Global Information Assurance Certification Paper

Information Security Management System

for

Patch Management Systems

By: John Hanna

G7799 Certification
Practical Assignment, Version 1.1
Submitted on: December 21, 2004

Course: SANS 17799 Security and Audit Framework
SANSFIRE 2004, Monterey, CA

Table of Contents

Abstract

The organization in question is a U.S. based financial institution. The main business of the organization is lending money.

The organization's internal Information Technology (IT) department is responsible for maintaining its IT infrastructure and applications. The IT department has implemented a patch management system for updating servers and clients. However, some clients, especially those with remote connections, are either updated by manually installing patches that are delivered to the client via email or CD. Other issues with the current patch management system have also been identified.

The practical assignment will address the development of an ISMS based on ISO 17799. The goal of the ISMS is to,

- Identify and analyze risks associated with the current patch management system.
- Create policies for mitigating risks.
- Develop controls for compliance with such policies.
- Develop an audit process for checking effectiveness of the system.
- Make recommendations for process improvement.

1. System Definition

1.1 Introduction

As part of G7799 certification, this practical assignment will address the development of an information security management system (ISMS) for a patch management system. The ISMS will be developed in accordance with the principals of 7799 (shorthand term for ISO 17799), and will follow SANS Plan Do Check Act (PDCA) process [1].

1.2 Scope of ISMS

The scope of the ISMS includes patch development, testing, and deployment to the following platforms and environments;

- All desktop workstations
- All networked and mobile laptops
- All file, print, and application servers
- Software packages running on the above platforms, including operating systems and third party applications

Also included in the scope are operational processes associated with patch management, such as test, backup and restore, log monitoring, and escalation processes.

The scope does not include information systems, such as servers, applications, and Websites, hosted at, or maintained by, third party vendors or suppliers.

For the purpose of this Patch Management ISMS, a patch is defined as software code, such as security update, hot fix, service pack, etc, which, upon installation, enhances the confidentiality, integrity, and availability of an information system.

1.3 Goals of ISMS

The main goal of the ISMS is to,

- Identify and assess risks associated with current patch management system.
- Create policies for mitigating risks.
- Develop controls for compliance with such policies.
- Develop an audit process for checking effectiveness of the system.
- Define areas for process improvement.

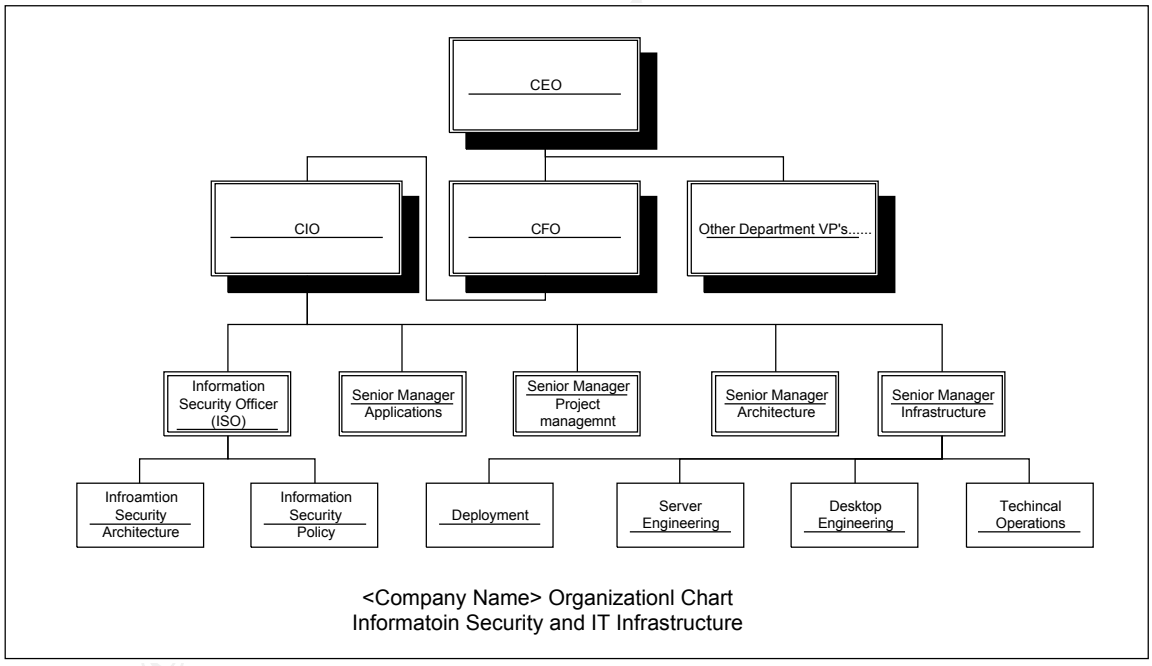
Controls developed for, or referenced throughout, the ISMS will be based on SANS BS 7799.2:2002 Audit Check List
< http://www.sans.org/score/checklists/ISO_17799_checklist.doc [2].

