Global Information Assurance Certification Paper

Implementing a Risk Assessment Program as part of an overall ISO17799 ISMS

Lee Coone
G7799 Certification
Practical Assignment version 1.1
NS2004 Las Vegas
October 2004

Table of Contents

List of Figures

Abstract:
Understanding the state of the operating environment of your organization is a vital part of an overall Information Security strategy. Are you vulnerable to attack by the dark forces amassed against your company? How can you tell? How do you go about determining the state of your company's ability to withstand an attack, from outside forces or inside the perimeter?

A Vulnerability Assessment toolkit, methodology, and remediation plan are essential to periodically review the security posture of your environment and proactively respond to the results.

This paper will develop an Information Security Management System (ISMS) that designs, implements and provides assurance that lowers the overall risk posture of an organization. This paper will also demonstrate the Plan, Do, Check, Act (PDCA) framework as detailed in the ISO/IEC 17799 standard.

I. Define the System

The enterprise is in the financial services industry (specifically, a mid-tier provider of retirement plan products and services, individual life insurance and annuities, long-term health insurance, group and credit insurance products) which operates in all 50 states and the District of Columbia. The parent company was formed in 2000 to blend the strengths of each of its partner companies to achieve greater collective results. The partner companies can trace their roots as far back as the mid-1800's. The executive management structure is stable, with little turnover. The enterprise has approximately 2000 employees; approximately 80% located at the home office of the largest partner company, with the estimated 20% distributed in small offices throughout the Unites States.

The enterprise, through mergers, acquisitions and partnerships from 2000, has shown steady growth. However, the stated growth targets for the enterprise are to double in overall size in the next 3 - 5 years, through organic growth and further mergers and acquisitions. To date, the partner companies have operated their own Information Technology departments, distinct and separate from each other. In order to facilitate the attainment of the stated growth targets, senior management re-instituted the position of Information Security Officer, and commissioned the position with the following responsibilities:

- Meeting the requirements of various legislative initiatives,
- Creating policies,
- Mitigating risk to acceptable levels,
- Recommending and implementing new technologies to ensure the security of the enterprise, and
- Managing the Vulnerability Management and Business Continuity environments.

Even though the most recent risk assessment performed against the enterprise computing environment was viewed by the assessing entity as "better than average", senior management has directed the Information Security Officer and his staff to develop an Information Security Management System (ISMS) for the enterprise, utilizing the ISO17799 standard as the methodology. As he is located at the largest partner company, the model developed at this location will be the template and the standard to be adhered to by all partner companies and affiliates. The initial direction of this effort will be to develop a Vulnerability Assessment toolkit, methodology and remediation program that can be effectively deployed to any current or prospective partner company or affiliate.

As part of the ongoing annual reviews of the enterprise, an external Information Security consulting firm is retained to perform a Vulnerability Assessment against selected areas of the enterprise's computing environment, such as the external-facing networked devices, or the primary computing devices within the corporate Intranet. With the advent of the regulatory atmosphere of today, such

as Gramm-Leach-Bliley (GLBA), Sarbanes-Oxley, the Health Insurance Portability and Accountability Act (HIPAA), and the Patriot Act, the need of mitigating the potential exposure inherent within a typical enterprise-computing environment outweighs the cost associated with multiple internal assessments annually. Additionally, with an in-house program, a more effective rotation of the environment can be implemented, more of the enterprise can be reviewed and a more secure overall computing environment made available.

The overall culture of the enterprise is one of conservatism, with the notable exception being that of the Information Technology area. The dynamic face of the IT landscape demands that new technologies be introduced. Sometimes the appropriate amount of research and development is not performed to determine how to incorporate the new technology across all areas of the enterprise. In this fashion, multiple systems performing the same task have been deployed. While this does solve the immediate business need, additional costs are incurred through duplication, increased staff needs and systems maintenance. To this end, executive management has directed senior IT staff to consolidate systems where appropriate, and to maximize the effort expended to leverage solutions across the enterprise, whenever possible.

The enterprise security program is evolving from a centralized, single-system model to a more flexible, multi-discipline model that provides expertise across a wide scope of skills and systems. Policies have been developed to meet the needs of various computing systems, and a generalized security awareness program has been developed and implemented. However, there is no consolidated method to assess the status of all systems with regard to operating systems patches, application vulnerabilities, open shares and the like. Currently our response is largely reactive, based on various alerting services, such as CERT, vendor sites, and third-party security providers and we are largely dependent upon these agencies for notification of associated vulnerabilities and risks.

This paper will serve to accomplish a major component of a total ISO17799 security program, that is:

- Identification of existing software tools that may provide the foundation of the toolkit.
- Research and identification of additional software tools to meet the requirements as detailed by the Information Security Officer.
- Development of a methodology that will provide the team that is responsible for a particular system with the documentation of all vulnerabilities found.
- In addition to the vulnerability documentation, a remediation plan will be developed in concert with the support team that will mitigate the risk associated with the vulnerabilities found.
- All supporting documentation for each assessment will be located in a

secure, central repository for audit and historical purposes.
- The developed program will be documented and included into the framework of a larger ISO17799 ISMS for the enterprise.

