Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Security Process for the implementation of a Companys extranet network

Security Policies, standards and procedures are the guidelines to detect, compare, control and determine if there is a security problem or risk associated to the company's productivity information flow. "Security policies and standards require clear, concise, well-defined security processes to make them effective" [1]. A security process must show control points to guarantee that policies, standards and procedures are in compliance with the required company's security levels. This paper will explore the development of ...

Copyright SANS Institute
Author Retains Full Rights

AD

Security Process for the implementation of a Company's extranet network connections.
Version 1.4 b Option 1

© SANS Institute 2003, Author retains full rights

Kirk Steinklauber
Date: May 27 2003

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

***Table of Contents*:**

1. Introduction **3**

2. Roles and Responsibilities **4**

3. Security Process **5**

4. Risk Management Process **6**

5. Security Design Process **10**

6. Security Implementation Process **20**

7. Verification Process **23**

8. Conclusions **26**

9. References **28**

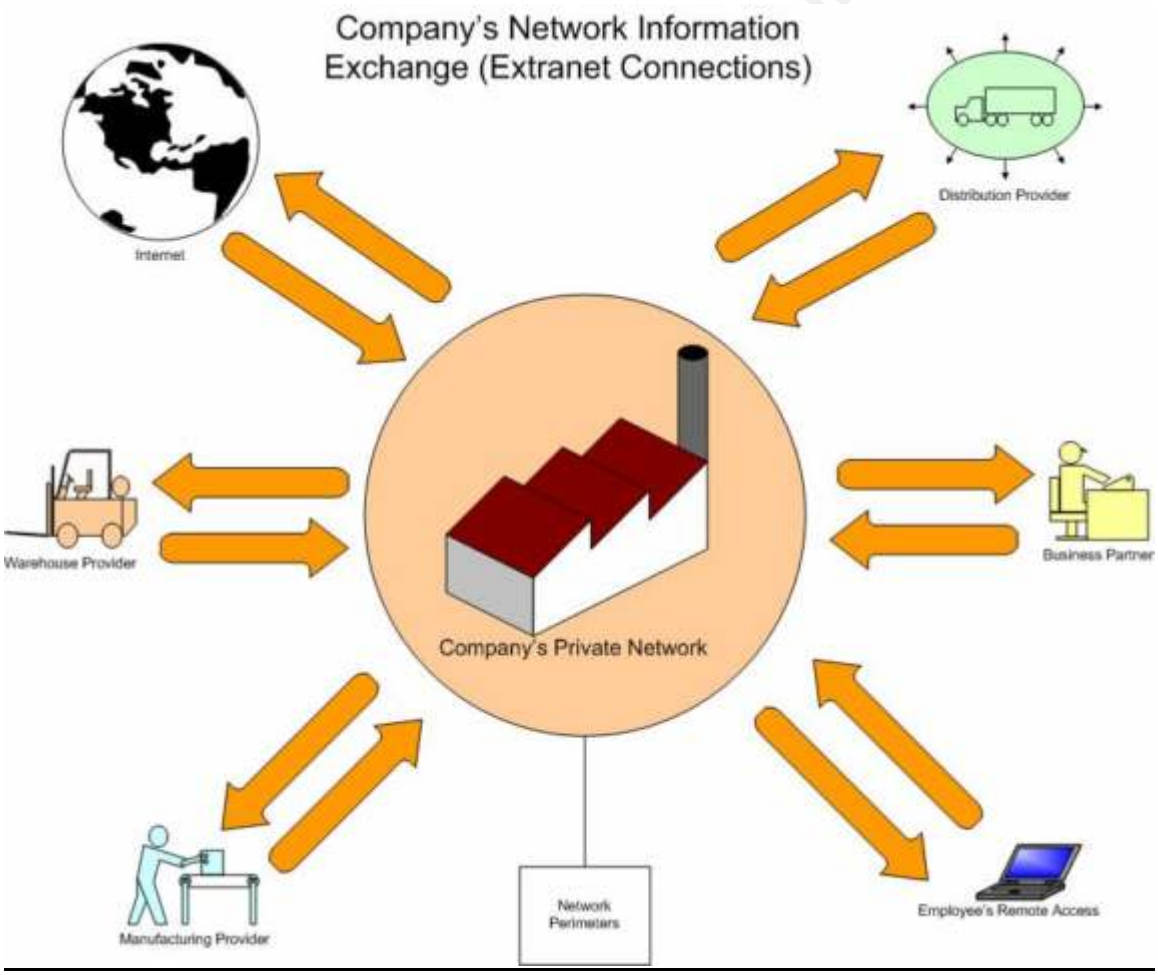
© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

1. Introduction

The current business climate requires companies to communicate and exchange information with a large number of customers, business partners, vendors, contractors and research communities. Besides of this fact, most of the companies offer remote access and internet access for their employees.

Under this scenario, companies must implement security controls in their network's perimeter. The problem is how to implement these controls, how to cover all the security aspects for each connection, how to implement policies, guidelines and procedures to provide an acceptable security level for the company according to their business needs.



Actually, many companies only regard security controls in their internet access and forget about the other business connections implemented with vendors, contractors, business partners, etc.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Security Policies, standards and procedures are the guidelines to detect, compare, control and determine if there is a security problem or risk associated to the company's productivity information flow. "Security policies and standards require clear, concise, well-defined security processes to make them effective" [1].

A security process must show control points to guarantee that policies, standards and procedures are in compliance with the required company's security levels.

This paper will explore the development of the security process required to build an effective standard policy to cover a company's network perimeter.

2. Roles and Responsibilities

For the purpose of this paper, it is necessary to define roles and responsibilities required for the security process model presented in this document. In a company two or more roles cannot be assigned to the same group or person.

- **Business Requirement Owner (BRO):** Each extranet connection must have a Business Requirement Owner according to a business need for its implementation. Generally, it is a business unit manager who requires a specific connection with a third party network in order to complete the designated tasks for its operation.
- **Information Technologies Provider (ITP):** Each extranet connection must be designed, implemented, and administered by the Information Technologies Provider. It should be the Technology business unit or Outsourcing business unit.
- **Business Security Controller (BSC):** Each extranet connection must be reviewed and must be in compliance according to the security policies and standards. In general, this would be the organization's security staff.

The BSC must receive and evaluate each connection requested by the BRO, and forward to the ITP the requirement for a proposal design for the connection if it is previously approved. The BSC must also approve or reject each proposal design from the ITP in order to satisfy the security levels by the policies and standards.