1.4 The Organization

<Company Name> is a financial institution based in the United States. The core business of the company is lending money, both to businesses and to consumers. The organization's business model is designed to provide industry leading financial services to customers. The company has branch offices throughout the United States and is supported by thousands of employees. <Company Name> currently handles annual transactions that run in the billions of dollars.

1.5 System Definition

<Company Name> has its own internal Information Technology (IT) department. The IT department, with its mission and goals closely aligned with the organization's business model, is responsible for developing and maintaining information systems and application to support business needs. The IT department is also responsible for maintaining the IT infrastructure. The figure below highlights the management structure of the IT department, with emphasis on information security and IT infrastructure.



<Company Name> Organizationl Chart
Informatoin Security and IT Infrastructure

The IT department maintains a large datacenter, hosting all application servers. The company's headquarters and all branch offices each have a file server and a print server. Every staff member has his/her own workstation, with the majority being desktop personal computers. Some staff members use laptop computers for conducting business. The majority of staff members work either from the headquarters building, or from any of the branch offices. However, some sales staff members (remote users) conduct their business either from their homes or from customer sites.

The IT department has implemented a patch management system for updating clients and servers. And although the patch management system is greatly automated, some clients, especially those with remote connections, are either updated by pulling patches from the IT's Website or by manually installing patches that are delivered to the client via email or CD.

1.6 Current State of Security

<Company Name> Board of Management and its Chief Information Officer (CIO) approved and released the company's top level information security policy. According to the policy, the following groups or positions have been established.

- Security Steering Committee (SSC): This committee was established to oversee the overall information security process. SSC members make decisions that affect the information security strategy of the company. They also review and sign all risk acceptance requests where there's an exception in compliance with enforced policies. Moreover, SSC members review and approve all information security policies.
- Information Security Working Group (ISWG): The ISWG was established to develop policies and standards based on information security threats faced by the organization.
- Local Information Security Forum (LISF): LISF members represent all <Company Name> business units. The LISF members review status reports, monitor compliance with policies, and report progress to the SSC.
- An information security officer was assigned the tasks of managing different aspect of information security.

The information security working group is tasked with the development of information security policies, standards, and guidelines to meet security requirements of IT and other business units within the organization. A high priority information security requirement is to maintain a highly secure IT environment, including prompt application of security updates to all servers and clients. Such updates are currently handled by the IT infrastructure team using automated patch management system. So far, the patch management system has been effective. However, instances have been experienced where systems were shut down after the delivery of patches. Other issues were related to delays in applying critical patches. Communication and coordination between administrators from different offices also added to the complexity of the patch management process.

2.0 Plan

The plan phase of PDCA is critical for the success of the ISMS. During this phase, subject matter experts team up to develop a project plan. For the purpose of implementing an ISMS for the patch management system at <Company Name>, members from information security, infrastructure, and audit teams need to be involved.

2.1 Project Plan

<Company Name> has a well defined and documented project management methodology. The project management process includes the following phases, initiation, planning, design, build, test, deployment, and closing. The project team will follow this project management lifecycle methodology design and implement the proposed ISMS. The goals of the ISMS, as identified in section 1.3, are considered the main deliverables of the project.

2 Project Timeline

Setting a timeline for the implementation of the ISMS depends on the criticality of the risks that <Company Name> faces. The risks are due to gaps or weaknesses in the patch management system. Generally speaking, since <Company Name> is a financial institution, which must follow strict data privacy laws and regulations, this project will be concluded within three months.

2.3 Resources

Management's sponsorship and support is critical for the implementation of the ISMS, including support from all senior IT managers. At a minimum, the CIO's approval and continued support are required. For this project, the information security manager is expected to be the project leader or the project manager. A good quality gate practice would require the project manager to sign-off at the end of each phase of the project lifecycle before allowing the project to move on to the next phase or go into production. Other project team members will be subject matter experts with representatives from Information Security Architecture, Server Engineering, Desktop Engineering, and Technical Operations. A representative from the company's audit department can add value to the project.

2.3.1 Infrastructure Security Forum

The criteria followed when selecting project team members was to ensure that patch management subject matter experts will play a leading role in the implementation of the ISMS. And in order to achieve increased efficiency in utilizing resources for this project, an Infrastructure Security Forum (ISF) will be established. The ISF will be chaired by the ISO, and its members will be the project team members. It's intended that the ISF will continue to function after project conclusion. Membership in the ISF will be reviewed to ensure that all information systems affected by patch management are included within the scope of the ISF. Members of the ISF will be nominated by their respective senior managers or by the ISO.