II. Plan

The first step in the planning phase of the ISMS is to form the committee that will be responsible for defining the business objectives of the ISMS. After the business objectives have been defined, risks that map directly to the objectives and the controls that will mitigate the risk will be identified. Some examples of business objectives that the committee should consider are listed here:

Business Objective	Provide secure, reliable transactions to customers during market hours.
Risk	Vulnerabilities cause outages for production systems, idling employees and delaying market trades, incurring fines and fee refunds.
Control	Tools that provide vulnerability identification and assess the security of systems, as part of an overall vulnerability assessment program within the framework of the corporate ISMS.

Business Objective	Provide trusted financial vehicles to customers for growth of personal and institutional portfolios.
Risk	Unauthorized access to customer data could result in compromise of confidential information and lead to loss of corporate image and customer base, as well as fines and levies by the regulatory agencies responsible for industry oversight.
Control	Regular, comprehensive reviews of systems for weak or non-existent security measures, and procedures and recommendations for remediation of the findings, as part of an overall vulnerability assessment program within the framework of the corporate ISMS.

Business Objective	To be the company of choice by providing value and building the highest level of trust with our customers.
Risk	Unauthorized access to customer data or unscheduled systems outages could result in compromise of confidential information and lead to loss of corporate image and customer base, costing the Enterprise both financially and in the industry and community.
Control	Regular, comprehensive reviews of systems for weak or non-existent security measures, and procedures and recommendations for remediation of the findings, as part of an overall risk assessment program within the framework of the corporate ISMS.

The overall scope of the information systems that require oversight for vulnerabilities is large. The majority of the enterprise systems are directly related to customer service, either by telephone requests or by Internet-based self-service transactions. Therefore, the availability of these systems is critical to the customer base for accurate trade execution, fund balances, or fund transfers between financial vehicles. The confidentiality, integrity, availability and security of these systems are monitored by the regulatory commissions at both the state and federal levels. In addition, various other regulatory standards, such as GLBA, Sarbanes-Oxley, the Patriot Act and HIPAA place additional management oversight and responsibilities on the confidentiality, integrity and availability of the information systems.

Once we have identified specific risks, we need to define the actual problems noted to set a baseline perspective. Without specific and effective controls to identify system vulnerabilities, a mitigation strategy or any measuring or monitoring capabilities in place, some estimates have to be made to determine the current state of systems vulnerability within the organization:

- As stated earlier, the enterprise has approximately 2000 employees, the majority of which are directly involved with customer service. If any of the systems that provide real-time customer account information is unavailable for any reason, the direct cost of downtime is substantial.
- The current network topology does not segment the workstation pool from the production environment. This lack of segmentation provides ready access for any device plugged into the network to production systems, with the ability to exploit any known vulnerability directly.
- Current operating procedures do not provide for a method of aggregating system logs for analysis to determine unauthorized access, misconfigurations, or other vulnerabilities.
- The common method of identifying existing vulnerabilities within the enterprise systems involves the contracting of an external entity. Due to the associated cost and the period of time to negotiate terms, the frequency of this type of assessment is relatively long between assessments, usually at most bi-annually for each environment (internal, external, and service network).

To determine whether the internal vulnerability assessment program being designed is successful, the following metrics will be used:

- Tools will be located and installed that can assess potential vulnerabilities across multiple operating systems, such as Intel / Windows, HP/UX and Linux; across multiple database environments, such as Oracle and SQL; and across network devices, such as Cisco, Symantec and McAfee.
- An effective system will be developed and proposed to senior

management for the aggregation and analysis of systems logs across all platforms (all production systems and network devices, and as many database systems as possible). Although this is an integral part of a risk assessment program, the system will not be the focus of this project and will be addressed at a future date.

- Personnel responsible for the management of the risk assessment program will demonstrate the ability to use the tools provided effectively by comparing their results against an assessment provided by an external vendor. The assessment budgeted for this fiscal year will be used for this purpose.

The implementation of the new assessment system will require focused research to determine the tools to be selected, and coordination between the various groups within the Systems area. A timeline for the development of the program has been set at 7 months, with a relatively high-level project plan:

Month 1-3:

- Determine the appropriate operating environment for the toolkit to be developed.
- Identify, research and procure the appropriate tools, either open-source or commercial, that will be included in the toolkit that will be used by the assessment / audit team.
- Develop the structure of the team to implement and administer the program.
- Develop policies and procedures that will encompass the new assessment program.
- Develop the training plan for team members that do not have experience with the tools or operating system chosen for the toolkit.
- Coordinate with the Procurement Team to contract for the external assessment to be used as the control.

Month 4-7:

- Test and implement the toolkit.
- Create an awareness program for the technical personnel that will be affected by the new program.
- Develop a mitigation program based on past remediation efforts and communicate it to the administrative staff responsible for the systems in question.
- Document the new assessment program, with a comparison of the results between the internal program and the external assessment.
- Educate senior management in the basics of the program, so their support, when required, is available and clear.

