Learning IT Risk Management Function

GIAC - GSEC Certification Option 1
Assignment version 1.4C

Submitted By: Gehad El Bendary

Submitted On: February 20, 2005

TABLE OF CONTENTS

ABSTRACT

This paper is meant to be a generic guidance and provides a reference for IT professionals and IT risk analysts to plan, establish, and maintain a successful an IT risk management function in organizations of all sizes and types. It takes the reader through the different necessary steps and explains how to conduct an IT risk management process (1) Risk Assessment (2) Risk Mitigation, and how to turn it into an ongoing process that drives the organization toward the most useful and cost effective controls to mitigate risks.

Readers are expected to interpret this paper in the context of their own environments and to develop their own specific risk management approaches. Ultimately it is up to the risk makers and the risk takers to develop and manage their own risk management programs.[1]

WHY RISK MANAGEMENT

In this digital era organizations use automated information technology systems to process their information for better support of their missions, IT risk management plays a vital role in ensuring IT resources and assets are being allocated in the most effective way to support the business and therefore its mission from IT-related risk. Also, the process to determine which security controls are appropriate and cost effective is quite often a complex and sometimes a subjective matter. One of the prime functions of IT risk management function is to put this process proactively onto a more objective and systematic basis. Management of IT risk is an integral part of good management. It is an iterative process of continuous improvement that is best embedded into existing practices or business processes. Therefore, the IT risk management function should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization. Some of the specific benefits of IT risk management include:

- Improved planning, performance and effectiveness
- Fewer surprises
- Exploitation of opportunities
- Economy and efficiency
- Improved stakeholder relationships
- Improved information for decision making
- Enhanced reputation
- Director protection

[1] SAI global Website, distributors of Australian Standards. AS/NZS 4360:2004 Risk management, the new edition of the world's premier risk management standard. 2004 <http://www.standards.com.au/catalogue/script/search.asp> (12 Feb 2005)

- Accountability, assurance and governance

STEPS OF IT RISK MANAGEMENT

We should first define important concepts of risk, risk management, risk assessment, risk mitigation and roles & responsibilities as it is used in this paper, as following:

Risk – "the probability of a vulnerability being exploited in the current environment, leading to a degree of loss of confidentiality, integrity, or availability, of an asset."[2]
Risk Management – "It is the overall effort to manage risk to an acceptable level across the business. "[3]
Risk Assessment – "It is the process to identify and prioritize risks to the business. "[4]
Risk Mitigation – "It is the process of identifying safeguards or controls that suitably prevent threat events, detect threat events for subsequent corrective action, or contain the loss that may arise from threat events."[5]

Establishment of clear roles and responsibilities of the necessary IT risk management steps is a critical success factor. The following describes the primary roles and responsibilities of concerned parties:

1. High Level Management – "sponsors and supports all activities associated with managing risk. "
2. Information Technology Team – "providing full support in system characterization process, selecting mitigation strategies and implementing and sustaining control solutions to manage risk to an acceptable level."
3. Risk Management Team – "driving the overall risk management function. "
4. Audit Team – "periodic review to evaluate and monitor efficiency and effectiveness of implemented controls. "

Risk management process encompasses two primary steps, as the following:

1. Risk Assessment

- Systems characterization
- Threat identification
- Vulnerability identification
- Control analysis
- Likelihood determination
- Consequences analysis
- Risk determination
- Control recommendations

[2] Dillard, Kurt and Pfost Jared. The Security Risk Management Guide. October 15, 2004. <http://www.microsoft.com/technet/security/topics/policiesandprocedures/secrisk/srsgch03.mspx> (12 Feb 2005)
[3] Same source as footnotes no. 2
[4] Same source as footnotes no. 2
[5] Ozier, Will. Introduction to Information Security and Risk Management. Vol. 6, March 1, 2003. <http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=543> (12 Feb 2005)

- Results documentation

2. Risk Mitigation

- Mitigation option
- Mitigation strategy

RISK ASSESSMENT

1.0 SYSTEMS CHARACTERIZATION

To accurately assess and measure the potential impact of an IT risk, you must identify and determine the assets (e.g. network components, servers, applications, data ....etc) that are involved in support of critical business processes. It's important that the inventory be exhaustive enough to ensure that a given business process is fully included in the assessment, while not being so inclusive that the assessment becomes unmanageable. For example, if you're trying to make sure fulfillment of a customer online transfer transaction through a bank website is properly protected and secured, you would include all systems, network components and any related processes, procedures or business rules that are involved in fulfilling the transfer.