Members of the ISF will,

- Review incidents related to patch management issues.
- Develop policies, standards, and guidelines based on past incidents.
- Define a timeline strategy for application of patches based on risk criticality.

- Review and recommend industry patch management best practices.
- Review and approve patch management process.
- Review and approve third party software upgrades.
- Review and approve patch management change control procedures.

2.4 Policies and Standards

Mandy Andress [3] defines a policy as, (Andress, p52)

> A security policy is a document or set of documents that describe, at a high level, the security controls that will be implemented in the company. Policies are not technology specific and do three things for a company:
> - Reduce or eliminate legal liability to employees and third parties
> - Protect confidential, proprietary information from theft, misuse, unauthorized discloser, or modification
> - Prevent waste of company computing resources

The above quote is very much applicable to the kind of risks that <Company Name> may face due to the nature of its business. Being a financial institution, <Company Name> must comply with many local, state, and federal laws and regulations, and the first 2 bullet points above summarize the policies that need to be implemented in order to mitigate any foreseeable risks to <Company Name>. Some of the laws and regulation that are applicable in this case are,

- Gramm-Leach-Bliley Act
- USA Patriot Act of 2001
- Sarbanes-Oxley Legislation
- California Data Security Act (SB 1386)

In order to apply reasonable controls which will eliminate or reduce the foreseeable risk, the following policies need to be developed and enforced. Areas of 7799 listed below are from SANS BS 7799.2:2002 Audit Check List < http://www.sans.org/score/checklists/ISO_17799_checklist.doc [2].

Policy Name:	Patch Management Policy
Purpose:	This policy defines controls to ensure that system and software patches are applied in an effective and timely manner. Patch development, testing, and deployment procedures must be defined. Deployment schedules are set based on the criticality of patches. All software packages installed on any hardware platform are included in the scope of this policy.
Audience:	This policy is applicable to system and application administrators.
Areas of 7799:	8.1 Operational procedure and responsibilities 10.5 Security in development and support process

Policy Name:	Mobile Computing Policy
Purpose:	Set controls for remotely accessing organization's networks and assets. Policy restricts remote users to using only company supplied hardware. Such controls ensure that remote users operate personal computers or laptops that are properly and routinely managed by system administrators.
Audience:	System administrators and remote users.
Areas of 7799:	8.1 Operational procedure and responsibilities 9.8 Mobile computing and teleworking 10.5 Security in development and support process

Policy Name:	System Backup Policy
Purpose:	Define system backup requirements. Policy needed to ensure that loss of data is avoided, downtime is minimized, and systems can be fully and effectively recovered after occurrences of failure.
Audience:	System administrators
Areas of 7799:	6.2 User training 8.1 Operational procedure and responsibilities 8.4 Housekeeping

Policy Name:	Information technology Roles and Responsibilities Policy
Purpose:	This policy ensures that roles and responsibilities are properly defined and adhered to by, among others, personnel involved in the patch management process.
Audience:	System and application administrators
Areas of 7799:	4.1 Information Security Infrastructure 6.2 User training 8.1 Operational procedure and responsibilities 9.7 Monitoring and logging 10.5 Security in development and support process

Policy Name:	Incident Handling Policy
Purpose:	This policy defines categories of incidents, escalation and reporting procedures, roles and responsibilities of incident handling team and end users, contact lists for incidents reporting and escalation, and requirements for feedback and follow up procedures.
Audience:	End users and system, network, and application administrators.
Areas of 7799:	4.1 Information Security Infrastructure 6.2 User training 6.3 Responding to security incidents and malfunctions 8.1 Operational procedure and responsibilities 9.7 Monitoring and logging

Policy Name:	Change Management Policy
Purpose:	This policy defines requirements for appropriate change control procedures, including testing, approvals, roles and responsibilities (separation of duties), system requirements, back outs, logging and monitoring, and emergency action plans.
Audience:	System, network, and application administrators.
Areas of 7799:	6.3 Responding to security incidents and malfunctions 8.1 Operational procedure and responsibilities 9.7 Monitoring and logging 10.5 Security in development and support process

2.6 Risk Management

Risk management is the process of assessing and controlling risks. Risk assessment identifies risks in a specific system, process, or organization. Risk controlling is the process of mitigating the risk, which involves eliminating, transferring, or reducing the impact of the risk.