The management structure of the Technical Services department is straightforward. The parties involved with this program are depicted in the

following diagram:

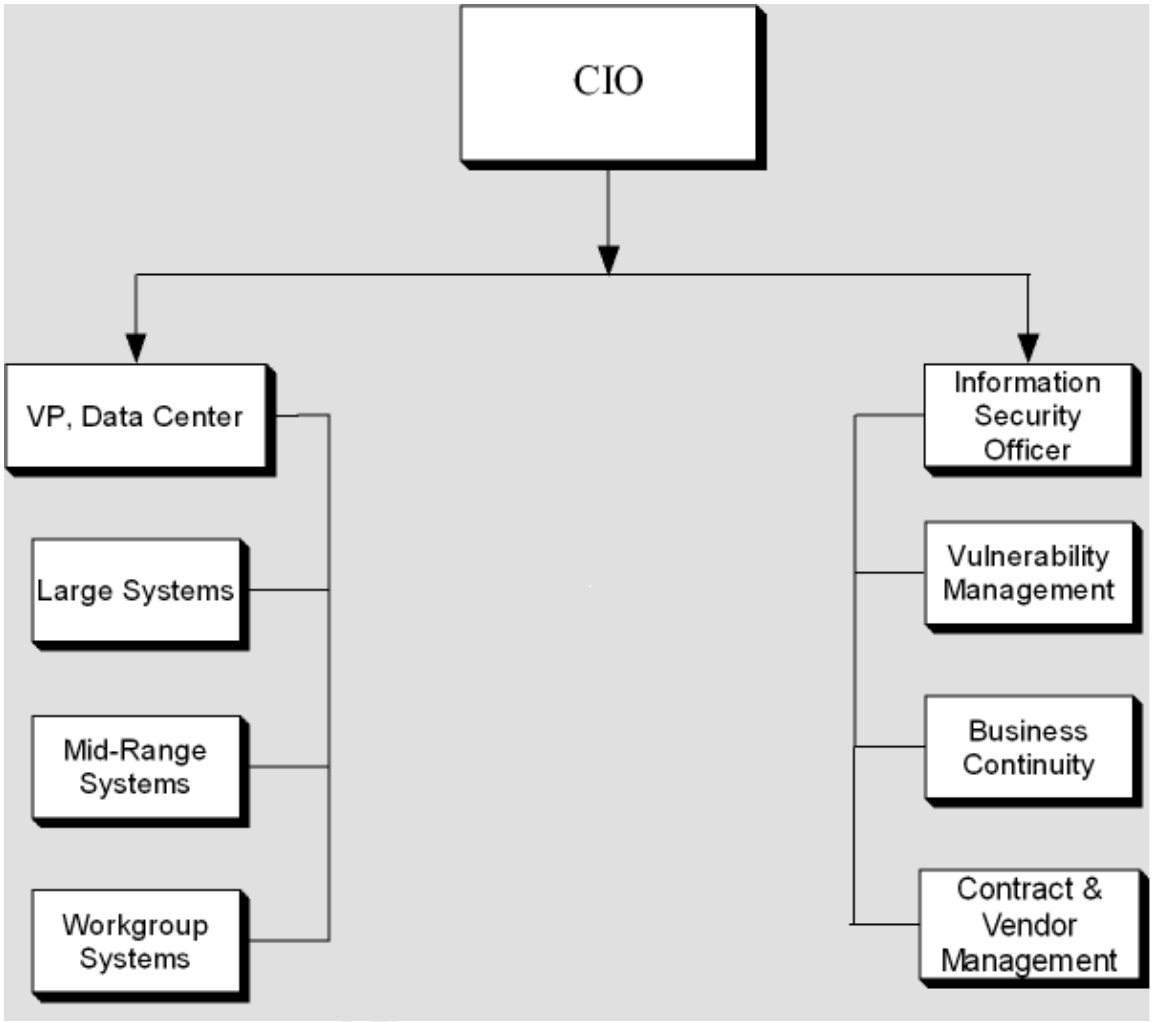

Figure 1: Organization Chart

As the Information Security Officer has the Vulnerability Management team in his area of responsibility, any expenditure incurred in the development of this program will be approved by him. The Vulnerability Management department will be primarily responsible for the maintenance and use of the toolkit developed, and they will be responsible for tracking the remediation efforts spawned by all assessments performed.

Many enterprise information security policies have been developed within the past year, but none that cover the areas that will be impacted by the new program. Therefore, a new policy will be defined that will delineate the areas of responsibility for all affected personnel and systems. Requirements of the tools to be included in the toolkit and procedures for their proper use will need to be documented as well. Last, how this new program fits the overall enterprise security framework will need to be demonstrated.

As the Vulnerability Management team is small (7, including the Information Security Officer) the number of personnel available to assist with this project is small, as well. The primary responsibilities for development of the program will fall on the Information Security Consultant from the Vulnerability Management team with experience in the operating environment that will be used for the toolkit (Windows or Linux), with assistance from the Information Security Officer, who has an extensive technical background and one other Security Analyst in the department. The other team members will be involved to varying degrees, as their skill sets and workload permit.