"Once the business-related systems have been identified, their value must be assigned"[6]. This is one of the most critical steps of the risk assessment process, without proper assignment of business value; the decision-making process supported by risk assessment will be flawed. It's worth the effort to make sure your inventory and definitions are as close to reality as possible as in the "garbage in, garbage out" tradition.

Using a well-structured systematic process for comprehensive identification is also important, because if a critical system component not identified at this stage may be excluded from further risk analysis, approaches used for system characterization include checklists, judgments based on experience and records, flow charts, brainstorming, systems analysis and workshop-based. The approach used will depend on the nature of the activities under assessment, types of risk, and the purpose of the risk assessment.

Business-process owners and IT individuals that they are in charge should be involved at this stage because they will be able to answer questions more accurately. "Additionally, engaging persons in charge in the risk assessment will let you demonstrate how serious you are about making sure the business is well-supported." [7]

Required Output of Step (1). Characterization of the IT system being assessed, a good picture of the IT system environment, and delineation of system boundary. Note "information should be ranked based on asset criticality"

Component	Description
Applications	[Describe key technology components including commercial software]

[6] Paul, Brooke, Risk-Assessment Strategies. October 30, 2000. <http://www.networkcomputing.com/1121/1121f32.html?ls=ncjs_1121bt> (12 Feb 2005)

[7] Same as footnotes no. 6

Databases	
Operating Systems	
Networks	
Interconnections	
Protocols	

2.0 THREAT IDENTIFICATION

A threat is an event that has the potential to cause harm to an IT system. Threat assessments identify the threats that the IT systems may face within your organization. Threats can be classified into three categories: natural threats, environmental threats and human threats. Examples of threats include floods, long-term power failures and network-based attacks for each of the categories, respectively. Threats can be intentional or accidental in nature.

"In assessing threats, it is important to consider all potential threat-sources that could cause harm to an IT system and its processing environment"[8], following table illustrate a sample of a network threat statement:

Threat	Impact
▪ Network based attacks ▪ Malicious software upload ▪ Unauthorized access to confidential information ▪ Long-term power failure ▪ System failures ▪ Technology investment mistakes ▪ Electrical storms ▪ Terminated employees	▪ Attack ▪ System intrusion& break in ▪ Browsing of propriety information ▪ Loss of trade secrets ▪ Data tampering ▪ Fraud, abuse and theft ▪ Systems incompatibility ▪ Business activities disruptions ▪ Reputation could be at risk ▪ Regulatory non compliance ▪ Increased cost of recovery

Table 1- Threat Identification

Reviews of the history of system break-ins security violation reports; incident reports; and interviews with the system administrators, help desk personnel, and business owners during information gathering will help identify threat. Also the following are some sources of information that will help to realistically assess threats:

- Federal Computer Incident Response Center (FedCIRC).[9]

[8] Stoneburner, Gary, Goguen Alice, and Feringa Alexis. Risk Management Guide for Information Technology Systems. July 2002. <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf> (12 Feb 2005)

[9] Federal Computer Incident Response Center Website. "Archived Advisories." <http://www.us-cert.gov/federal/> (14 Feb 2005)

- Mass media, particularly Web-based resources.[10]

Required Output of Step (2) is a threat statement containing a list of threats that are applicable to the IT system being evaluated and could exploit system vulnerabilities.