At <Company Name>, one of the major tasks of system and application administrators is to follow up with the software vendors regarding latest software updates, and to be aware of all risks associated with the software packages they administer. In addition, administrators obtain information on current threats and risks from other sources. One good example of such sources is SANS' list of top 20 vulnerabilities to different operating system platforms (www.sans.org/top20) [4].

Since only operating systems and third-party software are the only software packages included in the scope of the ISMS, it would be safe and acceptable to follow an ad hoc risk assessment methodology or process for the Patch Management ISMS. With ad hoc risk assessment methodology, "the process often immediately follows recent security incident or news story about a threat" (Andress p34) [3]. In other words, many organizations or system administrators initiate a patch management action as a result of one of the following;

- The release of a patch or a software update by the vendor.
- The occurrence of incidents related to lack of system or software updates.
- Alerts from different sources to the fact that other organizations are being impacted by vulnerability.

Vendors of operating systems and third-party software packages usually respond to evidence of threats to their products. They continuously test and update their software packages against known threats.

Mandy Andress summarizes a general risk assessment process as follows (Andress, p47) [3],

Step 1: Inventory, Definitions, and Requirements
Identify business critical processes, and identify and assign value to critical assets.

Step2: Vulnerability and Threat Assessment
Start analysis process.
Step3: Evaluation of Controls
Brainstorm potential controls and estimate their costs.
Step4: Analysis, Decision, and Documentation
Analyze controls for each threat and document assessment results.
Step5: Communication
Communicate results to appropriate parties.
Step6: Monitoring
Continuously analyze new threats and modify controls as necessary.

Patch management is now considered a top priority process for any information technology department. However, if such process is not designed and executed properly it could lead to the introduction of unforeseeable risks to the organization. Many resources are available on common or existing threats to information systems as a result of deficiencies in the patch management process. Microsoft Corporation summarizes the threats to IT systems, "Patch Management Process." Microsoft Corporation. 29 Jan 2004. <http://www.microsoft.com/technet/security/guidance/secmod193.mspx> [5], as follows,

- Denial of Service
- Tampering with data
- Repudiation
- Information disclosure
- Spoofing identity
- Elevation of privilege

In addition to risks that result from not applying patches in a timely manner, there's an additional risk which can be attributed to improperly installing a patch or from the inability to recover from a failed patch installation process.

The above list of threats will be the basis for the risk assessment process at <Company Name>. The controls used for mitigating risks are from SANS BS 7799.2:2002 Audit Check List
< http://www.sans.org/score/checklists/ISO_17799_checklist.doc [2].

The information security team at <Company Name> has developed and published an Information Security Risk Management Process [6]. According to this process, risk assessment can be accomplished by,

- Assessing potential business impacts

- Assessing levels of threat
- Assessing levels of vulnerability
- Calculating the level of risk

By following the above criteria for assessing the level of risk for the patch management ISMS, risks can be divided according to the following three risk levels,

Risk Level	Information System C.I.A. (*)	Likelihood of Threat	Seriousness of Vulnerability
High	High	High	High
Medium	Medium	Medium	Medium
Low	Low	Low	Low

(*) C.I.A.: Confidentiality, Integrity, and Availability

Risk 1
Nature of threat: Denial of service
Vulnerabilities:

- Ineffective patch management process, including the following;
  - Failure to apply patches
  - Delays in application of patches
  - Failure to apply patches to all affected systems
  - Inadequate testing of patches
  - Inability to restore from backup
- Flaws in operating systems or other installed software
  The above vulnerabilities are related to the patch management process and/or installed software and are applicable to all risks listed below.
- Inadequate network protection controls
- Missing anti-virus software, or outdated virus signatures
- Inexistence of intrusion detection and prevention systems
- Lack of network access controls
- Lack of incident monitoring and logging procedures

Likelihood of occurrence: High
Risk level: High
Description of the control selected:

4.1.2 Information security coordination
4.1.3 Allocation of information security responsibility
5.1.1 Inventory of assets
6.3.3 Reporting software malfunction
8.1.1 Documented operating procedures
8.1.2 Operational change
8.4.1 Information back-up
9.8.1 Mobile computing

9.8.2 Teleworking
10.5.1 Change control procedures
10.5.2 Technical review of operating system changes
The above selected controls are related to the patch management process and are applicable to all risks listed below.
6.3.1 Reporting security incidents
8.3.1 Control against malicious software
8.5.1 Network controls
8.7.4 Security of electronic email
9.4.1 Policy on use of network equipment
9.4.6 Segregation in networks
10.5.4 Covered channels and Trojan code
12.2.1 Compliance with security policy

Reasons for selecting control:

- Ensure that patches are properly tested and applied in a timely manner
- Ensure that patches are deployed to all affected systems, including mobile systems and systems used by teleworkers
- Ensure the accuracy of asset inventories
- Ensure that back-out (restore) procedures are tested
- Roles and responsibilities are properly defined

Reasons listed above are related to the patch management process and are applicable to all risks listed below.