The Information Security Consultant will identify and assess any potential impact on the information infrastructure that any assessment may cause, and develop a plan for risk mitigation with the help of the applicable systems technical support teams and the Information Security Officer.

The enterprise currently has a team that serves as the Information Security Committee that oversees all security-related activities of the enterprise, as well as development and dissemination of policies and procedures. The Committee consists of the following personnel:

- The Information Security Officer
- The Privacy Officer
- The Vulnerability Management team
- The Business Continuity team

This group currently acts as the Steering Committee for all security initiatives. The following individuals/teams will be most affected by the new program, as with both the current and future systems to be implemented under the enterprise ISMS:

- Information Security Consultant (me) – Manages the project, process and technology choices from an effectiveness and risk management perspective. This will involve identification of the appropriate tools, proper deployment of said tools and writing policies and procedures for the use of the vulnerability assessment toolkit. The security consultant will also define and evaluate the correct implementation of the system.
- Vice President, Infrastructure Services and subordinate technical support teams – This group will be responsible for monitoring the systems under assessment for undesired effects, as well as the remediation efforts to the findings of the assessment.

The Information Security Officer is responsible for the overall security posture and sets Information Security direction for the enterprise. The CIO is involved as the senior management representative and will interface with senior management staff as needed. The Business Continuity team is responsible for contingency plans in the event of outage caused by the assessment process.

The Contract & Vendor Management team is responsible for the negotiation of all necessary contracts for tools and the external assessment.

The policies to be created will be combined into a single, encompassing enterprise-wide policy. The general text within the policy will be clear and concise, using content taken directly from the SANS Policy project: (3) & (4)

1.0 PURPOSE

Define the policy/standard for vulnerability and/or risk assessments of Enterprise computing devices.

2.0 SCOPE/AUDIENCE

This policy includes all Enterprise owned and managed computing devices and is intended for all Enterprise technical staff.

3.0 POLICY

Periodic assessments will be executed against all Enterprise computing systems.

3.1 POLICY EXCEPTIONS

4.0 STANDARD

- All Enterprise production computing systems must have periodic assessments performed against them to ascertain the current level of vulnerability.
- Administrators of all Enterprise computing systems must have a mechanism of notification by the vendor or other recognized reporting entity to identify potential vulnerabilities for the systems they are held accountable.
- All personnel responsible for administration of Enterprise computing systems must have the knowledge and training to recognize and respond to reported vulnerabilities in an agreed-upon timeframe.
- All discoveries made during the execution of any assessment must be reported to management, along with the recommended plan of remediation. Management at that time will make the decision to proceed with correction or to accept the level of risk associated with the vulnerability.
- Risk assessments may be conducted at any entity within the Enterprise.
- Risk assessments may be conducted on any computing system, to include applications, servers and networks, and any process or procedure by which these systems are administered or maintained.
- Execution, development and implementation of remediation plans are the joint responsibility of IT / Vulnerability Management and the department responsible for the systems being assessed.
- Employees are expected to cooperate fully with any assessment being conducted on systems for which they are held accountable.
- Employees are expected to work with IT / Vulnerability Management assessment team in the development of a remediation plan.

5.0 DEFINITIONS

6.0 OWNERSHIP

7.0 AUDIT HISTORY

This policy will include the following key ISO17799 controls (1):

- **Allocation of information security responsibilities** – the policy states that members of the Vulnerability Management team will be responsible for performing the assessment with the properly configured tools, and those members of the relevant technical support teams will be responsible for performing the remediation efforts for the vulnerabilities discovered.
- **Independent review of information security** – the policy specifically relates to vulnerability or risk assessments against the production computing environment within the overall enterprise ISMS.
- **Control against malicious software** – as more advanced malicious coding techniques and specifically targeted attacks become apparent, the consistent review of the enterprise computing environment will provide better confidentiality, integrity and availability of enterprise information assets.

The policy objectives were defined as follows:

- Preventative controls should be in place to minimize the available vulnerabilities for each system.
- Detective controls should detect potential vulnerabilities in any of the systems' components, such as operating system, that have not been remediated.
- Reactive controls should allow the responsible teams to respond quickly to any vulnerability identified by various organizations, such as CERT, and deemed to be a threat to the enterprise and remediate the threat.

Then, the following controls were defined:

Preventative Controls (5):

- All <Enterprise> production computing systems must have periodic assessments performed against them to ascertain the current level of vulnerability.
- Administrators of all <Enterprise> computing systems must have knowledge of a mechanism of notification by the vendor or other recognized reporting entity to identify potential vulnerabilities for the systems they are held accountable.

Detective Controls (5):

- All <Enterprise> production computing systems must have periodic assessments performed against them to ascertain the current level of vulnerability.
- Administrators of all <Enterprise> computing systems must have knowledge of a mechanism of notification by the vendor or other

recognized reporting entity to identify potential vulnerabilities for the systems they are held accountable.

Reactive Controls (5):

- All personnel responsible for administration of <Enterprise> computing systems must have the knowledge and training to recognize and respond to reported vulnerabilities in an agreed-upon timeframe.
- All discoveries made during the execution of any assessment must be reported to management, along with the recommended plan of remediation. Management at that time will make the decision to proceed or to accept the level of risk associated with the vulnerability.