3.0 VULNERABILITY IDENTIFICATION

Vulnerabilities are weaknesses in a system that has potential to be exploited. Vulnerability identification scope must define whether only technical vulnerabilities will be identified or all vulnerabilities within an organization are targeted. There are different methods and techniques - depending on the criticality of the IT system and available resources - to simply complete the vulnerability identification process as following:

- Automated tools - many commercial and non commercial tools available such as Nessus, ISS' Internet Scanner, and Symantec's Net Recon, all are network tools to scan for vulnerabilities. Also Web application vulnerability assessment tools are available such as N-Stealth, Sanctum's AppScan, and SPI Dynamics WebInspect. However, these tools should not be the only resources used to perform an assessment. Vulnerabilities can exist within your environment that may be not "technical" in nature.
- Security test and evaluation - It includes the development and execution of a test plan (e.g., test script, test procedures, and expected test results).
- Vulnerability Sources – Internet is another source of information, review of industry sources (e.g., vendor Web pages that identify system bugs and flaws), also known system vulnerabilities posted by vendors, along with hot fixes, service packs, patches, and other remedial measures that may be applied to mitigate vulnerabilities. Documented vulnerability sources can be considered such as previous risk assessment documentation of the IT system assessed, The IT system's audit reports, system exception reports, security review reports, vulnerability lists, such as the NIST I-CAT vulnerability database, SANS institute, vendor and security advisories.[11]
- Security Checklist - A security requirements checklist contains the basic security standards that can be used to systematically identify the vulnerabilities of an IT asset.

Required Output of Step (3). Is a list of the system vulnerabilities that could be exploited by the potential threat-sources.

[10] Security Focus Website. "Incidents."<http://www.securityfocus.com/incidents> (14 Feb 2005), SANS Institute Website." Internet Storm Center Reports." <http://isc.sans.org/reports.php> (14 Feb 2005)

[11] ICAT Vulnerability Database Website. "CVE Vulnerability Search Engine." <http://icat.nist.gov/icat.cfm> (14 Feb 2005), SANS Institute." The Twenty Most Critical Internet Security Vulnerabilities." Version 5.0 October 8, 2004. <http://www.sans.org/top20/> (14 Feb 2005), Common Vulnerabilities and Exposures Website. "Standards for Information Security Vulnerabilities Names." <http://cve.mitre.org> (14 Feb 2005)

Threat	Vulnerability	Description	Impact
List Threat as listed in step (2)	List vulnerabilitie s	Describe vulnerabilities	Vulnerability impact

4.0 CONTROL ANALYSIS

This step goal is to analyze the controls that have been implemented, or are planned for implementation to minimize probability of a threat's exercising system vulnerability.

Security controls could be technical and/or non-technical. Technical controls are safeguards that are incorporated into computer hardware, software, or firmware (e.g., access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software). Non-technical controls are management and operational controls, such as security policies; operational procedures; and personnel, physical, and environmental security. The control categories for both technical and non-technical control methods can be further classified as either preventive or detective. These two subcategories are explained as follows:

- Preventive controls – "inhibit attempts to violate security policy and include such controls as access control enforcement, encryption, and authentication." [12]
- Detective controls – "warn of violations or attempted violations and include such controls as audit trails, intrusion detection." [13]

Development of a security requirements checklist or use of an available checklist will be helpful in analyzing controls in an efficient and systematic manner as referred before in step (3). It is essential to update such checklists to reflect changes in the control environment and ensure the checklist's validity.

Output from Step (4). List of current or planned controls used to reduce the impact of adverse events.

Threat	Vulnerability	Controls	Description	status	Type
List of Threat as listed in step (2)	List vulnerabilities as listed in step (3)	List controls	Describe controls	Planned or Current	Preventive Detective Technical or non technical

5.0 LIKELIHOOD DETERMINATION

[12] Stoneburner, Gary, Goguen Alice, and Feringa Alexis. Risk Management Guide for Information Technology Systems. July 2002. <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf> (12 Feb 2005)

[13] Same as footnote no. 11

It indicates a potential vulnerability that could be exercised by a given threat; the following factors must be considered:

- Threat-source capability.
- Nature of the vulnerability.
- Existence and effectiveness of current controls.

The likelihood can be described as high, medium, or low, following Table below describes these three likelihood levels.