- Prevention of introduction of malicious code
- Enhancing network security
- Timely detection and reporting of incidents
- Avoidance of downtime

Risk level after implementing control: Low

Risk 2
Nature of threat: Information disclosure and/or Tampering with data
Vulnerabilities:

- See patch management process vulnerabilities in Risk1 above.
- Inexistence of intrusion detection and prevention systems
- Lack of data access controls

Likelihood of occurrence: High
Risk level: High
Description of the control selected:
See patch management process selected controls in Risk1 above.
6.3.1 Reporting security incidents
9.6.2 Sensitive system isolation

Reasons for selecting control:

- See reasons for selecting controls for patch management process in Risk1 above.
- Timely detection and reporting of incidents

- Preventing unauthorized disclosure of, or access to, data
- Maintaining data confidentiality and integrity
- Avoidance of penalties and liability

Risk level after implementing control: Low

Risk 3
Nature of threat: Repudiation
Vulnerabilities:

- See patch management process vulnerabilities in Risk1 above.
- Inexistence of intrusion detection and prevention systems
- Lack of network access controls
- Lack of data access controls
- Lack of incident monitoring and logging procedures

Likelihood of occurrence: Medium
Risk level: Medium
Description of the control selected:

See patch management process selected controls in Risk1 above.
6.3.1 Reporting security incidents
8.5.1 Network controls
9.4.1 Policy on use of network equipment
10.3.4 Non-repudiation
12.2.1 Compliance with security policy
12.3.1 System audit controls

Reasons for selecting control:

- See reasons for selecting controls for patch management process in Risk1 above.
- Enhancing network security
- Timely detection and reporting of incidents
- Enhanced audit tracking capability
- Ability to resolve disputes about occurrence of event or action

Risk level after implementing control: Low

Risk 4
Nature of threat: Spoofing identity
Vulnerabilities:

- See patch management process vulnerabilities in Risk1 above.
- Missing anti-virus software, or outdated virus signatures
- Inexistence of intrusion detection and prevention systems
- Lack of network access controls
- Lack of incident monitoring and logging procedures

Likelihood of occurrence: Medium
Risk level: Medium
Description of the control selected:

See patch management process selected controls in Risk1 above.

8.5.1 Network controls
8.7.4 Security of electronic email
10.5.4 Covered channels and Trojan code

Reasons for selecting control:

- See reasons for selecting controls for patch management process in Risk1 above.
- Prevention of introduction of malicious code
- Enhancing network security
- Timely detection and reporting of incidents

Risk level after implementing control: Low

Risk 5
Nature of threat: Elevation of privilege
Vulnerabilities:

- See patch management process vulnerabilities in Risk1 above.
- Inadequate network protection controls
- Inexistence of intrusion detection and prevention systems
- Lack of network access controls
- Lack of incident monitoring and logging procedures

Likelihood of occurrence: Medium
Risk level: Medium
Description of the control selected:

See patch management process selected controls in Risk1 above.
8.5.1 Network controls
10.5.4 Covered channels and Trojan code

Reasons for selecting control:

- See reasons for selecting controls for patch management process in Risk1 above
- Prevention of introduction of malicious code
- Enhancing network security
- Timely detection and reporting of incidents
- Avoidance of unauthorized system changes
- Avoidance of downtime
- Reduced remediation time
- Maintaining data availability and integrity

Risk level after implementing control: Low

3. Do

This phase of implementing the ISMS addresses the steps or actions needed to resolve main problems identified with the patch management system thus far. A summary of the problems to be addressed is as follows,

- Issues with patch testing and deployment process
- Incident response process is inefficient
- Back-out procedures not properly tested

3.1 Problems, Actions, Steps

Problem: Issues with patch testing and deployment processes.

- Production issues: There have been isolated instances where production systems were affected by the deployment of patches. Such issues were attributed to the fact that the test environment does fully mirror the production one.
- Scheduling issues: Issues were identified and attributed to delays in application of patches. Delaying the deployment of a patch can add the risk of false sense of security, where management thinks that company assets are properly secured.
- Inventory issues: It's not clear whether remote (teleworkers) and/or mobile users are included in the patch deployment process.

Action: Action items to resolve problem(s) would include the following.

- Ensure that a proper test environment is available.
- Define a deployment schedule based on the criticality of the patches.
- Extend the current patch management process to include remote and mobile users.