In the case of a risk assessment program, these controls are straightforward. The Preventative controls are only effective when regular, comprehensive systems reviews are performed. If the technical support team of the selected system is not regularly notified of potential vulnerabilities, the potential of security weaknesses remaining available for exploitation are high.

The Detective controls also require the application of regular, comprehensive systems reviews. In this case, the technician performing the assessment must have extensive knowledge of the system, and of how the findings of the assessment affect the vulnerability posture of the system. The technician must have the ability to properly categorize and effectively communicate those findings so the technical support team can respond to the worst threats first.

The Reactive controls are meant to mitigate risks as quickly as possible without causing system outages. The technician performing the assessment must correlate the findings of the assessment, place a rating on each and generate a report for management's review. The technical support teams will be responsible for correcting the findings noted in the report in a timely fashion, or notifying management of the reasons for not correcting any findings. Management will have the responsibility to accept the team's explanation, and therefore accepting the level of risk, or providing the necessary mechanism to correct the risk.

If the preventative controls fail, what are the detective and reactive times we can expect? The first step is to estimate the worst case scenarios for each.

The worst case for detection is never. Even though the technical support teams are diligent concerning the ongoing support of their respective systems, due to the prevailing business climate of today's Information Technology staff, more and more is asked of these staff members with no increase in headcount. In addition, there is very little time or expertise to determine some of the exploits that are reported by various organizations, such as the Internet Storm Center or CERT. As we have seen in some of the alerts released by these organizations, vulnerabilities are an ongoing part of the information technology environment.

Some vulnerabilities are not discovered for months after release of a product. However, for the purpose of this project, we will assume a mean time for detection is 2 days. The Voice and Data Services team are extraordinarily vigilant with regards to network traffic, and would undoubtedly notice any such traffic spikes within this period.

The worst case for reaction and remediation will be set at 2 days also. The team responsible for resolution of issues, such as systems vulnerabilities or malicious activity, will need to determine the appropriate method of remediation and may have to rely on vendor intervention to provide corrective actions.

The following table was developed from the course training to document the range of detective and reactive times we came up with (5):

Event	Detect Time	Response Time	Exposure Time
Worst Case Scenario	2 days	2 Days	96 hours
Best Case Scenario	1 day	Same day as Detection	24 hours
Target	1 day	1 day	48 hours

Based on the above table, the enterprise would be well-served to remediate an issue within 48 hours, if the issue is of high enough severity and risk. A more normal response, in normal practice, is to develop a plan of remediation that allows for proper testing of the proposed corrective action. This plan usually takes much longer than the 96 hours given for the worst case scenario. The period listed for the worst case would be in the event that malicious activity was suspected or noticed.

In order to determine the major risk points, we examine the process flow chart for this process:

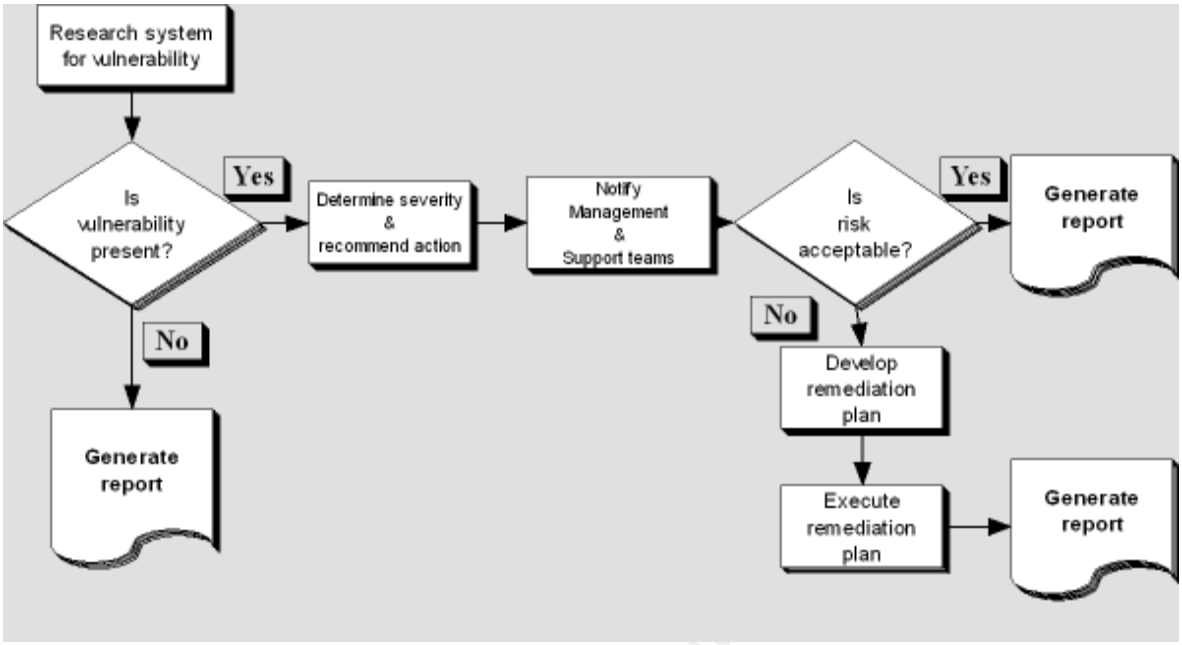

Figure 2: Process Flow chart

Where are the major failure points? A quick review of the process flowchart indicates several, with the following being the worst:

- The assessment tool does not pick up the vulnerability at all.
- The technician places the incorrect level of severity on the vulnerabilities found.
- Management inaccurately chooses to accept the level of risk associated with the vulnerability.