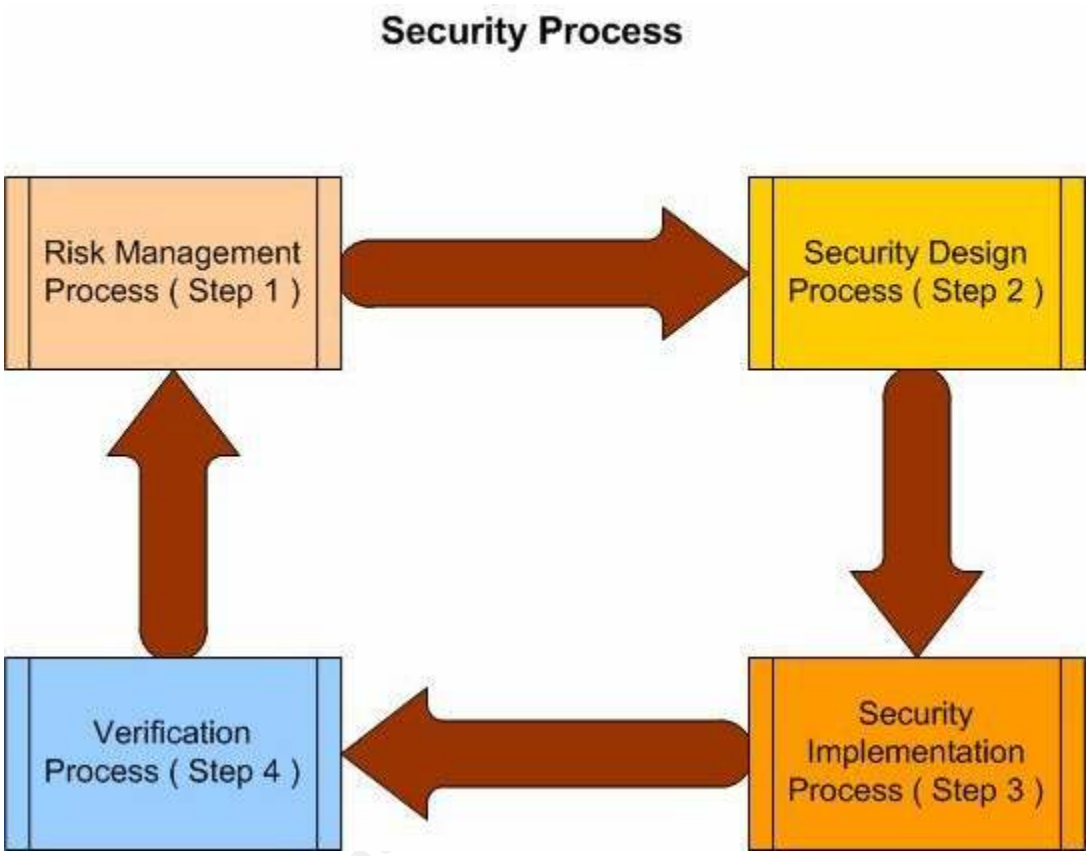
The BRO must request, maintain or cancel the network connection that it is responsible for. The BRO must authorize, revalidate and maintain physical and logical access according to the business need without violating any of the security policies and standards.

The ITP is the technology custodian of each extranet connection, also it is responsible to implement and maintain the security controls required by the policies and standards.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

3. Security Process

The figure below, the 4 stages or sub processes for the security Process model are shown:



The security process model is a cycle that starts when the BRO expresses the need to create a new extranet connection (Step one). The BSC studies the request and verifies the security implications for this new demand. If the connection is approved, the process moves on to the Security Model.

In Step two, the ITP must design and develop the connection's solution according to the security policies and standards. If the BSC approves the connection's security model, the process can go ahead to the next stage (Step three).

In the Security Implementation Process, the ITP configures the technology infrastructure following the security model, and does the necessary tests to guarantee that the security levels are correctly implemented. The BSC compares the implementation with the security model. If all is in compliance, the connection is authorized and the BRO can start using it in a production mode.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Once the connection is placed in production, the security process model continues to Step four. In the Verification process the ITP and the BRO must do periodic tasks, which are stipulated on the predefined procedures, in order to maintain the security levels of the connection.

After a minimal period of one year, the process goes ahead from Step four to Step one. The main idea is to validate each extranet connection on an annual basis and commit the BRO to check and adjust the security levels of the active connection if it is necessary. During this part of the process the connection must be evaluated to determine the need to maintain it active or to terminate it.

If the business requirements for a specific connection change during the first year period in the Step four, the BRO can request to start the Risk Management Process in order to boost the security process and adjust the security levels according to the evolution of the business needs.

After completing the first cycle of the security model, the steps two and three will help to adjust the security procedures, technology infrastructure and system configuration based upon the evolution of the business and to avoid new security threats.

This security process model may only be ended by the requirement of the BRO during any of the four sub processes. In the four sub processes of the security model there are control points such as evidence, records and procedures to support the compliance of the security policies and standards.

4. Risk Management Process

Each physical connection (inner or outer connection) between the company's private network and any external network using any physical media (such as modem, RDSI, ADSL, Optic Fiber, Clear Channel, Frame Relay, etc.) must be considered as an a **extranet connection**. Physical connections with branch offices are not considered extranet connections because they are part of the company's internal private network.

Every company is the owner of their network security perimeter; thus it cannot use the security levels of the remote networks which are connecting to the company. Every Organization must protect the three unique attributes of their information:

- **"Confidentiality** – Information should only be seen by those persons authorized to see it. Information could be confidential because it is proprietary information that is created and owned by the organization or it

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

may be customers' personal information that must be kept confidential due to legal responsibilities" [2].

- **"Integrity** – Information must not be corrupted, degraded, or modified. Measures must be taken to insulate information from accidental and deliberate change" [2].
- **"Availability** – Information must be kept available to authorized persons when they need it" [2].

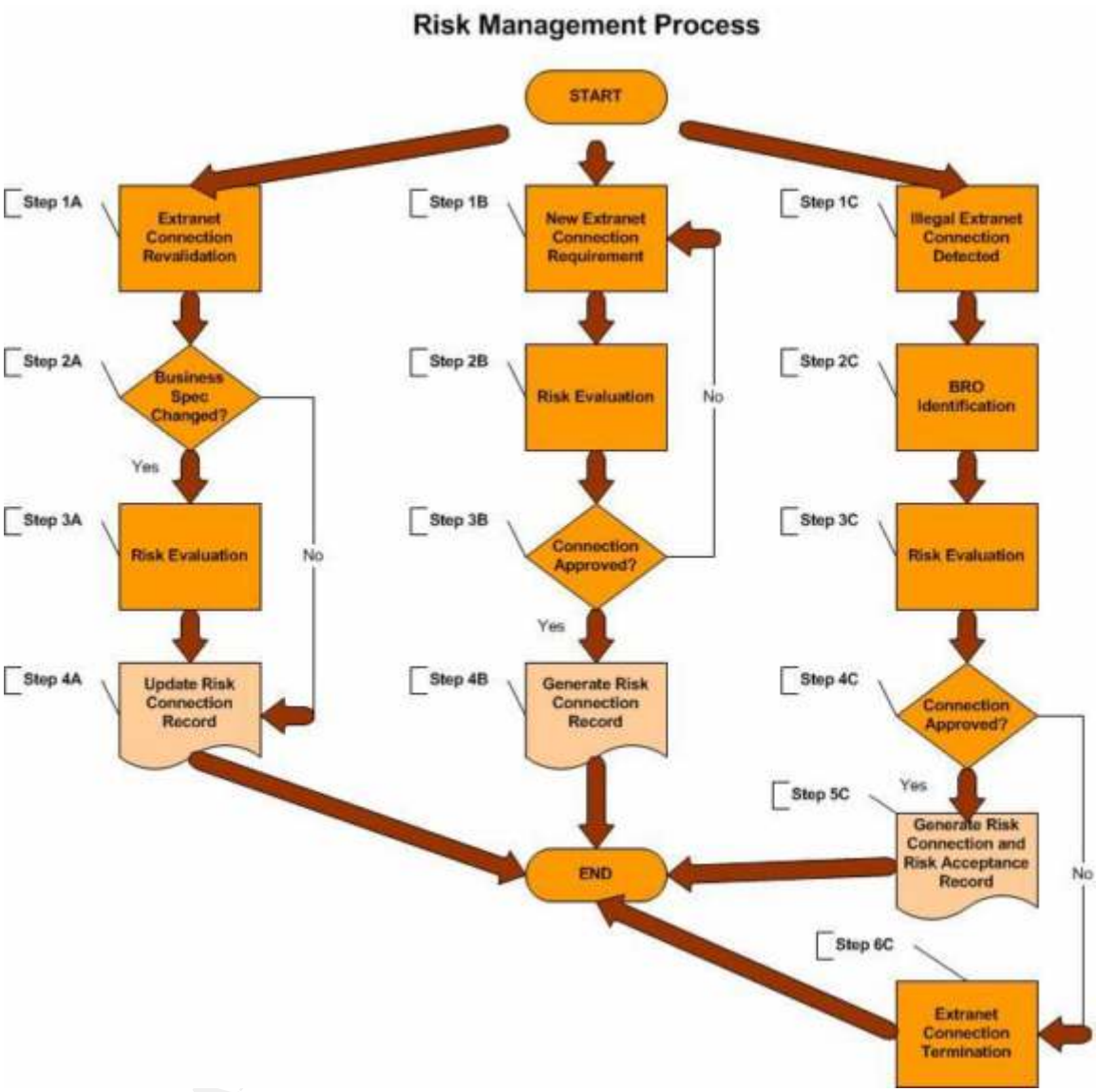
For each extranet connection, there is a risk associated in the exposure of any company's information attributes. A risk must be evaluated, documented, mitigated and eradicated.