Activities: The following is a set of activities recommended for the implementation of the above action items.

- ITM Senior Manager of Infrastructure assigns a task to both Desktop Engineering and Server Engineering teams to review the test environment.
- Local Infrastructure Security Forum addresses needed controls for making test environment in compliance with security policies, including separation of test and production environments.
- Both engineering teams review current test environment and make recommendations to IT management for necessary improvements.
- Engineering teams develop and publish patch testing procedures.
- Information security team document and publish guidelines for deadlines for the deployment of patches based on the criticality of each patch.
- Technical operation team will inventory all assets that are to be included in the patch management process.
- Engineering teams develop a process that includes deployment of patches to all assets.

Problem: Incident response process is inefficient

- Incident response process is fragmented and is currently supported by multiple teams, each based on their area of expertise and responsibility.
- Documented incident response procedures do not exist.
- Incident response contact and escalation list does not exist

Action: Action items to resolve problem(s) would include the following.

- Develop an enterprise-wide incident response process.
- Publish incident response process and contact/escalation list.

Activities: The following is a set of activities recommended for the implementation of the above action items.

- Information security team will define and document requirements for an enterprise-wide incident response process.
- Information security team to consult with other teams, such as, technical operations, infrastructure engineering, audit, physical security, and helpdesk for process definition and adoption.
- Review incidents logged by multiple teams and consolidate results.
- Use results as an input for the development of a new incident management process.
- Develop a single repository for documenting incidents history and actions taken to resolve incidents.
- Include incidents' history into the risk management process.
- Develop necessary policies to apply controls for avoiding similar issues in the future.

Problem: Back-out procedures not properly tested

- Recent incidents indicate that the integrity of some of system backups can not be confirmed.
- Similarly, back-out procedures, in some cases, are not tested prior to deployment of patches.

Action: Action items to resolve problem(s) would include the following.

- Develop and enforce data backup policy, mandating tests to ensure the integrity of the backup process.
- Clearly define and test back-out procedures prior to deployment of patches.

Activities: The following is a set of activities recommended for the implementation of the above action items.

- Information security team will develop data backup policy.
- Technical operations will document and test backup and restore procedures.
- Desktop and server engineering teams define and document back-out procedures for the patch management process.
- Backup policy and back-out procedures to be presented to the infrastructure security forum for review and approval.
- Once approved, infrastructure security forum will make back-out procedures one of the requirements for the change control process.
- Information security team conducts spot checks on system backups and patch deployment back-put process.

3.2 Statements of Applicability

Control: 5.1.1 Inventory of assets

Patch management process is all about applying patches to systems affected by known vulnerabilities. Failure to apply a patch to at least one affected system can negate the benefits from applying the same patch to thousands of other systems. This in turn will render the organization fully exposed to the risks associated with the intended patch. Therefore, it's imperative that an accurate inventory of all assets within the organization is maintained at all times. This control is for ensuring that an asset inventory or a register is maintained and users and location of assets are identified.

This control is applicable to the Patch Management ISMS.

Control: 8.4.1 Information back-up

As with any software installation or upgrade, certain risks can be attributed to patch management, such as, production downtime, corruption of software, system failures, or loss of data. Therefore, it's extremely important that proper, tested, and consistent backup processes exist in order to ensure that system recovery is possible after a failure. It is also necessary to periodically test the backup processes by conducting partial or full system/data restores. This control ensures that backups are taken regularly, backup media are stored securely, and backup media can be restored.

This control is applicable to the Patch Management ISMS.

Control: 8.6.2 Disposal of Media

A requirement of the patch management process is to ensure that systems are fully operational before the installation of patches. Another requirement is to maintain regular and tested system and data backups. Such backups are needed in order to restore the system to its initial state in case a failure occurs during the installation of patches. This control addresses procedures to securely dispose off media of systems that are no longer used. Systems that are no longer used are not included in the scope of the patch management process.

This control is not applicable to the Patch Management ISMS.

4. Check

4.1 Audit Checklists

The following list of controls will be used to audit the patch management system at <*Company Name*>. The criteria for this audit checklist was developed based on BS 7799 Standard. The patch management ISMS is also included in the scope of the audit process.

The goals of the audit process are,

1. Ensure that identified patch management risks are mitigated or reduced.

2. Ensure that the implemented controls are effective in tracking the compliance of the patch management system with published policies.
3. Identify further weaknesses with the selected information system (patch management).
4. Ensure that the implemented ISMS is effective.
5. Identify areas for improvement within the patch management system or within the ISMS
6. Conduct tests listed below for each control according to time interval agreed to by management, subject matter experts, and local information security manager. Intervals of 3, 6, and/or 12 months are recommended.