Likelihood Level	Likelihood Definition	Indicators
High	The threat is sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.	▪ Potential of it occurring several times within the time period (for example - five years). ▪ Has occurred recently.
Medium	Threat is capable, but controls are in place that may impede successful exercise of the vulnerability.	▪ Could occur more than once within the time period (for example - five years). ▪ Could be difficult to control due to some external influences. ▪ There is a history of occurrence
Low	Threat lacks capability, and controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.	▪ Has not occurred. ▪ Unlikely to occur.

Table 2 - Likelihood Level & Definition[14]

Required Output of Step (5) is a Likelihood rating (High, Medium, and Low)

Threat	Vulnerability	Controls	status	Type	likelihood levels
List of Threat as listed in step (2)	List vulnerabilities as listed in step (3)	List controls	Planned or Current	Preventive Detective Technical or non technical	Medium Low High

[14] Stoneburner, Gary, Goguen Alice, and Feringa Alexis. Risk Management Guide for Information Technology Systems. July 2002. <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf> (12 Feb 2005)

6.0 IMPACT ANALYSIS

It is a major step; measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of vulnerabilities. Impact analysis can be described in terms of loss or degradation of any, or a combination of the following three security goals:

- Integrity
- Availability
- Confidentiality

The following Table provides a brief description of each security goal and the consequence (or impact) of its not being met:

Security Goal	Consequence / Impact
Integrity	Use of compromised system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. Loss of integrity reduces the assurance of an IT system.
Availability	Loss of system functionality and operational effectiveness may result in loss of productive time, affecting the end users' performance of their functions in supporting the organization's mission.
Confidentiality	Loss of public confidence, embarrassment, or legal action against the organization.

Table 3 – Security Goal Definition

6.1 Quantitative & Qualitative analysis

There are many different methodologies for prioritizing or assessing impact of risks, but most are based on one of two approaches or a combination of the two: qualitative risk management or quantitative risk which are defined respectively as "words used to describe the magnitude of potential consequences and the likelihood that those consequences will occur", "numerical values for both consequences and likelihood using data from a variety of sources".

In conducting the impact analysis, consideration should be given to the advantages and disadvantages of qualitative versus quantitative assessments.

	Quantitative	Qualitative

Advantage	▪ Risks are prioritized by financial impact; assets are prioritized by financial values. ▪ Results facilitate management of risk by return on security investment ▪ Results can be expressed in management-specific terminology (e.g., monetary values and probability expressed as a specific percentage) ▪ Accuracy tends to increase over time as the organization builds historic record of data while gaining experience	▪ Enables visibility and understanding of risk ranking ▪ Easier to reach consensus ▪ Not necessary to quantify threat frequency ▪ Not necessary to determine financial values of assets ▪ Easier to involve people who are not experts on security or computers
Disadvantage	▪ Impact values assigned to risks are based on subjective opinions of participants ▪ Process to reach credible results and consensus is very time consuming. ▪ Calculations can be complex and time consuming ▪ Results are presented in monetary terms only, and they may be difficult for non-technical people to interpret. ▪ Process requires expertise, so participants cannot be easily coached through it	▪ Insufficient differentiation between important risks ▪ Difficult to justify investing in control implementation because there is no basis for a cost-benefit analysis ▪ Results are dependent upon the quality of the risk management team that is created

Table 4 – Quantitative & Qualitative Comparison [15]

Additional factors often must be considered to determine the magnitude of impact; these may include, but are not limited to:

- Frequency of the threat-source's exercise of the vulnerability over a specified time period (e.g., quarterly).
- An approximate cost for each occurrence of the threat-source's exercise of the vulnerability.
- A weighted factor based on a subjective analysis of the relative impact of a specific threat's exercising a specific vulnerability.

Impacts could be tangible which can be measured quantitatively in lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action. Other impacts (e.g., loss of public confidence, loss of credibility, damage to an organization's interest) cannot be measured in specific units but can be qualified or

[15] Dillard, Kurt and Pfost Jared. The Security Risk Management Guide. October 15, 2004. <http://www.microsoft.com/technet/security/topics/policiesandprocedures/secrisk/srsgch02.mspx> (12 Feb 2005)

described in terms of high, medium, and low impacts.