The purpose of the Risk Management Process is to document in a central repository (such as DB, application, etc.) each extranet connection with basic information like:

- **Name of the connection:** Each connection must have a name to identify it from the other extranet connections.
- **BRO Identification**: For each connection is necessary to identify the owner of the extranet connection (BRO).
- **Purpose of the connection**: In the Risk Management documentation must be specified the business needs to implement an extranet connection.
- **Funding of the Connection:** In the Risk Management documentation must be cleared about the funding that support the connection made by the BRO.
- **Services required in the connection:** In this section of the documentation, must be specified the services and applications that are required to communicate between the company's private network and the external connection such as FTP, Web, Telnet, DB, etc.
- **Data Protection:** In this part of the documentation is necessary to specify according to the company's information classification for each service required by the BRO, if the transmission of the information is private, confidential, etc.
- **Type of connection:** There are three possible scenarios in the Risk Management Process model for extranet connections: new connection, connection revalidation and illegal connection. In the documentation have to be specified what of this three possible scenarios is the case that applies.
- **Status of the Risk Management:** There are three possible statuses: Approved, Rejected and Revision Required. When the Risk Management Process starts, the documentation must have the status of Required Revision. When the BSC reviews the documentation, it can change the status with the respective comments. If there is no change in the status, the BRO must adjust the requisite and will solicit a new review with the BSC.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The figure below presents the Risk Management Process model:



The process starts selecting the appropriate scenario for the extranet connection.

Each step of the process is explained:

<u>Extranet Connection Revalidation:</u> Approved extranet connections that are in compliance with the company's security levels must be validated after one year of the verification process or if the evolution of the business needs (Step one-A) require that the BRO's request to change the solution's specifications.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Either If the specifications have changed after one year, or the BRO's requisites are different from the original plan (Step two-A), the BSC must execute a Risk Evaluation to determine if the security levels have being compromised following the compliance in the security policies and standards (Step three-A).

The BSC will provide the necessary recommendations after the Risk Evaluation. Also the documentation must be updated (Step four-A) in order to revalidate the legacy of the connection. After the Risk Evaluation, the BSC has the authority to reject the new specifications in the case of non compliance with the predefined security policies and standards. If this happens, the BRO can either maintain unchanged or terminate the connection.

If the specifications remain unchanged the record must be updated prior to validation of the following statements: the extranet connection is still required by the BRO (because of the business needs) and the BSC revalidates the legacy of the connection (Step four-A).

New Extranet Connection Requirement: This part of the process starts with the identification of a new extranet connection required by the BRO. The Risk documentation has to be created by the BRO in order to be reviewed by the BSC (Step 1B).

The BSC reviews the information and executes the Risk Evaluation to validate the new requirements against the security policies and standards (Step two-B). If the Connection is not approved, the BRO must review the BSC recommendations and adjust the requirement in order to accomplish the security levels required by the policies and standards (Step three-B).

If the Connection is approved, the Risk Documentation will be created with the approval of the BSC (Step four-B).

Illegal Extranet Connection Detected: This part of the process starts with the identification of an existing extranet connection that is generally detected by the company's security tools or the company's monitoring process. This connection is illegal because it is not approved by the BSC accordingly to the company's security levels (Step one-C).

The BSC must try to determine the cause of the implementation of this irregular connection without the compliance of the security policies and standards. In this part of the process the BSC has to identify the owner (the BRO) of the illegal connection to commit him to start the security process (Step two-C).

The BSC executes the Risk Evaluation according the information presented and the security status of this active connection (Step three-C). If the extranet connection is approved (Step four-C), the Risk Documentation must be generated with the approval of the BSC. Then, the active connection has to be

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

suspended until the security controls are implemented through the security process (Step five-C).

If the connection needs to be active before the implementation of the appropriate security controls defined in the Security Model Process and the Security Implementation Process a Risk Acceptance document has to be approved and signed by the BRO.

With the Risk Acceptance document, the BRO accepts knowledge and responsibility of the risk associated to maintain an active connection without any security controls. Meanwhile, an action plan must be documented and implemented in order to mitigate the risk associated in the active connection while the whole security process is completed (Step five-C).

If the extranet connection is rejected, the active connection must be terminated immediately because there is a high security exposure and is not qualified under the company's security levels in that moment (Step six-C).

5. Security Design Process

The base of a good security design is the documentation of the **technical specifications** and the **compliance procedures** required for the security device responsible to protect the network's perimeter (typically called firewall infrastructure).

The Security Design is one of the most important steps to implement the required security levels in all extranet connections.

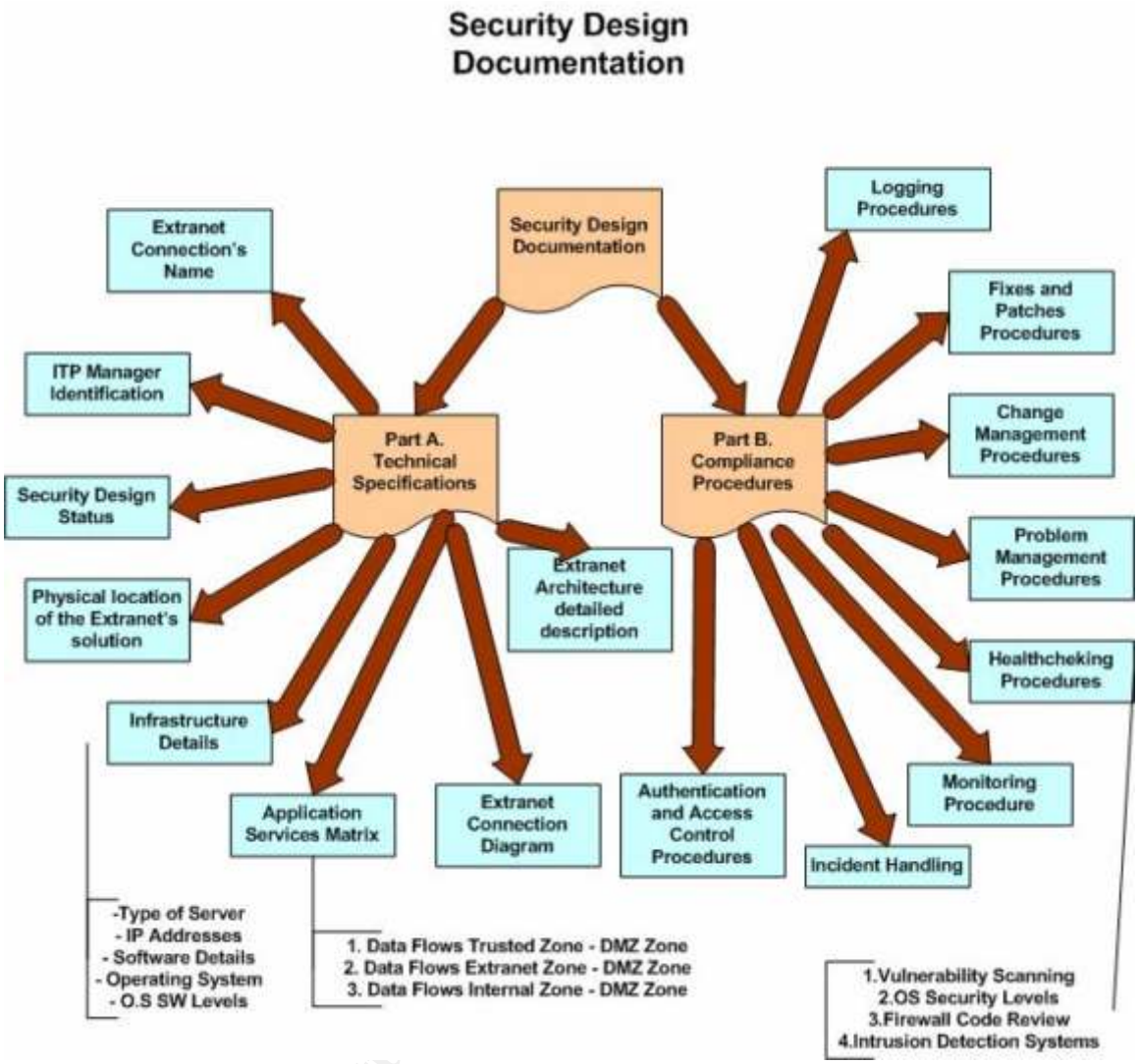
In order to simplify the complexity of the documentation, a standard Compliance Procedures can be documented and applied for all company's Extranet Connections, instead using specific Compliance Procedures for each Implementation. Obviously, there will be exceptional cases that require specific Compliance Procedures to adjust the security levels required by the security policies.