Control	4.1 Information Security Infrastructure
Control Section	4.1.1 Management information security forum
Control Objective	Infrastructure Security Forum exists within the organization
Control Importance	Members of the Infrastructure Security Forums are responsible for ensuring the effectiveness of the patch management process.
Control Test Steps	1. Review the organizational structure of the infrastructure department. 2. Review roles and responsibilities of members of the infrastructure forum. 3. Review charter of operation of the infrastructure security forum. 4. Review meetings minutes of the infrastructure security forum.

Control	4.1 Information Security Infrastructure
Control Section	4.1.2 Information Security Coordination
Control Objective	Cross-functional security forum exists within the organization
Control Importance	Cross-functional members will address and resolve issues that affect multiple teams within the organization
Control Test Steps	1. Review roles and responsibilities of the infrastructure security forum. 2. Check participation of all infrastructure teams, such as desktop, laptop, server, and network teams in the infrastructure security forum. 3. Review incident response and escalation procedures. 4. Review incident response logs for evidence of input from all infrastructure teams.

Control	6.2 User training
Control Section	6.2.1 Information security education and training

Control Objective	All employees of the organization receive regular training and security updates.
Control Importance	Educating and training employees on information security results in better compliance and faster and appropriate response to incidents.
Control Test Steps	1. Review the organization's information security awareness and education strategy and policy. 2. Review employee education history. 3. Review information security awareness content development and delivery methods.

Control	6.3 Responding to security incidents and malfunctions
Control Section	6.3.1 Reporting security incidents
Control Objective	Reporting procedure exists for effective reporting of security incidents.
Control Importance	Reporting of security incidents accelerates problem resolution. It also helps in isolating incidents in certain areas of IT systems and in identifying root causes of incidents, leading to avoidance of similar incidents in the future.
Control Test Steps	1. Review incident response contact list. 2. Review incident response logs. 3. Review incident response action plans. 4. Review trouble ticket system for evidence of unreported incidents.

Control	6.3 Responding to security incidents and malfunctions
Control Section	6.3.4 Learning from incidents
Control Objective	Process improvement based on quantifying and monitoring incidents.
Control Importance	By analyzing incidents, the root cause of system problem can be identified and mitigated. Similar incidents can be avoided in the future.
Control Test Steps	1. Review incident logs. 2. Review action plans for resolving incidents. 3. Review feedback process and action plan for avoiding similar issues in the future.

Control	8.1 Operational procedure and responsibilities
Control Section	8.1.1 Documented operating procedures
Control Objective	Backup procedures exist and are being followed.

Control Importance	Ensuring that system backups are performed regularly is a critical success factor in recovering from system failures resulting from system upgrades.
Control Test Steps	1. Review system backup procedures. 2. Review history of system backups. 3. Review routine testing procedures of system backup/restore.

Control	8.1 Operational procedures and responsibilities
Control Section	8.1.2 Operational change control
Control Objective	Approvals are required before any changes are made to production systems.
Control Importance	Obtaining approvals prior to implementing system changes ensures that pending changes are properly tested and thoroughly investigated prior to implementation. All affected parties are included in the approval process.
Control Test Steps	1. Review the organization's change control process. 2. Review change control approval process. 3. Review history of previous change control requests, scope of requests, approvals, and impact on production systems. 4. Review change control escalation process. 5. Review change control back out procedures.

Control	8.1 Operational procedures and responsibilities
Control Section	8.1.3 Incident management procedures
Control Objective	Incident handling procedures exist and are being followed. Procedures exist to address different types of incidents.
Control Importance	Following predefined incident handling procedures ensures that incidents are reported to appropriate staff in a timely manner. Incident handling team follows right procedures for handling reported incidents in order to minimize impact. Root cause analysis can be conducted on reported incidents so that they can be avoided in the future. Incidents give indication that some systems are missed during the patch management process.
Control Test Steps	1. Review incident management process. 2. Review incident logs. 3. Review contact lists for incident reporting.

Control	9.7 Monitoring and logging
Control Section	9.7.1 Event logging
Control Objective	Exceptions and security events are logged and kept for future investigations.

Control Importance	Event logs are considered important audit trails for tracking source of events, including problems resulting from systems updates that affect the availability of data.
Control Test Steps	1. Check that incidents are properly recorded or logged. 2. Check that incident records are regularly monitored.

Control	9.8 Mobile computing and teleworking
Control Section	9.8.1 Mobile computing
Control Objective	Policy exists to address risks with mobile computing.
Control Importance	To address the additional controls needed for mobile equipment due to higher risks associated with operating in unprotected environments.
Control Test Steps	1. Review patch management procedures for mobile equipment. 2. Review incident logs related to mobile equipment.