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) May significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

Table 5 – Magnitude of Impact Definition [16]

Required Output of Step (6) is a Magnitude of impact (High, Medium, or Low)

Threat	Vulnerability	Controls	likelihood levels	Impact Levels
List of Threat as listed in step (2)	List vulnerabilities as listed in step (3)	List controls as listed in step (4)	High Medium Low	High Medium Low

7.0 RISK DETERMINATION

The purpose of this step is to assess and determine the level of risk. This can be expressed as a function of:

- The likelihood of a given threat-source's attempting to exercise a given vulnerability – as explained in step (5)
- Impact if a threat-source successfully exercise the vulnerability – as explained in step (6)
- The adequacy of planned or existing security controls for reducing or eliminating risk – as explained in step (4)

A risk scale and a risk-level matrix must be developed to measure risk; following is a standard risk-level matrix;

Threat Likelihood	Impact

[16] Stoneburner, Gary, Goguen Alice, and Feringa Alexis. Risk Management Guide for Information Technology Systems. July 2002. <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf> (12 Feb 2005)

	Low (10)	**Medium** (50)	**High** (100)
High (1.0)	**Low** 10 X 1.0 = 10	**Medium** 50 X 1.0 = 50	**High** 100 X 1.0 = 100
Medium (0.5)	**Low** 10 X 0.5 = 5	**Medium** 50 X 0.5 = 25	**Medium** 100 X 0.5 = 50
Low (0.1)	**Low** 10 X 0.1 = 1	**Low** 50 X 0.1 = 5	**Low** 100 X 0.1 = 10

Table 5 – Magnitude of Impact Definition [17]

Table above shows how the overall risk ratings might be determined based on inputs from the threat likelihood and threat impact analysis, determination of a risk is derived by multiplying the ratings assigned for threat likelihood and threat impact. The matrix is a 3 x 3 matrixes, threat likelihood (High, Medium, and Low) and threat impact (High, Medium, and Low). Depending on the purpose of risk assessment desired, 4 x 4 or a 5 x 5 matrix may be used, include a Very Low /Very High threat likelihood and a Very Low/Very High threat impact to generate a Very Low/Very High risk level. A "Very High" risk level may require possible system shutdown or stopping of all IT system integration and testing efforts.

Matrix above shows how the overall risk levels of High, Medium, and Low are determined as following:

- Probability assigned for each threat likelihood level is 1.0 for High, 0.5 for Medium, 0.1 for Low
- Value assigned for each impact level is 100 for High, 50 for Medium, and 10 for Low.

The risk scale used to compare against risk level presents actions that senior management, mission owners, must take for each risk level, following table shows risk scale and necessary action required.

Risk Level	**Necessary Action Required**
High	There is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	Corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	Decision must be taken whether corrective actions are still required or decide to accept the risk.

Table 6 – Magnitude of Impact Definition [18]

[17] Same as footnotes 16

[18] Stoneburner, Gary, Goguen Alice, and Feringa Alexis. Risk Management Guide for Information

Required Output of Step (7) is a prioritized risk level based list with (High, Medium, Low Risk level)

Threat	Vulnerability	Controls	likelihood levels	Impact Levels	Risk Level
List of Threat as listed in step (2)	List vulnerabilities as listed in step (3)	List controls as listed in step (4)	High Medium Low	High Medium Low	High Medium Low

8.0 CONTROL RECOMMENDATIONS

The step of control recommendations for identified risks is the results of the risk assessment process and provides input to the risk mitigation process. It should be noted that not all possible recommended controls can be implemented to reduce loss. The following factors should be considered when IT risks analysts recommending controls and any other alternative solutions to minimize or eliminate identified and assessed risks:

- Effectiveness of recommended controls
- Legislation and regulation compliance
- Organizational policy compliance
- Operational impact
- Safety and reliability

To determine which controls are required and appropriate for a specific organization, a cost-benefit analysis should be conducted for the proposed recommended controls to demonstrate the costs of implementing the controls and it can be justified by the reduction in the level of risk. In addition, the operational impact (e.g., effect on system performance) and feasibility (e.g., technical requirements, user acceptance) of introducing the recommended option should be evaluated carefully.