The documentation in the Security Design is the key to accomplish the company's security policies for the network's perimeter.

The ITP must prepare and present the Security Design for the review and approval of the BSC for each requirement to implement or revalidate an extranet connection.

In the figure below represents a summary of all items presented and required in the Security Design Documentation:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



For the **Technical Specifications** the information required is:

Extranet Connection's Name: Each extranet connection must have a unique name to identify it from the other extranet connections.

ITP Manager Identification: For each extranet connection the ITP Manager is the responsible in the solution's technical development.

Physical location of the extranet's solution: Each technical infrastructure must be installed in control access areas with all necessary physical controls required in a Datacenter Service.

Security Design Status: In the Security Design documentation there are three possible statuses: Approved, Rejected and Revision Required. When the Security Design Process starts, the documentation must have the status Revision Required. When the BSC reviews the documentation can change the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

status with the respective comments. If there is no change in the status, the ITP must adjust the requirements and requests a new review with the BSC.

Infrastructure Details: In this part of the documentation, the ITP must identify all software infrastructure required for the implementation. For each infrastructure component the following information must be completed in a matrix:

- **Type of Server**: Identify if the server is a Firewall, Mail Server, DNS Server, Web Server, Application Server, etc.
- **IP Addresses:** Identify for a specific server each network adapter IP Address. A Firewall must have at least 2 network interfaces for example.
- **Software Details**: Identify for each server the software that must be installed for the solution's deployment (i.e. Exchange Server, Apache Server, Checkpoint Firewall 1, etc.).
- **Application Software Levels**: Identify the software levels for each application running in the extranet solution. This is required because the highest level of software code minimizes security problems with the application's bugs.
- **Operating System**: Identify for each server the Operating System required (i.e. Cisco IOS, Windows 2000, Linux, AIX, Solaris, etc.).
- **Operating System Software Levels**: Identify the operating system levels for each server running in the extranet solution. This prevents bugs that can be exploited by hackers.

Application Services Matrix: Direct connections between the extranet network and the company's internal network cannot be allowed in an Extranet Connection.

"The firewall will only allow certain services to be accessed by users on the Internet. These known services can then be given special attention to make sure that they are the latest, most secure versions available. In this way, the focus can shift from hardening an entire network, to just hardening a few internal machines and services [3]".

"Demilitarized Zones (DMZs) are used in situations where few machines service the Intranet and the rest of the machines are isolated behind some device, usually a firewall. These machines either sit out in the open or have another firewall to protect the DMZ. This can be a very nice arrangement, from a security perspective, as the only machines that accept inbound connections are "sacrificial lambs." [3]"

For the purpose of this paper there are four possible network zones defined:

- **Internal Zone**: This zone represents the company's internal network.
- **DMZ Zone**: This zone represents a physical isolated network segment for the configuration of the servers' infrastructure to handle the inbound and

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

outbound traffic between the extranet connections and the company's internal network. For an extranet connection, more than one DMZ Zone can exist.

- **Extranet Zone**: This zone represents a non trusted network connection between the company and the required connection.
- **Trusted Zone**: This zone represents an isolated network where a clear channel is established between the required connection and the company. The connection is not made using public networks like the internet.

There are some rules that must be followed in order to establish a good security level in an extranet connection between the defined zones:

- The ITP must have the control and administration of the Internal Zone, DMZ Zone and the Trusted Zone.
- The Trusted Zone must use non-routable IP Addresses. In some cases the DMZ Zone could use non-routable IP Addresses too.
- Direct connections between Internal Zone and the Extranet Zone are not allowed.
- Data communication between zones must be controlled and limited using a control access device (such as a firewall). VLANs are not considered a control access device.
- Data communication between DMZ Zone and the Internal Zone must use strong authentication.
- The Extranet Connection Services must use proxy systems or proxy applications in the DMZ Zone for the data exchange.
- The Extranet Zone only can communicate with the DMZ Zone using strong authentication and encryption (128 bits minimum). Connections with other zones can be done using the proxy services in the DMZ Zone.
- The Trusted Zone only can communicate with the DMZ Zone using strong authentication. Connection with other zones can be done using the proxy services in the DMZ Zone.

In the Application Services Matrix section the ITP must document the data communication flows between the network zones with the appropriated services.

In the matrix there are only three possible information flows according to the pre-defined rules between network zones:

- Data flows in the Extranet Zone with the DMZ Zone.
- Data flows in the Trusted Zone with the DMZ Zone.
- Data flows in the Internal Zone with the DMZ Zone.

For each network application there must be documentation in the matrix, the IP Source, the IP Destination and the Communication Ports.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

All applications services must be in compliance with the communication rules for the network zones. If it is not possible, the security levels could be compromised and an alternate solution that satisfies the rules must be implemented.

Extranet Connection Diagram: The ITP has to provide a detailed network diagram of the solution with the specifications of the network zones, the servers required in the solution and the IP Addresses for each component.

Extranet Architecture Detailed Description: In this section, all the applicable information that shows how the solution is going to work must be documented by the ITP.

For the **Compliance Procedures** section of the Security Design, the information required in the documentation is:

Logging Procedure: In this part of the documentation a procedure must be documented to handle and manage all logs records. In the Firewall and the Servers located in the DMZ Zone the logs must be retained at least for sixty days.

Firewall logs must be maintained in the Internal Zone (i.e. like a Logging Server) in order to prevent logs corruption when a security incident is occurs.

The Logging Procedures must include logging review and reports generations at least in a weekly basis for the Firewall.

Fixes and Patches Procedures: In this part of the documentation a procedure must be documented to handle and manage all fixes and patches.