The primary methods for mitigating the risks, as well as the controls needed to implement an effective assessment program are as follows:

- As stated earlier, policies and procedures will be developed, approved and put into place to state the Enterprise's stance on risk assessment effectively and the value of such.
- Information Security personnel need to be adequately trained in the proper use of the selected tools.
- Periodic notification by the appropriate vulnerability reporting agencies needs to be sought by each systems technical support team for each platform or application for which they are held accountable.
- Senior management needs to be educated on the reasons a finding is given a particular severity level, and the options for either risk mitigation or remediation.

To place these in terms of controls defined in the ISO17799 standard, the following may apply (1):

- 3.1.1 & 3.1.2 – Creation of a security policy document (specific to risk assessments), and the ownership, review and maintenance of this document.
- 4.1.7 – Independent review of information security to validate the in-house program is effective and organizational practices reflect the policy.
- 6.3.1 – Reporting of security incidents, where a defined process has been set up for documentation of findings and the associated remediation or risk mitigation efforts.
- 8.1.4 – Segregation of duties, where the assessing entity is not responsible for performing the remediation efforts.
- 8.3.1 – Control against malicious software, with the definition of software in this instance to mean the various vulnerabilities or misconfigurations that are reported.

III. Do

The plan has been developed for implementation of a self-administered risk assessment plan. Now, it is time to lay out a program for each aspect of the plan.

1. Create an effective risk assessment security policy

Problem:

The enterprise has always contracted the execution of a vulnerability assessment to an external authoritative "expert" entity. Therefore, there has been no approved policy to support the development of an in-house assessment program.

Action:

To address this, a security policy will be created with scope across the enterprise.

Steps:

1 – Research available policies for pertinent details to include in the new policy.
2 – Draft an information security policy that encompasses enterprise computing systems and risk assessments.
3 – Review and approve the policy, with final approval by the Information Security Officer
4 – Publish the approved policy to the appropriate parties and make accessible to the enterprise.

2. Develop the toolkit necessary to assess the enterprise environment

Problem:

To date, there has been no effort to locate or procure appropriate tools that can provide the various vectors of a typical vulnerability assessment or penetration test.

Action:

A review of the computing environment is required to determine the types of tools needed. After the tools are identified and acquired, technicians will be trained in the proper configuration, use and interpretation of results.

Steps:

1 – Perform a systems inventory to determine the scope of the toolset requirements.
2 – Review any software already available in-house for applicability.
3 – Locate any additional tools needed, purchase new equipment, etc.
4 – Develop assessment platform, and procure appropriate training for staff responsible for executing the assessment.
5 – Document operating environment and create procedures on proper configuration, operation, capture of raw data and reporting of findings to management and technical staff teams.

3. Develop technical staff awareness training

Problem:

To date, only select platforms have been included in vulnerability assessments. All technical staff areas across the enterprise need to be made aware of this audit function and their roles in it.

Action:

Develop an awareness program that highlights the positive aspects of assessments, and disseminate to all technical staff areas. Develop regular, consistent schedules for review of all enterprise computing environments, to include test systems.

Steps:

1 – Draft a suggested awareness program that invites the technical staff to partner with Vulnerability Management, and present to the Information Security Officer.
2 – After approval from the Information Security Officer, finalize the awareness program and distribute to technical staff areas.
3 – Ensure that communication methods are in place for feedback, and regularly check for use.

4. **Provide technical staff areas with available resources for self-review of current risks.**

Problem:

Technical staff members are very busy and may not know many resources to draw on to keep up with the current methods of attack related to the systems in their area.

Action:

Research and provide a current list of recommended resources that can be used by the staff.

Steps:

1 – Identify various alerting organizations for each major computing system across the enterprise.
2 – Generate a document that details location or URL, systems reviewed, method of notification, etc.
3 – Disseminate to technical staff areas and place in accessible repository.
4 – Regularly review for applicability, update and make available in repository.

5. Provide validity of internal program results

Problem:

There is no method available internally to provide validation of the results obtained from the toolkit.

Action:

Vulnerability Management will contract with an external authoritative "expert" agency to provide control data that will be used to measure the veracity of the in-house program.

Steps:

1 – Coordinate with Contract & Vendor Management team to engage a previously contracted agency to perform a vulnerability assessment against selected Enterprise computing systems.
2 – Develop an assessment plan that will be executed concurrently by both the external agency and Vulnerability Management.
3 – Upon completion of both teams, compile the results of both assessments.
4 – Generate a comparison report for management review to validate or refute the accuracy of the in-house program.

At this point, we can develop Statements of Applicability for the controls we are implementing and those we decided not to. An example for one of the controls we are implementing for the assessment program is listed here (2):

Statement of Applicability for Enterprise Risk Assessment Program
Implement: Fully
Justification for partial or non-implementation: Not applicable

8.3 Protection against malicious software
8.3.1 Control against malicious software

	Description	Implement	Justify	Method	Comment
Control Reference					
8.3.1	Detection and prevention control against malicious software and appropriate staff awareness procedures shall be implemented.	Fully	n/a	Refer to Corporate Risk Assessment Policy and Procedures	For purposes of this control, malicious is to mean systems vulnerabilities

Another example for an implemented control (2):

Statement of Applicability for Enterprise Risk Assessment Program
Implement: Fully
Justification for partial or non-implementation: Not applicable

4.1 Information security infrastructure
4.1.7 Independent review of information security

	Description	Implement	Justify	Method	Comment
Control Reference					
4.1.7	Regular, independent audits of information security policies and procedures will be performed.	Fully	n/a	Refer to Corporate Risk Assessment Policy and Procedures	Independent audits validate or refute the in-house program.

For an example of a control not implemented in this system, the following example is offered (2):

Statement of Applicability for Enterprise Risk Assessment Program
Implement: No
Justification for partial or non-implementation: Not applicable

6.1 Personnel Security
6.1.2 Personnel screening and policy

	Description	Implement	Justify	Method	Comment
Control Reference					
6.1.2	Background investigations will be performed prior to offering a position.	No	n/a	n/a	n/a

IV. Check

Item #1, create an effective risk assessment security policy, and item #3, develop technical staff awareness, will have auditing checklists created to check for compliance. Item #2, developing the risk assessment toolkit, and item #4, developing a list of available resources for the technical staff areas, will not due to the dynamic state these items will be in at all times. All information contained in the following checklists is derived from the ISO17799 audit checklist from SANS (1).

Security Policy checklist (1)

The approved security policy for the risk assessment program portion of the Enterprise ISMS is included in Appendix A.

Reference: 3.1.1 **Audit area:** Information Security policy document

Audit Question

Whether there exists an Information security policy, which is approved by the management, published and communicated as appropriate to all employees.
Whether it states the management commitment and set out the organizational approach to managing information security.

Importance of control

The existence of an information security policy pertaining to the conducting, reporting and remediation of vulnerabilities across the enterprise is important. Clearly stating the expectations to technical staff areas of steps to be taken and scope will foster a consistent approach to minimizing vulnerabilities across the enterprise.

Expectations for compliance

The security policy for risk assessment exists and is available to all enterprise employees in both hardcopy and electronic media (via the Intranet). The policy is effective and makes sense for all areas of the Enterprise.

Audit steps / procedures	Findings	Compliance
1. Check to see if policy exists, and has been approved by management.	Policy exists, and has signature approval.	**YES**
2. Policy is included in written policy handbook, and is available to all Enterprise employees.	Policy is included in master Enterprise policy handbook.	**YES**
3. Policy is available via electronic means on the Enterprise portal, along with all other Enterprise policies.	Policy is available in HTML format on the portal.	**YES**
4. Policy is clear and understandable. Review by members of technical staff areas confirms this.	Personnel in technical staff areas comply with the principles contained within.	**YES**

Technical staff awareness training checklist (1)

The information security awareness training for the technical staff areas will touch on the following:

- Various aspects of general information security,
- The importance of locating and using resources for notification and explanation of vulnerabilities discovered within their respective environments,
- The methods to identify potential compromise,
- When and how to notify the Vulnerability Management team for assistance, and
- The mechanism to report such findings and the remediation effort taken, or the cost of not remediating.

Reference: 6.2.1 **Audit area:** Information security education and training

Audit Question

Whether all employees of the organization and third party users (where relevant) receive appropriate Information Security training and regular updates in organizational policies and procedures.

Importance of control

In the context of the risk assessment program, the technical staff areas are the first line of defense in vulnerability mitigation. The more information they have, and the more they feel included in the development and execution of the overall plan, the more effective and diligent they will be in minimizing the overall risk posture of their respective areas and systems.

Expectations for compliance

New employees receive security awareness training as part of their new hire orientation, and receive information on location of security related documentation. All employees are required to acknowledge, either electronically or by signature, receipt and review of the information security guidelines annually. In addition, Information Security periodically generates articles for inclusion in Enterprise publications.