Required Output of Step (8) is a Recommendation of control(s) and alternative solutions.

9.0 RESULTS DOCUMENTATION

Once the risk assessment phase has been completed (threat-sources and vulnerabilities identified, risks assessed, and recommended controls provided), "Different levels within the organization need different information from the risk management process"[19].

Technology Systems. July 2002. <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf> (12 Feb 2005)

[19] The Institute of Risk Management Website. A Risk Management Standard. 2002. <http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf> (12 Feb 2005)

- Board of directors
- Mission owners
- Individuals
- External reporting (if applicable or based on organization activity)

Results should be documented in an official report and/or briefing presentation. This report will help senior management, the mission owners to make proper decisions. Report should be presented in a systematic and analytical approach so that senior management will understand the risks and allocate resources to reduce and correct potential losses. It should include but not limited to the following:

- Observation number and brief description of observation (e.g., Observation 1: No network diagram exists cataloguing all network components)
- Listing of the threat-source and vulnerability pair
- Analysis and listing of existing mitigating security controls
- Likelihood determination and evaluation (e.g., High, Medium, or Low)
- Impact analysis discussion and evaluation (e.g., High, Medium, or Low)
- Risk rating based on the risk-level matrix (e.g., High, Medium, or Low risk level)
- Recommended controls or alternative options for reducing the risk to an acceptable level.

Required Output of Step (9) is a Risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation.

RISK MITIGATION

1.0 MITIGATION OPTION

Risk mitigation as defined previously is a systematic methodology used to reduce risks through any of the following risk mitigation options[20]:

- Risk Assumption - To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level.
- Risk Avoidance - Eliminating the risk cause and/or consequence (e.g., stop certain functions of the system or shut down the system when risks are identified).
- Risk Limitation - Implementing controls that minimize the adverse impact of a threat's exercising vulnerability (e.g., use of supporting, preventive, detective controls).
- Risk Planning - Developing a risk mitigation plan that prioritizes, implements, and maintains controls.
- Research and Acknowledgment - To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability.
- Risk Transference - Using other options to compensate for the loss, (e.g., purchasing insurance).

2.0 MITIGATION STRATEGY

Senior management, mission owners will need to implement recommended controls to mitigate risks and protect the organization. Mitigation step involves the selection and implementation of security controls to reduce risk to the acceptable level. The following activities need not be performed as sequenced.

- Select appropriate safeguards or controls
- Accept residual risk
- Implementing controls and monitoring effectiveness

Implemented controls to continue to be effective, IT risk management process needs to be an ongoing process. This requires a periodic assessment and improvement of safeguards and reanalysis of risks.

Monitoring process should be established and to be an ongoing process, it provides assurance that there are appropriate controls in place for the organization's activities and that the procedures are understood and followed. Concerned departments should provide progress reports to IT risk analysts on a periodic basis. Key elements of an effective monitoring

[20] Stoneburner, Gary, Goguen Alice, and Feringa Alexis. Risk Management Guide for Information Technology Systems. July 2002. <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf> (12 Feb 2005)

program include:

- Mitigation or corrective action plans
- Clear assignment of responsibilities and accountability
- Management reporting

Metrics, as part of the monitoring process, will aid IT risk analyst in its ability to assess the effectiveness of implemented mitigation strategy. The specific metrics reported, and the frequency, will depend upon the IT environment of the organization. Some common examples are:

- The current number of risk issues identified for each IT discipline (updated regularly to reflect new or mitigated issues)
- The current number of risk acceptance issues approved by senior management (a database or other repository of the descriptions, mitigation options, and evidence of management acceptance should be maintained)
- The average time elapsed between vulnerability or weakness and implementation of corrective action
- Percentage of total systems for which security controls have been tested and evaluated in the past year
- Percentage of systems compliant with the separation of duties requirements
- Current and historical counts of events or issues (external and internal) events that deviate from the control standards
- Current counts of internal audit, external audit, or regulator identified issues.