For the purpose of this paper, the suggestions to apply properly the patches and fixes in all cases are:

- For Systems connected to the internet, new critical fixes and patches must be applied immediately.
- For Systems connected using Trusted Zones, new critical fixes and patches must be applied in the next 24 hours.
- For Systems connected to the internet, new medium impact fixes and updates must be applied in the next 24 hours.
- For Systems connected using Trusted Zones, new medium impact fixes and updates must be applied in the next 72 hours.
- For Systems connected to the internet, new low impact fixes and updates must be applied in the next 72 hours.
- For Systems connected to the internet, new low impact fixes and updates must be applied in the next 7 days.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Change Management Procedure: In this part of the documentation a procedure must be documented to handle all change records for maintenance and administration of the Extranet Connection Infrastructure.

All software configuration changes, hardware changes, software updates and maintenance processes must be implemented using record changes. These records must have the ITP Manager Approval, detailed description of the change, time and date of the programmed maintenance, name of the technical person responsible of the implementation, verification steps of the success of the change and duration of the change.

The Change Management Procedure must guarantee that all changes must be supported with an approved record. If the change cannot be completed successfully, a rollback process must be implemented in order to reestablish the service.

The Procedure must certify that the security levels are maintained before, during and after the change implementation. The company's internal network cannot be exposed for any reason.

If the security controls need to be disabled in the Firewall during a change management, the Extranet Zone and Trusted Zone interfaces must be disabled prior the implementation.

If there is a problem installing a Fix in the software level, and the defined date for its installation has expired, a Risk Acceptance document must be created and signed by the ITP Manager. In this document, the ITP Manager must provide an action plan to close the issue.

If the Requirement forces to change the specifications of the data communication flows in the firewall rules, the Risk Management Process must be initiated again to restart the security process. In this case, the Security Design Specifications are required to change and a New Security Design must be implemented, reviewed and approved by the BSC.

The Change Management Records must be updated and closed after the success of the implementation.

Problem Management Procedure: In this part of the documentation a procedure must be documented to handle all problem records in the Extranet Connection Infrastructure.

All hardware and software problems must be registered in a problem record repository. Depending on the problem impact to the end users, a severity problem record must be open according to:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- A Problem impacting all users must have severity 1. For the purpose of this paper, these problems must be solved maximum in 8 hours (this can vary depending on the service level agreement provided by the ITP).
- A Problem impacting a specific service must have severity 2. For the purpose of this paper, these problems must be solved maximum in 24 hours (this can vary depending on the service level agreement provided by the ITP).
- A Problem impacting a specific user group must have severity 3. For the purpose of this paper, these problems must be solved maximum in 72 hours (this can vary depending on the service level agreement provided by the ITP).
- A Problem impacting a specific user must have severity 4. For the purpose of this paper, these problems must be solved maximum in 5 days (this can vary depending on the service level agreement provided by the ITP).

In a Record problem, a technical resolution owner must be assigned to solve the problem. Also, detailed description of the problem must be documented, what application, and which server and services are involved.

If the problem is a security problem, an incident handling procedure must be executed in order to preserve and protect the security levels of the company's internal network.

When the problem is solved, the problem record must be updated with the root cause analysis and closed by the resolution owner.

Incident Handling Procedure: In this part of the documentation a procedure must be documented to handle all possible security incidents in the extranet connection.

This procedure must contain the best practices according to the computer forensics techniques. "Computer forensics investigators examine computer hardware and software using legal procedures to obtain evidence that proves or disproves allegations. Gathering legal evidence is difficult, and requires trained specialists who know computers, the rules of evidence gathering and how to work with law enforcement authorities" [4]. "When forensic examiners find computer evidence, they must present it in a logical, compelling and persuasive manner so that a jury will understand and a defense counsel cannot rebut. This requires step-by-step reconstructions of actions with documented dates and times; charts and graphs that explain what was done and how, testimony that explains simply and clearly what a suspect did or did not do, and exhibits that can withstand scrutiny" [4].

In a majority of companies, there is a security team called Computer Emergency Response Team (CERT) responsible for the design and implementation of the Incident Handling procedures to react when the security incidents occurs.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

If there is no CERT present in a company, the ITP must design and develop the incident handling procedure for each extranet connection. It's possible to use a standard procedure to handle all extranet connections.

Health Checking Procedures: In this part of the documentation a procedure must be documented to maintain and review periodically the security levels in the extranet connection's technical infrastructure.

This procedure must define what tests and technical reviews must be done in the technical infrastructure (Firewalls, DMZ Servers, etc.) and the periodicity to execute them.

For the purpose of this document and depending of the extranet connection, there are 2 possible time periods defined for the execution of the Health Checking Procedure:

- For Systems connected to the internet must be executed every week.
- For Systems connected using a clear channel must be executed every 3 months.

The minimal tests and technical reviews recommended are:

- **Firewall Vulnerability Scanning**: There are tools such as Nmap, LANGuard Network Scanner, IBM Network Security Auditor (IBM NSA), etc. for the firewall's network port scanning.
- **Intrusion Detection Systems**: There are many tools and standards in the market to deploy Systematic Attack Detections. One of the best tools is using Intrusion Detection Systems (IDS). "Network Intrusion Detection systems are perimeter protection device(s) that monitor network traffic and can detect whether an enclave is under some specific, recognized attack" [5]. All servers in the extranet connection (Firewall, DMZ Servers, etc.) must have Intrusion Detection Systems implemented.
- **Operating System Security Levels**: Each server in the extranet connection must have security settings implemented in their Operating System. All services that are not used must be disabled, and the Operating System Resources (OSR) must be protected. By default, any Operating System doesn't have security settings applied. There are security standards to configure any Operating System with the proper security levels. There are tools like Symantec Enterprise Security Manager (ESM) to review and report the Operating System Security Settings according to a predefined security policy template and Operating System software levels.

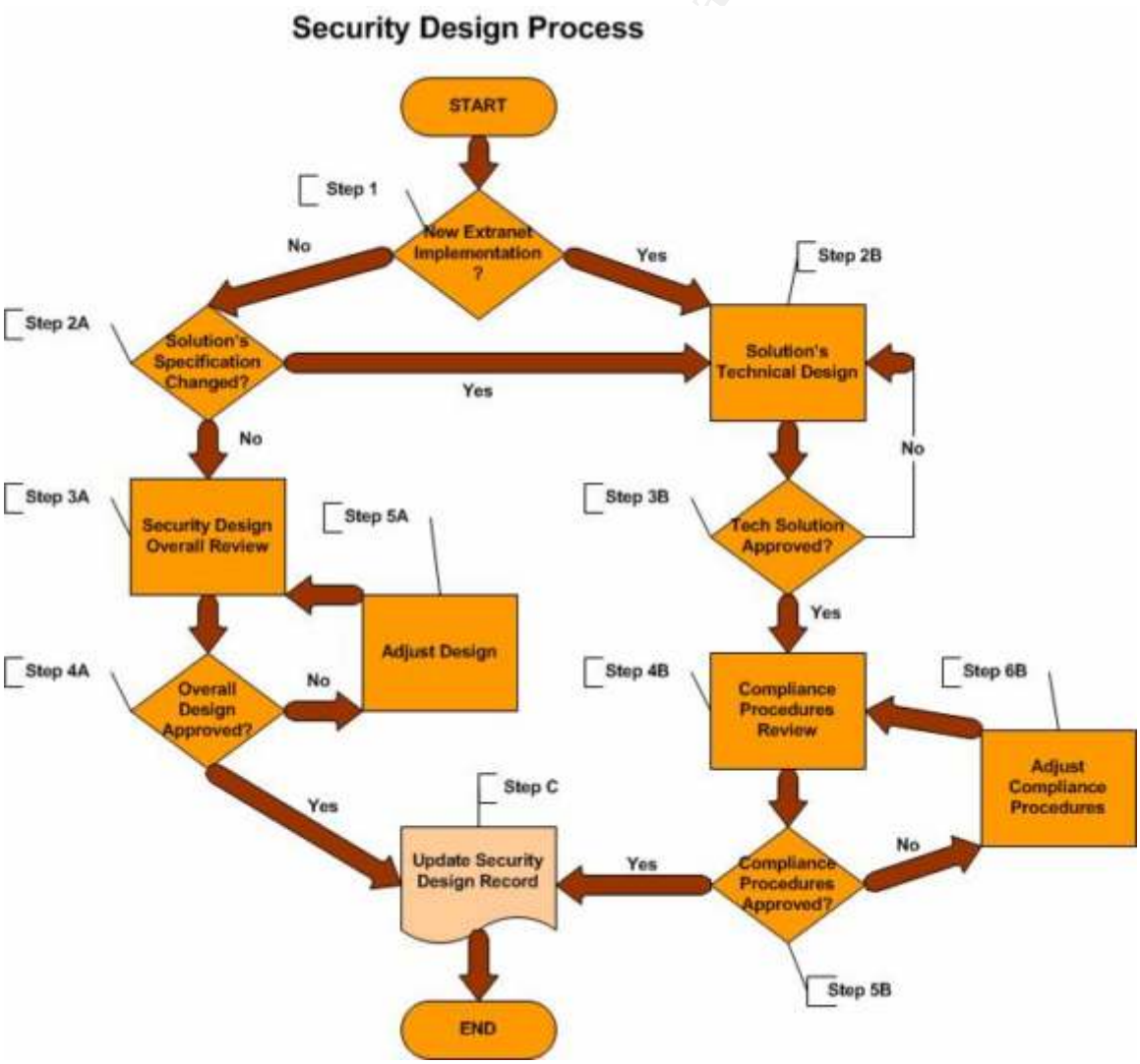
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- **Firewall Code Review**: The firewall rules must be reviewed in order to verify if the firewall rules maintain the approved security design.

