ownership of procedure, who may declare the procedure “in effect”, contact information and methods, and dependencies for this system's recovery.

6.c. Verify that the document has a regular review cycle. Verify that it has been reviewed according to the cycle timing.

6.d. Determine the extent to which the recovery procedure has been tested and the results of the most recent test. Determine whether difficulties have been addressed through procedure revision.

6.e. Verify that multiple copies of the procedure exist in locations that are distributed according to the plan requirements. Verify that in the identified major disaster scenarios, the intact procedure copy would be reasonably available from one of the alternate locations.

### 4.2. ANNUAL RULE REVIEW AUDIT CHECKLIST

This checklist will help ensure that all rules previously submitted (and approved for implementation) are reviewed annually to decrease the risk that an aging rulebase may unintentionally allow unauthorized access to servers that either no longer exist or to addresses re-purposed to a server that may perform a different task.

1. Does a policy exist?

   1.a. Request a copy of the Annual Rule Review Policy from management.

   1.b. Interview staff to determine whether staff is familiar with and has access to the policy.

   1.c. Verify that the policy is reasonably available to the requesters.

2. Does a report exist that shows which rules are expired?

   2.a. Obtain a copy of the monthly “rules due review” report.

   2.b. Obtain a database dump of rule review dues dates which are older than today and verify that those items are represented on the production “rules due review” report.

3. Are the end user and network security notified when a rule expires?

   3.a. Select a rule on the report. Determine whether the requester of record and contact them to determine whether they received a notification from the system of their rule's review anniversary.

   3.b. For the same rule, determine whether the network security staff received notification of the rule's anniversary.

4. Is user forced to act in order to keep the rule in place?

4.a. Identify a recently reviewed and renewed rule. Verify through interview of the requester that they were required to take positive manual actions to cause the renewal to occur.

4.b. For the same renewed rule, verify through interview of the approving manager that positive manual actions were required to approve the renewal.

5. Are rules determined to not be renewed proactively handled?

5.a. Identify a rule that was identified for removal through the requester positively choosing to not request renewal. Verify the requester choose to decline the renewal and the action generated a deletion request.

5.b. Identify a rule that was removed due to lack of action by the requester. Verify that a request was generated after a pre-determined period for removal due to lack of response from the requester of record.

5.c. Identify one or more rules that were indicated for deletion (regardless of reason). Verify through inspection of the active rulebase in the firewall management system that the rule(s) are not present in the rulebase.

5.d. Verify for deleted rules that the audit trail indicates who performed the removal and when the rule was deleted.

6. Did the rule get updated to show another year of validity if business case is proven?

6.a. Identify a rule that has completed at least one renewal cycle. Verify through inspection of the audit trail that the business case for renewal was stated with the date and person making the assertion recorded.

6.b. For the same rule, verify that the renewal period was for one year (or less) from approval and not longer.

7. Does a report exist that would show any rule that is older than 13 months?

7.a. Request a copy of a report that would indicate exceptions to the review process. Specifically verify that the report either solely focuses upon or significantly highlights rules not renewed and not deleted which are over one month overdue on renewal.

## 5. ACT PHASE

The initial ISMS committee has identified several administrative issues with the existing system and management is supporting the implementation of remediations. As part of their charter, the initial committee is providing recommendation for the ongoing participants in the standing ISMS for the system. This is described in section 2.2.

During the review of historical firewall change requests, it was noted that a high percentage of requests were “emergency” requests. While there may be business reasons for a limited number of such rapid changes, the more limited technical review of such changes introduces additional risk. Two significant efforts are required for the next quarterly review cycle: first, a determination of the root causes for requests being placed in to the emergency cycle (to determine whether there is abuse) and, second, a consideration of how to alter the process, awareness or emergency approvers list to accomplish a reduction in the ratio of emergency- versus normal-cycle requests.

Some requesters have noted limitations in the firewall change request portal for larger or more complex change requests. While the portal is out-of-scope to this ISMS, the requests have been passed along to the portal support team for future implementation. It is recognized that improvements to the tools supporting the system result in improvement to processing efficiency and accuracy.

Due to the reliance on two other portal systems (the firewall change request portal and the server assessment request/reporting portal), it is being recommended that the scope of this ISMS be expanded in future review cycles to include those systems. This recognizes that the data in those systems is critical to the daily processes of maintaining rules in the firewall change management system and to the audit of the firewall change system. This request also aligns with management's stated goal of expansion of the ISO 17799 methodology to the entire data center and the systems within it.

Finally, the initial review of the system has heightened staff awareness of the latent security concerns with the existing deployment. As a “showcase” system for the further expansion of the ISO 17799 methodology in the organization, management is developing a process for staff and requesters to submit suggestions for process improvement. While this initially will be informal, the acceptance of such input indicates a more proactive stance to improving this established system.

## 6. BIBLIOGRAPHY

The following reference material was utilized in the review and documentation process by the author and the initial-round ISMS committee.

*ISO 17799 process-specific material:*


- Introduction to BS ISO/IEC 17799: Policy, ISMS and Awareness (course book 11.1); SANS ( Hoelzer, David, editor); 1994.
- Risk Management, Security Compliance and Audit Controls (course book 11.5); SANS ( Hoelzer, David, editor); 1994.
- Information Security Management BS7799.2:2002 Audit Check List for SANS; Thiagarajan,Val; 2003.


*General systems security and risk analysis:*


- Secure Computers and Networks: Analysis, Design, and Implementation; Fisch, Eric A. & White, Gregory B.; 2000.
- Managing Information As A Corporate Resource; Tom, Paul L.; 1987.


Additional materials utilized included internal organization documents that are not referenced to mask the identity of “ACME”.

## 7. APPENDICES

### 7.1. INFORMATION SECURITY PASSWORD POLICY & STANDARDS

#### Purpose

This document outlines requirements for Information Security Staff utilization, creation and maintenance on Information Security managed resources. This practice also preserves the confidentiality and integrity of the ACME data by only allowing authorized users to access protected information.

Passwords will not be manually synchronized between differing authentication authorities. Each system type accessed will be configured with unique passwords. For example, a user will not configure their password for their email account so that it is identical to the password utilized to access the firewall console.

Password changes on the primary internal Windows domain are required to be changed every ninety days. When the Windows domain password expiration notice is received, users are required to also change passwords in other authentication systems. The following standards should be utilized in the creation of a password.

#### Password Strength Standard

Passwords are used to access the network, email, intranet websites and other applications. Information Security staff access appliances that protect the ACME networks, systems and data. Strict attention must be paid to password characteristics, whether or not system-enforced. All users must ensure that passwords are not re-utilized between separate authentication domains.

Strong passwords have the following characteristics:

- At least seven (7) characters in length
- Previous ten (10) passwords cannot be used
- Contain at least three (3) of the following four (4) classes of characters:
  - English uppercase letters (A,B,C,…)
  - English lowercase letters (a,b,c,…)
  - Westernized Arabic numerals (0,1,2,…)
  - Non-alphanumeric (special) characters (#, &, !, %,@,?,* and so on)

Strong passwords do not have the following characteristics:

- Contains user name or portions thereof
- Contains first or last name or portions thereof
- Consists of a single word in a dictionary with a number or special character at the beginning or end[10]

Additionally, passwords should not be written down or shared unless the authentication domain does not technically provide for unique passwords per login account. A password should be changed immediately if it is suspected that it has been compromised (an unauthorized person has unrestricted access to it).



10 Using multiple words with a number or non-alphanumeric character is acceptable as a strong password. Examples of a strong password include DOG6cat and CB354-a.

This checklist has been developed for use by the network security staff to ensure that all reviewers have the same framework for evaluating requests before presentation to management for implementation approval. This represents both the results of research in request archives (for additional information requests from management) and interviews with staff to obtain their undocumented review points. Review and revision of this checklist is recommended at least annually.

**Part I: Initial sanity check**

- Are appropriate services requested per application definition?
- Are there no extraneous services or protocols?
- Has technical need been confirmed for:
  - Bi-directional (externally initiated communications)?
  - External access to intranet? (Is business justification given?)
  - Application owner approval for access?
- Can the source or destination network range be narrowed or made more restrictive than requested?

**Part II: Appropriate services and their location in the network**

- Does the database administrator team manage SQL servers in request?
- Has the server completed a security assessment in the past sixty days?
- Has the application completed an automated application vulnerability review?
- Is SSL being used (for web applications)?
- Does a standard service exist for ports requested for opening?
  - Can Terminal Services be used as opposed to NetOp, PCAnywhere, VNC?
  - Can secured file transfer service be used as opposed to FTP?
- Is the server in the correct network location for the hosted service?
  - Internal domain

- Internet DMZ
- Database secured subnet

**Part III: Functionality checks**

- Will requested services operate as requested (use of standard ports)?
- Has the requester provided information on services on non-standard ports?
- Does another workaround already exist which will meet the requester need?

**Part IV: Unusual risks**

- Is the service/data access offered a gross risk to the organization (high sensitivity)?
- Are steps taken to reasonably mitigate major risks (controls in services)?
- Are waivers necessary for exceptions to server security assessment? Are they properly authorized (Director level or above of information owners management chain)?
- For connections to external parties, are appropriate equivalent security practices present? Does the other party utilize anti-virus, patching and other measures to provide protection against transitive risks?

**Part V: Approvals**

- Has network security management approval been requested and obtained?
- Have all the involved support groups been notified and approval given for use?
  - Has messaging team approved any used of SMTP?
  - Has database team approved access to database servers?