CONCLUSION

Information technology systems may be in risk of falling out of alignment with the business it is meant to protect, therefore Identifying, assessing and mitigating IT risks is an essential and critical function to be performed, which in nature is an ongoing process that evaluates the IT environment and potential changes. Success factor of a risk management function will be but not limited to the following:

- Senior management's commitment
- Full support and participation of the IT team
- Competence of the risk assessment team, which must have the expertise to apply the risk assessment methodology to a specific system, identify mission risks, and provide cost-effective safeguards that meet the needs of the organization
- A clear definition of roles and responsibilities
- Awareness and cooperation of members of the user community, who must follow procedures and comply with the implemented controls to safeguard the mission of their organization
- IT team is responsible for implementing controls that have been selected when the probability of an exploit presents an unacceptable risk
- An ongoing evaluation and assessment of the IT-related mission risks

REFERENCES

Stoneburner, Gary, Goguen Alice, and Feringa Alexis. Risk Management Guide for Information Technology Systems. July 2002. <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf> (12 Feb 2005)

The Institute of Risk Management Website. A Risk Management Standard. 2002. <http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf> (12 Feb 2005)

Dillard, Kurt and Pfost Jared. The Security Risk Management Guide. October 15, 2004. <http://www.microsoft.com/technet/security/topics/policiesandprocedures/secrisk/srsgch03.mspx> (12 Feb 2005)

Ozier, Will. Introduction to Information Security and Risk Management. Vol. 6, March 1, 2003. <http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=543> (12 Feb 2005)

Paul, Brooke. Risk-Assessment Strategies. October 30, 2000. <http://www.networkcomputing.com/1121/1121f32.html?ls=ncjs_1121bt> (12 Feb 2005)

SAI global Website, distributors of Australian Standards. AS/NZS 4360:2004 Risk management, the new edition of the world's premier risk management standard. 2004 <http://www.standards.com.au/catalogue/script/search.asp> (12 Feb 2005)

Baccam, Tanya. Reducing the Security Risk to Your Enterprise. January 2002. <http://www.vigilar.com/img/whitepapers/20020210_Assessment_Whitepaper.pdf> (14 Feb 2005)

Paul, Brooke. Risk-Assessment Strategies. October 30, 2000 <http://www.networkcomputing.com/1121/1121f32.html?ls=ncjs_1121bt> (14 Feb 2005)

Edmead, Mark. Explaining the Risk Management Process. 09 Oct 2002 <http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci855103,00.html> (14 Feb 2005)

Federal financial institution examination council (FFIEC) Website. Management Booklet. Date Unknown <http://www.ffiec.gov/ffiecinfobase/booklets/mang/toc.htm> (14 Feb 2005)

National Webcast Initiative Website. Detailed Security Risk Assessment Template. Date Unknown <http://www.cscic.state.ny.us/msisac/webcasts/8_04/804_template.pdf> (14 Feb 2005)

Swanson, Marianne and Guttman Barbara. Generally Accepted Principles and Practices for Securing Information Technology Systems. September 1996<http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf> (14 Feb 2005)

Federal Computer Incident Response Center Website. Archived Advisories. <http://www.us-cert.gov/federal/> (14 Feb 2005)

Security Focus Website. "Incidents."<http://www.securityfocus.com/incidents> (14 Feb 2005)

SANS Institute Website." Internet Storm Center Reports." <http://isc.sans.org/reports.php> (14 Feb 2005)

ICAT Vulnerability Database Website. "CVE Vulnerability Search Engine." <http://icat.nist.gov/icat.cfm> (14 Feb 2005)

SANS Institute." The Twenty Most Critical Internet Security Vulnerabilities." Version 5.0 October 8, 2004. <http://www.sans.org/top20/> (14 Feb 2005)

Common Vulnerabilities and Exposures Website. "Standards for Information Security Vulnerabilities Names." <http://cve.mitre.org> (14 Feb 2005)

Swanson, Marianne, Bartol Nadya, Sabato John, Hash Joan and Graffo Laurie. Security Metrics Guide for Information Technology Systems. July 2003 <http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf> (18 Feb 2005)