Authentication and Access Controls Procedures: In this part of the documentation a procedure must be documented to manage all user ids (including privileged users like system administrators) and IT resources accessed in the extranet connection. The ITP is responsible to control all users and resources access, but the BRO is the only person that can authorize or deny access to its extranet connection IT infrastructure (add-remove-modify-review-annual revalidation of all user ids and IT resources).

Monitoring Procedure: In this part of the documentation a procedure must be documented to determine how it is going to monitor in the extranet connection activity in real time to detect possible security problems.

The figure below presents the Security Design Process model:



© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The process starts checking if the Security Design is going to be applied to an existing Extranet Connection or to a new one (Step one). The BRO must pass to the ITP the required applications and services for the Extranet Connection Security Design.

For existing Extranet Connections, the BSC reviews if the Solution's specifications have been changed (Step two-A). If this is true, the solution Technical Specifications must be redesigned and re-documented just like a new connection (Step two-B).

If this is not true, the BSC reviews the Technical Specifications Documentation and Compliance Procedures in order to validate the security compliance according to the security policies (Step three-A).

The BSC can approve or reject the documentation presented by the ITP (Step four-A). If the design is rejected because it is not in compliance with the security policies, the ITP must adjust the design (Step five-A) and request again to the BSC the review of the Security Design Overall (Step three-A again).

If the design is approved, the BSC must update the Security Design Documentation and change the status of the connection to approved (Step C).

For a new Extranet Connection the ITP must prepare the technical design of the solution and present the Technical Specifications to the BSC for review (Step two-B).

The BSC reviews the Technical Specifications and approves or rejects the solution's design (Step three-B). If the solution is rejected, the ITP can review and update the documentation to request a new review with the BSC (Step two-B again).

If the Technical Specifications are approved, the ITP must review the Compliance Procedures to guarantee that the security levels are according to the company security policies (Step four-B).

Compliance Procedures can be rejected or approved by the BSC (Step five-B). If it's rejected, the ITP must adjust and update the Compliance Procedures (Step six-B) in order to be reviewed again by the BSC (Step five-B again).

If it's approved, the BSC must update the Security Design Documentation and change the status of the connection to approved (Step C).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

6. Security Implementation Process

The purpose of the Security Implementation Process for each extranet connection is to install, configure and test the IT Technical Infrastructure (routers, servers, hubs, firewalls, hubs, etc.) proposed and previously approved in the Security Design Process. At the end of the implementation, the ITP must execute the technical tools defined in the Compliance Procedures in order to demonstrate that the implementation satisfies the approved Security Design.

The results of the security tests must be documented in a central repository (like DB, application, etc.) for each Extranet Connection in order to be reviewed and approved by the BSC.

The basic information required in the documentation is:

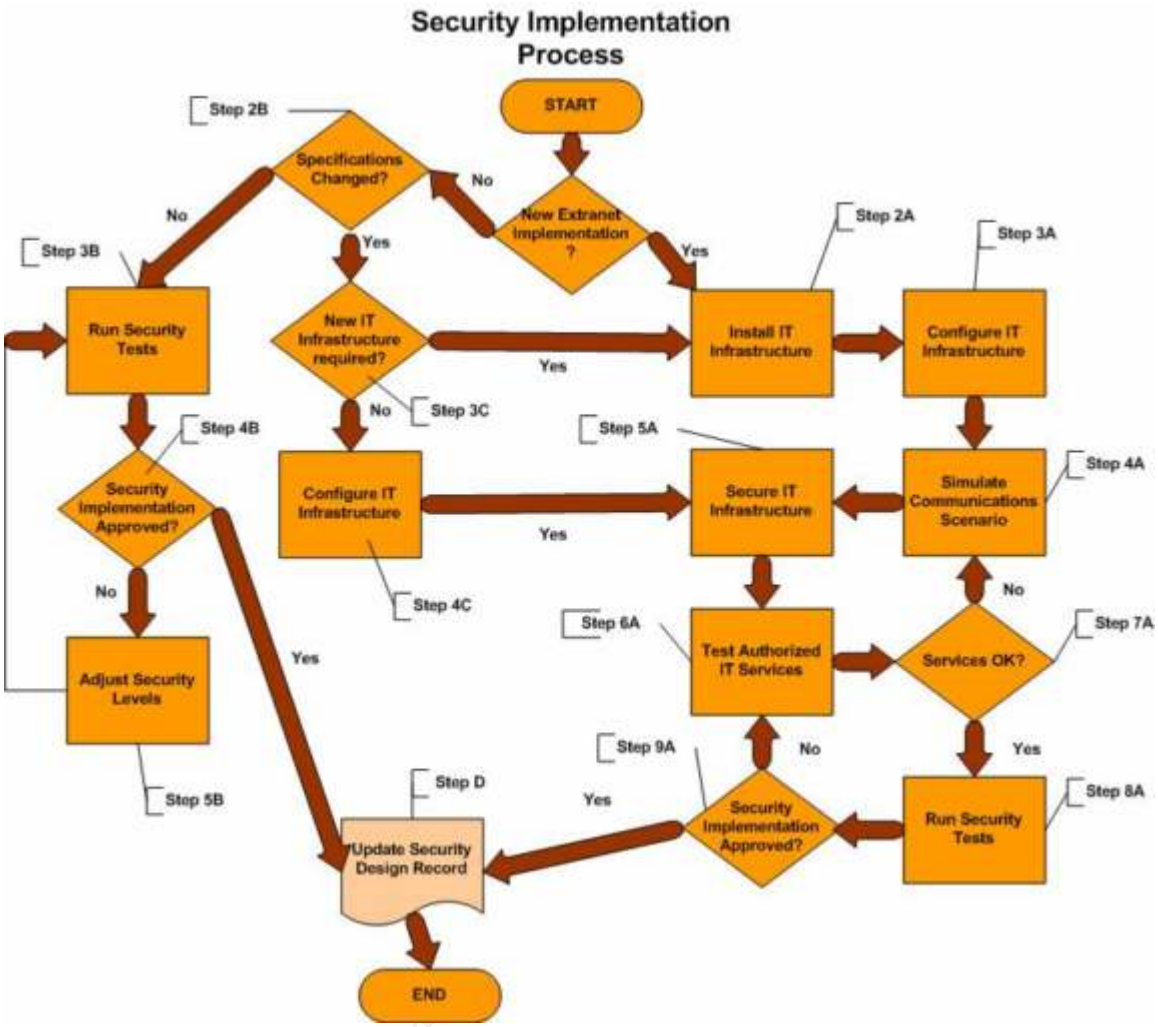
Health Checking Results: All evidence required in the Health Checking Procedures must be recollected and documented.