Control	9.8 Mobile computing and teleworking
Control Section	9.8.2 Teleworking
Control Objective	Policies, standards, or procedures for teleworking activities.
Control Importance	To ensure that proper inventory is kept for teleworking equipment. And to ensure that teleworking equipment are included in the patch management process.
Control Test Steps	1. Review inventory logs of teleworking equipment and users. 2. Review patch management process for teleworking equipment. 3. Review incidents reported on teleworking equipment.

Control	10.5 Security in development and support process
Control Section	10.5.1 Change control procedures
Control Objective	Strict controls in place over implementation of changes to information systems.
Control Importance	Failure to follow change control procedures may result is system failures, downtime, loss of data, and wasted manpower.
Control Test Steps	1. Review change control procedures, such as, testing, back out, escalation, and approvals. 2. Review policy, standard, or guideline for following change control procedures. 3. Review past and current change control requests.

Control	10.5 Security in development and support process

Control Section	10.5.2 Technical review of operating system changes
Control Objective	Processes and procedures are in place to ensure that applications are tested after changes to operating system.
Control Importance	Testing of applications after making changes to operating systems in test and production environments will reduce the risk of downtime on multiple production systems.
Control Test Steps	1. Review operating system patch management process. 2. Review test procedures for operating system patches in test environment. 3. Review patch management process for patches applied to operating systems in production environment. 4. Review application testing procedures in test and production environments.

4.2 System Improvement

The above audit checklist is designed to ensure that appropriate controls are implemented for checking the compliance of the patch management process with current policies and standards. With the adoption of a process of repeated testing (see test steps for the controls above), a measure of the effectiveness of the ISMS and its controls can be established. Action items for process improvement can easily be identified in areas where consistent failures are persistent. Action items may include the development of additional policies, addition of further ISMS controls, or modification of the control test steps for existing controls.

5. Act

5.1 System Maintenance

The following steps are measures needed to properly maintaining the Patch Management ISMS.

- Repeated incidents give an indication for a need to review the list of implemented ISMS controls. Action items taken after the reporting of incidents must include steps for reviewing missing or inadequate ISMS controls.
- Ensure that the purchasing department has direct input into the asset inventory process.
- Policies developed for the Patch Management ISMS are to be included in the yearly policy maintenance (review) cycle.
- Add the ISMS review process to the roles and responsibilities of the Infrastructure Security Forum.
- Seek professional assistance by engaging external auditors in the ISMS review process.
- Ensure that risks reported by software vendors and supplier are addressed

by the ISMS.

5.1 Areas of Improvement

The following are considered areas of improvement for both the Patch Management ISMS and for the Patch Management System.

- Develop and implement a corrective action process to,
    - Ensure that proper actions are taken to resolve identified issues.
    - Identify personnel responsible for resolving issues.
    - Ensure that similar issues are avoided in the future.
    - Establish a repository of past issues.
- Enhance the incident response process to include metrics for keeping track of past incidents. Such metrics serve as a measure of the effectiveness of the ISMS.
- Adopt a proactive approach for securing servers and workstations.
- Explore the possibility of separation of duties by transferring the responsibility of patch deployment to a dedicated deployment team.
- Develop and conduct an employee training plan to ensure that consistent levels of knowledge are maintained within the IT department.
- Establishing a Secure Coding Forum for the organization will enhance the security of the in-house developed applications.
- Engage in dialogue with IT departments from other organization with similar business models.

6. Conclusion

The Patch Management ISMS will target and resolve critical issues with one of <Company Name> critical information systems. Moreover, the successful implementation of the ISMS will enhance the level of information security for the entire organization. This ISMS can serve as a model for implementing similar ISMS models for other information systems within <Company Name>. It is also a first step towards achieving ISO 17799 registration.

Appendix A – References

1. SANS Institute. Track 11- 17799 Security & Audit Framework. Volumes 11.1 – 11.5. SANS Press, 2004.

2. Thiagarajan, Val, and Algis Kibirkstis. Information Security Management, BS 7799.2:2002 Audit Check List for SANS. SANS. 20 Dec. 2004 < http://www.sans.org/score/checklists/ISO_17799_checklist.doc>

3. Andress, Mandy. Surviving Security. Indianapolis: SAMS Publishing, 2002.

4. "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus." SANS. 20 Dec. 2004 <http://www.sans.org/top20/>

5. "Patch Management Process". 29 Jan. 2004. Microsoft. 20 Dec. 2004 <http://www.microsoft.com/technet/security/guidance/secmod193.mspx>

6. "Information Security Risk Management", <Company Name>, April 27, 2004.