Audit steps / procedures	Findings	Compliance
1. Do new employees receive security awareness training during new hire orientation?	Members of the Information Security team present training during all new hire orientations.	**YES**
2. Is there irrefutable acknowledgement on file for all users (either hardcopy or electronic)?	Electronic acknowledgements are stored in a secure repository. Hardcopy acknowledgements are stored in a secure facility.	**YES**
3. Is information security documentation available via the Intranet to all employees?	All public policies are available in HTML format on the portal.	**YES**
4. Are all enterprise employees required to annually review and sign, either electronically or hardcopy, the Enterprise Information Asset Protection policy?	Training and acknowledgements are updated annually for all enterprise employees.	**YES**

V. Act

At this point, we have a workable risk assessment program in place. The toolkit has been developed, the technical staff has been made aware of the program and the role they play in the successful execution of the program, and management has been educated to their role in promoting Information Security throughout the enterprise. Now, the program needs care and feeding to remain effective and relevant. The various ways we will accomplish this task are as follows:

- Regularly review and revise policies to keep them relevant with the direction of the Enterprise. All policies are reviewed at least annually for relevancy and applicability. After the Policy team has reviewed and modified the current policy for any changes in the operating environment,

the Information Security Officer performs a final review, approves the updated policy for release to the portal, and replaces the prior version in the master policy handbook.

- Regularly review the tools initially selected for the toolkit for applicability and ability, as well as evaluation of any new tools. As the threats become more intricate and new vulnerabilities are discovered by vendors and reporting agencies, the tools required for detection and correction will change. The question needs to be asked of each tool: Is this the best tool for the task? Are there new tools that can provide a more comprehensive review, or span more systems? In addition, as new tools are included, training for proper use and interpretation will be required.
- Periodic meetings with each technical staff area will be held, to maintain the relationship between the Vulnerability Management team and the technical staff. This relationship is critical in reducing the exposure of the enterprise from potential systems outages.
- On a less regular basis, but still relevant for auditing purposes, an outside entity will be contracted to perform a vulnerability assessment. This will serve several purposes:
    - First, it will either validate or repudiate the findings of the internal team's assessment.
    - Second, it will provide senior management with a mechanism to measure the success or failure of the internal program. This is important due to the budget associated with the program, as well as the personnel cost.
    - Third, it will provide Internal Audit with a independent review of the computing environment in question for regulatory and reporting purposes.
- Regular, consistent assessments will improve the overall security posture of the Enterprise, thereby lowering the overall cost of doing business by minimizing the potential for systems outages, and by extension employee downtime due to outages.
- Review of the methods utilized to track the remediation efforts can lead to improved tracking and reporting mechanisms for both Internal Audit and senior management.

VI. Conclusion

The primary result of this assignment is to establish a process that can be repeated across the enterprise to manage the constant barrage of potential system compromises that can threaten the viability of an organization. A secondary result is development of a repeatable process that can be used to include other systems in the overall ISO17799 ISMS framework.

The next phase in development of an enterprise ISMS will be to apply the process developed here on other areas of the enterprise computing

environment, with the overarching goal of achieving ISO17799 compliance for the organization.

References

1. Thiagarajan, Val in conjunction with the SANS Institute.
   "BS7799.2:2002 Audit Checklist". October 2003
   Available at http://www.sans.org/score/checklists/ISO_17799_checklist.pdf

2. Wilbert, Perri.
   "Getting Serious about Security, article 5". October 16, 2001
   Available at http://security.kingsley.co.za/articles/article5.htm

3. SANS Institute Security Policy Project.
   Available at http://www.sans.org/resources/policies/Audit_Policy.pdf

4. SANS Institute Security Policy Project. Available at
   http://www.sans.org/resources/policies/Risk_Assessment_Policy.pdf

5. SANS Track 11 – SANS 17799 Security & Audit Framework
   Course material, day 5 "Time-Based Analysis". Pages 83 – 108

Appendix A – Risk Assessment Policy (3) & (4)

1.0 PURPOSE

Define the policy/standard for vulnerability and/or risk assessments of Enterprise computing devices.

2.0 SCOPE/AUDIENCE

This policy includes all Enterprise owned and managed computing devices and is intended for all Enterprise technical staff.

3.0 POLICY

Periodic assessments will be executed against all Enterprise computing systems.

3.1 POLICY EXCEPTIONS

4.0 STANDARD

- All Enterprise production computing systems must have periodic assessments performed against them to ascertain the current level of vulnerability.
- Administrators of all Enterprise computing systems must have a mechanism of notification by the vendor or other recognized reporting entity to identify potential vulnerabilities for the systems they are held accountable.
- All personnel responsible for administration of Enterprise computing systems must have the knowledge and training to recognize and respond to reported vulnerabilities in an agreed-upon timeframe.
- All discoveries made during the execution of any assessment must be reported to management, along with the recommended plan of remediation. Management at that time will make the decision to proceed with correction or to accept the level of risk associated with the vulnerability.
- Risk assessments may be conducted at any entity within the Enterprise.
- Risk assessments may be conducted on any computing system, to include applications, servers and networks, and any process or procedure by which these systems are administered or maintained.
- Execution, development and implementation of remediation plans are the joint responsibility of IT / Vulnerability Management and the department responsible for the systems being assessed.
- Employees are expected to cooperate fully with any assessment being conducted on systems for which they are held accountable.
- Employees are expected to work with IT / Vulnerability Management assessment team in the development of a remediation plan.

5.0 DEFINITIONS

6.0 OWNERSHIP

7.0 AUDIT HISTORY