Logging Configuration Results: The Servers' logs must be in compliance with the security levels required by policies.

Software Level Results: The applications and Operating Systems must use an acceptable software level that prevents bugs and system failures.

The figure below presents the Security Implementation Process model:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



The process starts checking if the Security Implementation is going to be applied to an existing Extranet Connection or to a new one (Step one).

For New Extranet Implementation, the ITP must install the necessary IT Infrastructure: routers, switches, hubs, DMZ Servers, Firewalls, etc. according to the approved Security Design (Step two-A).

The ITP must configure the IT Infrastructure services that support the Extranet Connection: Web service, FTP service, DNS service, etc. (Step three-A).

The ITP must create a lab to simulate the communications with the extranet entity or network in order to test the functionality and communication of the desired infrastructure services (Step four-A).

If all is going well, the ITP must configure and implement security controls in the IT Infrastructure: configure access lists in the routers, configure firewall rules, secure servers' operating system, secure applications and so on (Step five-A).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

In the lab, the authorized IT services through the Extranet IT Infrastructure must be tested according the approved Security Design (Step six-A).

If everything is OK (Step seven-A), the next step is to run the Security Tests: Health Checking Tests, Logging Tests and compliance with the software levels (Step eight-A). Otherwise the next step is going to the Step four-A again.

The BSC must review the results of the Security Tests and must validate that Technical Specifications and the Compliance Procedures are in accordance to the solution's implementation (Step nine-A).

If the BSC approves the tests, the documentation must be updated and the status of the Extranet Connection is finally approved in order to be used by the BRO. In this case, the Extranet Connection is legal and can be officially placed in a production mode (Step D).

For existing Extranet Connections the ITP checks if the specifications of the actual solutions have to be modified (Step two-B).

If the Specifications need to be changed, the ITP must check if new IT infrastructure is required to be installed (Step three-C). If so, the next step is going to the Step two-A. Otherwise the ITP must configure the actual IT infrastructure (Step four-C).

If the Specifications remain unmodified, the ITP must run the Security Tests to the Extranet Connection IT infrastructure (Step three-B).

The BSC must review the results of the Security Tests and validate that Technical Specifications and the Compliance Procedures are in accordance with the solution's implementation (Step four-B).

If the Security Implementation is rejected, the ITP must review and adjust the security levels of the IT infrastructure according to the security policies (Step five-B). After that the next step is going to Step three-B again.

If the BSC approves the tests, the Extranet Connection is revalidated to continue its normal operation (Step D).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

7. Verification Process

The purpose of the Verification Process for each extranet connection is to periodically generate all audit evidence documented in the Compliance Procedures of the Security Design.

The results of the Compliance Procedures execution must be documented in a central repository (like DB, application, etc.) for each Extranet Connection for audit purposes.

All Compliance Procedures must generate all necessary evidence to support any audit reviews and must guarantee the compliance in the security levels.

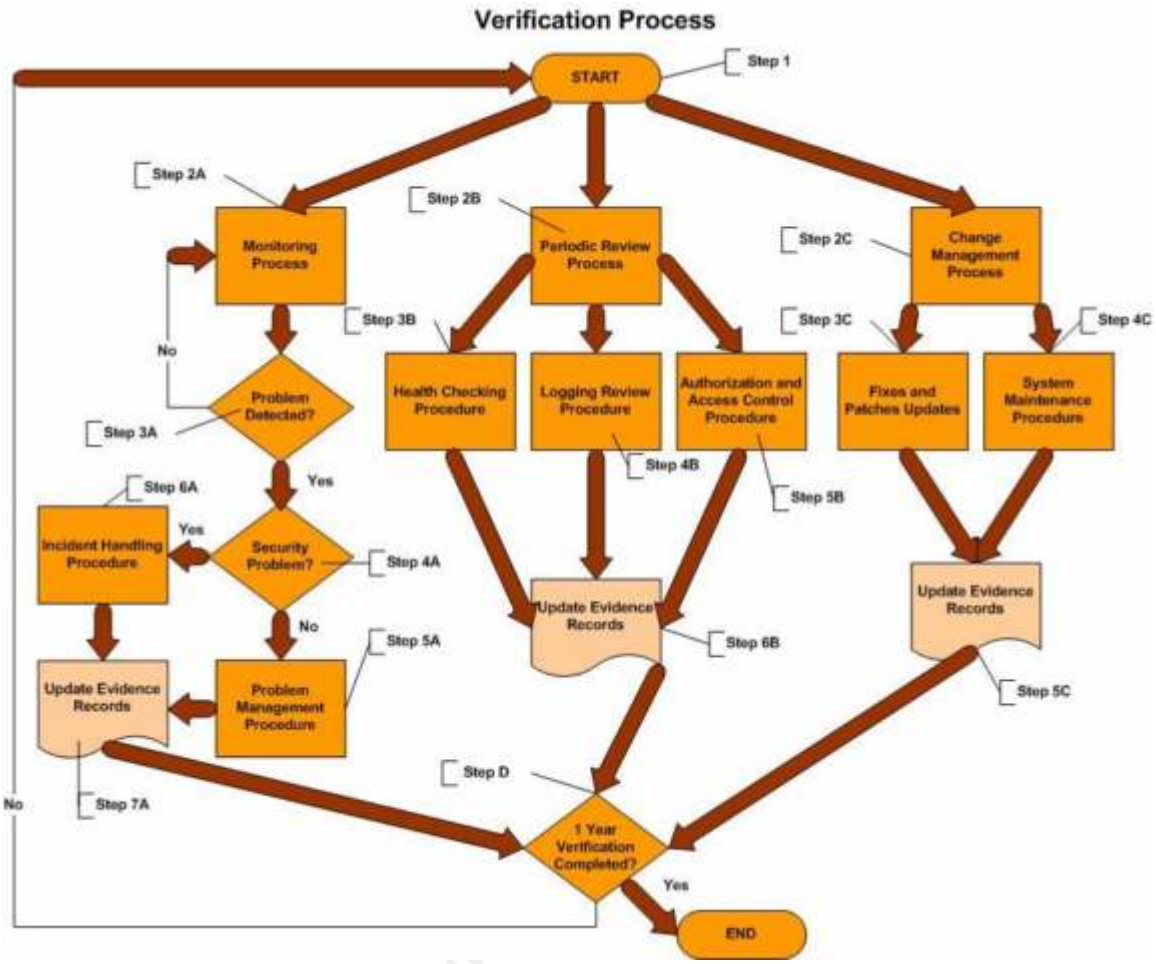
For the Verification Process, the evidence that must be generated for audit reviews is:

- **Logging Procedure**: Access Control Device's security reports based on system logs (i.e. Firewall logs reports).
- **Fixes and Patches Procedures**: Reports with the list of all fixes and patches applied in the extranet connection IT infrastructure history.
- **Change Management Procedure**: List of all change records with the detailed information of all maintenance applied to the extranet connection IT infrastructure.
- **Problem Management Procedure**: List of all problem records with the detailed information of all fix problem implementations to the extranet connection IT infrastructure.
- **Incident Handling**: List of all evidence and incident records with the detailed information of all fix security implementations to the extranet connection IT infrastructure.
- **Health Checking Procedures**: List of all evidence reported by the vulnerability scans, Firewall code review, Systematic Attack Detections and OS Security Levels.
- **Authentication and Access Control Procedure**: List of all evidence for the requirement process to add, remove, modify, review and annual revalidation of all user ids and IT Resources.
- **Monitoring Procedure**: List of all monitoring events generated by the available tools configured for the extranet connection.

For Internet Systems, the period of this verification process must be executed weekly, and for the rest of the systems must be executed every 3 months.

The figure below presents the Verification Process model:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



The Verification Process starts any time with any of the defined Compliance Procedures required to be executed (Step one).

There are three possible scenarios for the Verification Process:

Monitoring Process: This process executes the defined Monitoring Procedure to detect problems in the Extranet Connection (Step two-A). If a problem is detected (Step three-A), the ITP and/or CERT must validate if the Problem is a Security Problem (Step four-A).

Each problem detected must be managed using the Problem Management Procedure (Step five-A).

If there is a Security Problem detected, the Incident Handling Procedure must be invoked by the respective ITP and/or CERT (Step six-A).

All Problems and Incidents must be documented in updated records to maintain the history control of all events at the end of the process (Step seven-A).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Periodic Review Process: This process executes some of the Compliance Procedures defined to maintain and review the security levels of the Extranet Connection required periodically by the security process (Step two-B).

The Health Checking Procedures verifies that the configurations in the IT infrastructure are in compliance with the security levels required by the approved Security Design (Step three-B).

The Logging Review Procedure guarantees that system logs of all Extranet Servers are reviewed in order to detect possible security events that could impact the extranet service (Step four-B).

The Authorization and Access Control procedure maintain controls of all Users and IT Resources accessed through the Extranet Connection (Step five-B).

For each Compliance Procedure the necessary evidence must be documented to maintain the audit records of all events at the end of the process (Step six-B).

Change Management Process: This process executes the defined Change Management Procedure to implement system maintenance and software updates in all IT infrastructures (Step two-C).

When new fixes and patches are available for any of the IT infrastructure, a change management record must be opened and the Fixes and Patches Procedures must be executed (Step three-C).

When System Maintenance is required in any of IT infrastructure like configuration files changes, execution of special tasks, etc. a change management record must be open and approved by the ITP Manager (Step four-C).

If the change requirement implies modification of the Security Levels approved in the Security Design of the Extranet Connection, the Risk Management Process must be invoked instead to restart the overall Security Process.

The Change Management records are the necessary evidence to be documented to maintain the audit records of all events at the end of the process (Step five-C).

The Verification Process must end after one year of execution. In this point the Risk Management Process starts again, and the Security Process cycle completes one loop.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

8. Conclusions

Many people think that the security process is mainly used to configure servers with the proper security settings. A good security process must be a cycle that always loops checking the security levels according to the security policies and improves it according to the evolution of the environment and new technologies tools.

The documentation is the basis to deploy the proper framework to build a security structure for a company's IT infrastructure. The documentation avoids the misunderstanding in the definition of what is secure and what is not.

The basic documentation required to build a security structure is:

Security Policies: Are the guidelines or normatives that define levels of sensitivity in the information management and information flows to protect the three unique information attributes: "Confidentiality, Integrity and Availability".

"In business, a security policy is a document that states in writing how a company plans to protect the company's physical and information technology (IT) assets. A security policy is often considered to be a "living document", meaning that the document is never finished, but is continuously updated as technology and employee requirements change. A company's security policy may include an acceptable use policy, a description of how the company plans to educate its employees about protecting the company's assets, an explanation of how security measurements will be carried out and enforced, and a procedure for evaluating the effectiveness of the security policy to ensure that necessary corrections will be made" [6].

Security Procedures: Are the defined and documented operational steps to verify that Security Policies are applied and maintained correctly.

Security Processes: Are the defined tasks and activities that should be executed in the Security lifecycle with the Security Procedures' support.

The typical threats used against network security are:

"**Port Scanning** – Hackers use scanning tools to search through various hosts connected to a network looking for ports that are enabled or open. They will compare this information to known security vulnerabilities to see if they can gain access to the targeted hosts.

To reduce the threat: Turn on only the services that are needed and use Network Address Translation to block the addresses from being publicly available on the Internet

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Denial-of-Service (DoS) – Designed to deny access to computing or networking resources by overwhelming the host or network with continuous requests. In other words, DoS attacks send more requests than the host or network can handle.

To reduce the threat: Make sure the servers in the perimeter network are not running too close-to-capacity, and use packet filtering firewalls to prevent obviously forged packets from entering into the perimeter network. In addition, keep all hosts and servers up to date on security patches and fixes.

IP Address Spoofing – Hackers find a trusted IP address and modify it so that it appears to be coming from a trusted host, when it is really not.

To reduce the threat: Configure your routers and firewalls to reject any inbound packets that claim to originate from a host within the internal network. This way, no external machine can take advantage of internal network trust relationships.

IP Address Sniffing - Potential intruders "sniff" (monitor) a network to capture valuable information such as IP addresses, usernames and passwords as users log onto a remote system.

To reduce the threat: Enforce strong password use and use proxy servers and NAT to reduce IP address sniffing.

Viruses, Trojan horses and Worms – Though they are different, each one of these malicious programs can have a disastrous effect on your enterprise computers and possibly your entire network.

To reduce the threat: Always run antivirus software with a current virus definitions file, and never run an unsolicited program without first trying it out on an isolated test host. Educate all employees to be careful about opening suspicious email from unknown sources" [7].

All network security risks can be eliminated or minimized identifying and controlling all extranet connections using a process to support it. The security process presented in this paper represents the best practices used to secure network perimeter and this does not represent a standard to secure it.

"Information systems security. Computer and network security. Internet security. It's a complex world, and growing more so every day. With these changes, some truths and approaches to security remain the same, while others are new and radically different. Developing a sound security strategy involves keeping one eye on the reality of Internet-speed changes in threats and technology, and the other on the reality of the corporate environment. Purchasing security devices is easy. Knowing how and what to protect and what controls to put in place is a bit

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

more difficult. It takes security management, including planning, policy development and the design of procedures" [8].

9. References

1. "Security Process Development".
URL: http://www-1.ibm.com/services/security/spdspec.html

2. La Piedra, James. "The Information Security Process Prevention, Detection and Response".
URL: http://www.giac.org/practical/gsec/James_LaPiedra_GSEC.pdf

3. Mc Graw-Hill. "Firewalls Complete – Internetworking Protocols and Standards: An Overview". 16 October 2002. URL:
http://secinf.net/firewalls_and_VPN/Firewalls_Complete/Firewalls_Complete__Internetworking_Protocols_and_Standards_An_Overview.html

4. Walker, Don. "Computer Forensics: Techniques for catching the 'perp' protect company data". April 2001.
URL: http://www.serverworldmagazine.com/monthly/2001/04/forensics.shtml

5. Yarnell, Frank. "Development of a Network Intrusion Detection Policy". 18 September 2002.
URL: http://www.giac.org/practical/GSEC/Frank_Yarnell_GSEC.pdf

6. "Security Policy". 28 April 2001.
URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci548251,00.html

7. "Building a Security Framework". 28 February 2003. Article ID: 2011.
URL: http://enterprisesecurity.symantec.com/article.cfm?articleid=2011&EID=0

8. Avolio, Frederic M. "Best Practices in Network Security". 20 March 2000.
URL: http://www.networkcomputing.com/1105/1105f2.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: August 31st, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced