Global Information Assurance Certification Paper

Performing a Process-Based Information Security Risk Assessment

GIAC Security Essentials Certification (GSEC)

Practical Assignment - Option 1
Version 1.4b Option 1 (amended August 29, 2002)

Shirley Warthen
April 7, 2004

Introduction:

This paper is an investigation of a process-based technical risk assessment. Theoretically, this approach will provide a picture of where the risks lie, what process is generating the risk, and provide an easier method of defining how the risks can be mitigated. In addition, as potential countermeasures are identified, mitigation steps can begin prior to the completion of the entire assessment.

Background:

"Risk is the possibility of suffering harm or loss. It is the potential for realizing unwanted negative consequences of an event. It refers to a situation where a person could do something undesirable or a natural occurrence could cause an undesirable outcome, resulting in a negative impact or consequence." (Alberts, p.1)

Common sense and best practice calls for a proactive stance in risk control. In addition; GLBA, HIPPA, and Sarbanes-Oxley; the three newest information related laws, mandate a risk assessment approach to Information Management in order to assure that confidential information remains confidential. There are many different standards and ideas of how to perform an Information Security Risk Assessment. Most methods use an asset-based approach and are very complex. Because of the complexity and scope, these assessment methods are very time and resource consuming.

A complete risk assessment includes every aspect of the business it reviews, and is important to perform. Because it takes a global approach, it takes a tremendous amount of time, effort, and resources. In the process, it may miss some of the technical issues that introduce risks and miss steps that could mitigate risk. In order to narrow the scope and speed up the process; including the mitigation process; this assessment will focus on an organization wide view of information security risks and technical processes only.

The precedence for the use of a process-based approach to analysis comes from the Federal Financial Institutions Examination Council (FFIEC). "Member agencies of the Federal Financial Institutions Examination Council (FFIEC) defined such a process-based approach to security in the "Guidelines Establishing Standards to Safeguard Customer Information" to implement section 501(b) of the Gramm–Leach– Bliley Act of 1999 (GLBA)." (FFIEC, p1)

In order to evaluate the level of risk, the assets or resource and their value must be considered during the risk assessment process. The asset must be protected, however, this assessment method doesn't use the asset as the primary focus. It is the process, application, or function used to access the

asset that is the source of the risk. Therefore, the source of the risk is the focus of this risk assessment.

Three types of knowledge are needed at different stages of the assessment process; business, technical, and information security. Business managers and employees understand the business needs and the tasks they perform to operate the business. Technicians understand the technical process but may not comprehend the business processes or the reasons for those processes, in addition technicians traditionally are focused on availability and making systems perform for the business processes. An information security focus is the third type of knowledge needed for the analysis process. Together the processes used to operate the business can be effectively defined. Once those processes are defined, the risks can be reviewed, current and potential countermeasures identified and residual risk measured. All three types of knowledge, and support from management from each segment, needs to be part of the review to gain a clear understanding of the reasons for changes that ultimately will occur. In addition, in order to accurately evaluate the impact of potential risk mitigation steps all three perspectives must be included.

Ongoing communication between the three knowledge sources and with management is essential to the success of this process. Scheduled sessions, status reports, and documentation regarding all communication are a necessity. As the SANS GSEC course states, "If it is not in writing it never happened." (Cole, p.337)

Technical Basics:

Maintaining network security should be a primary Information Technology professional concern. In addition, monitoring network security is a daily process; it only takes one technical mistake to expose the business to very-high risk. Technical risk assessments could be a full time job and waiting until the assessment is complete leaves the company vulnerable. Action must be taken to mitigate the risks and continued assessment must be performed to assure all risks are investigated and mitigation performed.

In order to understand the organization's vulnerabilities, an accurate inventory of systems and the services, processes, and software that run on those systems is an essential tool. A list of services isn't enough. In the past year vulnerabilities have been identified in DirectX and ASN.1 library, both of which are internal to the operation of Microsoft Windows Operating system, proves that knowing just the services active on each machine isn't enough. The internal operation of each system includes potential risk. It is essential to read vulnerability notices as they are released, researching anything that isn't familiar and document the research as it's performed, noting each new threat researched. Keep lists noting what each threat effects. Chances are good that a new implementation

could be impacted by a vulnerability that was announced prior to implementation. Incorporating software tools that check for vulnerabilities (Nessus, HFNetCk, etc.) into this process can help, however, this should be combined with knowledgeable human evaluation. A technical person with comprehensive knowledge of the system combined with vulnerability assessment software can identify vulnerabilities that need to be acted upon immediately.

Notices from Cert, Sans, Microsoft, and many other information sources arrive almost daily with newly identified vulnerabilities. Since the IT environment changes daily and most organizations have systems that change continuously, this must be a cooperative effort.

Risk Assessment Steps:

There are multiple steps to any analysis many of which can simply be described as gathering who, what, when, where, why, and how for each step. The information gathering stage will reveal answers to many of the steps. Try to glean information for all the steps as you investigate the process or application.

Make lists and add information to the lists throughout the process. For example, while you are listing the business processes in step one the criticality of that process may become very evident – note that information, everything that can be learned about a process can yield information essential to the assessment process.

1. List business process and applications (business element).

List every service or product provided by the business, include a brief description, the method used to provide the business element, and list the technical resources used in the process. Flow-charting or diagramming the process will help to identify every detail, missing a step of the process could result in unidentified risks. This list should include everything, rating each process or application for business criticality, breadth of use, and volume of use as they are identified. This will clarify which ones are key or critical processes or applications.

Business Criticality – impact of damage or loss. - Can the business continue to operate without the process or application?
Breadth of use – How many business functions depend on the process or application?
Volume of use – the process may only be used in one area and have significant impact on the business due to quantity.

Describe or define the process being evaluated including the details about how the process works. List everything that influences the process including people,

physical location, equipment, operating system, software, communication, and data. Each piece of the process has the potential to introduce different types of risks. The method used to track the process can be a list, flowchart, or any other method that results in a clear understanding of every detail of the process. It may be helpful to create two different documentation methods (i.e. bulleted list and flow chart) or have two people document the same process in two different ways. Whatever works for the team of people that perform the assessment.

Some business elements to consider are: (remember – who, what, when, where, why, and how)

- Access
- Anti-Virus practices
- Application Management practices
- Authentication
- Availability
- Backup and restore processes
- Communication
- Customer services provided
- Data storage management
- Data storage methodologies
- Electronic connections with business partners, evaluate each connection separately.
- External Email received (Malware vulnerabilities)
- Firewall management practices
- Information
- Integration
- Management
- Modem use
- Outbound external Email (Confidentiality, Reputational risk)
- Password change practices
- People
- Physical access to technical resource (servers, routers, etc.)
- Products created and/or sold
- Security Practices
- Server Management practices
- System access methodology
- System Architecture/Infrastructure
- Technical staff security training
- Usage
- User Management practices
    - Creation
    - User log-on hours
    - Password settings

    - Account expiration settings
    - User permissions (including inherited permissions)
- Utilization of External Internet based services
- WAN and LAN communication methodologies and pathways
- Web Services provided

This is not a complete list, just an alphabetical list to get started. Categorizing the results of this step will help clarify the analysis steps to follow.

2. Identify the types of business risk.

List the types of risk inherent to the type of business being analyzed. Although business risk isn't the focus of this assessment, technical risk can impact many or all of the business risk areas. "Business activities present various combinations and concentrations of risks depending on the nature and scope of the particular activity." (FRB SR 95-51, p.4) Understanding the types of risks is essential to evaluating the level of risk.

For some businesses, risk identification is done for them by their regulators. For the financial industry, the Board of Governors of the Federal Reserve System, one type of bank regulator, has categorized the types of business risks for banks as:

> *Credit risk* arises from the potential that a borrower or counterparty will fail to perform on an obligation.
>
> *Market risk* is the risk to a financial institution's condition resulting from adverse movements in market rates or prices, such as interest rates, foreign exchange rates, or equity prices.
>
> *Liquidity risk* is the potential that an institution will be unable to meet its obligations as they come due because of an inability to liquidate assets or obtain adequate funding (referred to as "funding liquidity risk") or that it cannot easily unwind or offset specific exposures without significantly lowering market prices because of inadequate market depth or market disruptions ("market liquidity risk").
>
> *Operational risk* arises from the potential that inadequate information systems, operational problems, breaches in internal controls, fraud, or unforeseen catastrophes will result in unexpected losses.
>
> *Legal risk* arises from the potential that unenforceable contracts, lawsuits, or adverse judgments can disrupt or otherwise negatively affect the operations or condition of a banking organization.
>
> *Reputational risk* is the potential that negative publicity regarding an institution's business practices, whether true or not, will cause a decline in the customer base, costly litigation, or revenue reductions. (FRB SR 95-51 p.4)

All of the above listed risks could impact a majority of businesses. Credit Risk seems like a financial industry specific risk, however, Accounts Receivable Risk could be substituted for Credit Risk as it has the same general impact.

3. List the general categories of technical risks and vulnerabilities.

Again, understanding the risks and vulnerabilities is essential to evaluating the level of risk. Vulnerability is defined as any flaw, weakness, exposure, condition, or situation in a system's design, implementation, operation, or management that could increase the potential that a threat will result in a loss or exploit.

Systems are very complex with diverse processes and functionality. Every process and function can present it's own risks. Every week new vulnerabilities are discovered, malicious code appears to have taken on a life of it's own as it changes to avoid detection through polymorphism.

Two key words here are **general categories.** In order to expedite the analysis process the initial technical list should be a general listing. A person could spend their career developing a comprehensive list of technical risks.

The details are important but, at this point, they could result in a failure to complete the risk assessment. Later in the analysis and mitigation process, a more detailed review of the specifics of the associated vulnerabilities will need to be incorporated for a complete picture and risk mitigation.

Categorizing the risks could be helpful. Consider confidentiality, integrity, and availability as the vulnerability list is developed:

- Access Control and/or Authentication Component – is the process or application being evaluated a part of providing access to systems?
- Accessibility via modem – are modems connected to any of the resources utilized for the process or application?
- Proximity to the Internet access – is the system or application isolated from Internet access?
- Confidential Information Stored – is non-public information stored within the process, application, or included in the resources used?
- Customer Related Use – Do customers have direct access or do employees use the process or application to provide information or service.
- Data Access – the number of access points to a data source.
- Unauthorized access (Physical or electronic, hackers or vandals)
- Information Quantity – how much confidential information is included or accessed?
- Hardware age – how old is the hardware currently in use?
- Hardware redundancy – is replacement hardware available immediately,

are there redundant components in the system?

- Hardware Specialty – can replacement hardware be acquired easily from any source or is it custom equipment that is not easily obtained?
- Infrastructure design – The physical and logical architecture, organization of data, network communication, system capacity as it relates to business needs.
- Malicious Code (virus, worm, trojan)
- New technologies – any new implementation comes with additional vulnerabilities, including the technical learning curve.
- Operating System Vulnerabilities – what is the level of vulnerability inherent to the operating system? One part of this component is the number of Services enabled.
- Services activated - (IIS, FTP, DHCP, SMTP, etc.) some operating systems install and activate all services, others install with only the basics, either way only the services required for the system to operate properly should be active.
- System Controls allowed from outside source - ActiveX or Java Applet controls sent by external source to workstations with local administrator access, allows the external source to control functionality. This could result in vulnerabilities that may not be identified immediately, which could spread throughout the entire network.
- Technical Mistakes – "Technological holes account for a great number of the successful break-ins, but people do their share, as well." (Mistakes, p.1)

4. Develop a rating scale for each technical risk category.

Risk assessment isn't just a yes or no process, the level of risk is important.

Each component listed will have some level of risk; therefore, in order to rate the component, a list pertaining to the potential level of risk should be developed. This can be a 0 to 5, 0 to 10, 0 to 100, or any logical rating criteria that pertains to the item being rated. An example of the rating scale for a few categories listed in steps one and three are shown below:

Business Criticality

1 Not critical
5 Significant
10 Essential

Breadth of use – evaluate the percentage of employees that utilize the process or application in support of their activities

0 Minimal use (testing or non production)
10 Used by a few

25 Used by several
60 Used by majority
90 Used by most
100 Used by all

Accessibility via modem

0 No modem connected to system or any systems in the network segment.
10 Modem connected, off unless technical employee monitoring use throughout entire use.
25 Modem connected, off unless support scheduled, use not visually monitored. – Highly Trusted external user based on historical experience.
75 Modem connected, off unless support scheduled, use not visually monitored. – No historical experience with external user.
100 Modem connected with active remote software enabled - on all the time.

5. Process Analysis.

A risk analysis is an ongoing information gathering process. During the evaluation steps note any additional information not previously identified that should be included in the assessment. Continue to clarify the teams understanding and document the elements listed in step one rating them using the lists created in steps two, three, and four.

Perform the following for each process and application identified in step one:

▷ Identify

Analyze the inherent risk based on the business risk elements and technical risk elements identified. In order to accurately measure the current status of OS vulnerabilities, technical vulnerability (VA) scans should be performed during this phase of the analysis.

▷ Measure

Analyze and assess the size and significance of risk, the current risk mitigation practices. Use a matrix of risk elements with control elements, assessing how the inherent risks are lessened.

Create a results summary, by process and application, of the residual risk.

Assess the stability of the residual risk, is it stable, increasing, or decreasing.

▷ Facilitate appropriate follow-up action.

Develop a plan for managing and addressing the mitigation of risk (internal controls) for those areas of greatest residual risk and those areas of increasing residual risk.

▷ Control

Document and test the follow-up actions

▷ Monitor

Create a review schedule to assess the risk mitigation controls, by process and application, based on the risk ratings. The risk ratings could easily change as different portions of the process change.

Any very-high or high rating should be communicated immediately to management. This may enable the risk to be mitigated quickly especially if it is just a matter of turning off an unused vulnerable service.

6. List the risk mitigation practices available for each process. (Controls)

Risk mitigation, control, or countermeasure is any "Action or combination of actions involving physical, technical, administrative, procedural, or other measure(s) taken to reduce the severity of risk" (Risk, USCG, p.3)

This step can be very effective in brainstorming sessions. Participants need to be willing to look at both the practices that are currently in use and any mitigation steps that could be performed. Don't overlook the obvious and don't dismiss what initially seems to be ludicrous. As with any brainstorming session, comments build upon each other and may result in a great solution.
Achieve an appropriate level of protection as it relates to the value of the assets and the prevention of unauthorized access, which could lead to the loss of integrity (modification), availability (destruction), and confidentiality (disclosure).

Some Risk mitigation practices that can be considered are:

- Active management oversight and controls
- Change management - Repair or Addition of functionality, followed by assessment and new baseline
- Configuration management - Establish baseline then manage that condition (Maintaining hardened systems)
- Accurate inventory of systems, services, and processes
- Evaluate new implementations for threats and vulnerabilities
- Defense-In-Depth (not satisfied with one mitigation when several are available)
- Detection methods (fraud, abuse, intrusion, baseline notification)
- Disable unused services, regular review to confirm no change to active services
- Document "mean time between failures" for hardware (match to hardware age)
- Documented measurable limits, goals, objectives

- Employee training specific to evaluated element
- Encryption (files systems, communication)
- Incident handling preparation (identify, contain, eradicate, recover, learn, prevent repeats)
- Information systems management practices
- Methods to monitor exposure
- Mitigation follow-up processes
- Monitor volume of activity (Anomaly detection)
- Monitoring and testing
- Network Segmentation
- Password strength and assessment
- Patch management
- Penetration analyses
- Written policies, procedures, and limits including testing of each
- Principal of Least Privilege
- Problem resolution follow-up (short term fix vs. long term solution)
- Procedure to address any new vulnerabilities detected
- Properly configured firewalls
- Risk evaluation prior to new implementations
- Risk management systems (comprehensive, detailed, and developed)
- Separation of duties, "Appropriately segregating duties is a fundamental and essential element of a sound risk management and internal control system." (FRB SR 95-51, p.8)
- Separation of services
- Server Hardening
- Strong authentication programs
- Technical mistakes used as learning experiences and teaching tools
- Vendor pre and post implementation assessment
- Virtual Private Network (VPN)
- Vulnerability assessment tools, guidelines, and practices
- Well-designed and documented system architecture

7. Define the mitigation cost

Identify the cost including actual dollars, time, and resources to implement and maintain the mitigation steps that are not currently in use, matching cost against the risk rating.

Beginning with an educated estimate of the costs is a wise use of time. This could quickly reveal situations where the cost is much greater than the risk. Exact cost may take some research; so working with educated estimates allows the team to continue the evaluation.

8. Prioritize potential mitigation steps.

One mitigation step could reduce the risk in many different processes or applications that were analyzed. Include a ranking that indicates how effective the step could be to the overall business. Risk mitigation that takes little time and resources or mitigation steps that have a good overall impact receive a higher priority. Determine what risk mitigation steps can be reasonably accomplish simultaneously.

Consider confidentiality, integrity, and availability. Without availability, there is no functionality but excellent confidentiality and integrity. Balancing availability with confidentiality and integrity is one of the tricks of Information Security. Perfect confidentiality and integrity can be maintained if information is locked up where no one has access; however, as soon as it becomes available for use there is some level of risk.

The level of residual risk is determined by contrasting the threats with the existing countermeasures.

If the existing countermeasures are effectively protecting the asset from all threats, then residual risk will be low. If, however, the existing countermeasures are not adequate to prevent or withstand an attack, residual risk is higher. Vulnerability is measured in terms of the probability of a loss event occurring.

9. Document the recommended mitigation steps.

No company has unlimited resources so this list should be based on the prioritization performed in step eight.

In addition, develop a method to track the priority, management approval, managements determination of acceptable risk levels, and track the implementation process.

Conclusion:

The process of risk evaluation and mitigation is a balancing act. In the risk assessment process, the business and its goals must be given precedence. Mitigation shouldn't cost more than the value of the asset or the benefit the company will receive from the process.

Management directs the process but every aspect of the business operation needs to be evaluated and included in the evaluation process. The "owners" of the process usually know why they do what they do and the expected results. Those same "owners" will have to abide by the risk mitigation that is implemented; therefore, it is essential to include them in the assessment process so they understand why the change is necessary.

Assigning risk is not a clear mathematical process, it's important to remain objective while evaluating and assigning meaningful risk levels.

This risk assessment should result in a list of processes utilized in operating the business including associated risks, vulnerabilities, systems utilized in the process, information accessed by the process, the business requirement it satisfies, risk mitigation practices or countermeasures, current residual risk, potential additional mitigation steps and their associated cost, and final residual risk. The evaluated process must still satisfy the business requirement with risk mitigation in place.

References:

1. Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security Essentials with CISSP CBK Version 2.1. USA: SANS Press, April 2003.

2. Rode ,Craig. “Mitigating the Complexities of Security Management.” 17 March 2004. URL: http://www.net-security.org/article.php?id=666 (3/21/2004)

3. “SANS Glossary of Terms Used in Security and Intrusion Detection.” SANS InfoSec Reading Room, Getting Started/InfoSec. May 2003. URL: http://www.sans.org/resources/glossary.php (3/21/2004)

4. “Mistakes People Make that Lead to Security Breaches” SANS InfoSec Reading Room, Getting Started/InfoSec. 23 October 2001. URL: http://www.sans.org/resources/mistakes.php (3/21/2004)

5. FDIC. “Financial Institution Letters, FIL 68-99 Risk Assessment Tools and Practices for Information System Security.” 17 July 1999 URL: http://www.fdic.gov/news/news/financial/1999/FIL9968a.HTML (3/21/2004)

6. FDIC: Financial Institution Letters, FIL 131-97, "Security Risks Associated with the Internet." December 18, 1997. URL: http://www.fdic.gov/news/news/financial/1997/fil97131.html (3/21/2004)

7. FFIEC. IT Examination Handbook. “Information Security”. December 2002. URL: http://www.ffiec.gov/ffiecinfobase/booklets/information_secruity/information_security.pdf (11-25-2003)

8. FDIC. “Manual of Examination Policies Section 4-6; ELECTRONIC BANKING.” February 2002. URL: http://www.fdic.gov/regulations/safety/manual/Section4-6.html (3/21/2004)

9. Alberts, Christopher J. Dorofee, Audrey J. “Volume 9: Process 7 – Conduct Risk Analysis” Introduction to the OCTAVESM Method.. June 30, 2001. URL: http://www.cert.org/octave/methodintro.html (3/21/2004)

10. Alberts, Christopher J. Dorofee, Audrey J. “Volume 9: Process 7 – Conduct Risk Analysis” OCTAVE Method Implementation Guide. June 2001. URL: http://www.cert.org/octave/omig.html (3/21/2004)

11. Alberts, Christopher J. Dorofee, Audrey J. “OCTAVESM Criteria, Version 2.0.” December 2001. URL: http://www.cert.org/archive/pdf/01tr016.pdf (3/21/2004)

12. Alberts, Christopher J; Dorofee, Audrey J; Allen, Julia H. “OCTAVESM Catalog of Practices, Version 2.0.” October 2001. URL: http://www.cert.org/archive/pdf/01tr020.pdf (3/21/2004)

13. Bröckers, Alfred. “Process-Based Software Risk Assessment.“ 5 April 1995. URL: http://wwwagse.informatik.uni-kl.de/pubs/repository/broeckers95a/1995-ewspt.pdf (3/21/2004)

14. “Risk Based Assessment.” Maritime Transportation Security Act Information (MTSA). URL: http://www.uscg.mil/d13/units/msopuget/Risk%20Based%20Assessment.pdf (3/21/2004)

15. Nicastro, Felicia M. “Security Patch Management” . URL: http://www.ins.com/downloads/whitepapers/ins_white_paper_security_patch_mgmt_0303.pdf (3/23/2004)

16. Carlson, Tom. “Information Security Management: Understanding ISO 17799. URL: http://www.ins.com/downloads/whitepapers/ins_white_paper_info_security_iso_17799_1101.pdf (3/23/2004)

17. Davis, Adam. “Understanding the Risks of SNMP Vulnerabilities”. URL: http://www.ins.com/downloads/whitepapers/ins_white_paper_risk_of_SNMP_vulnerabilities_0302.pdf (3/23/2004)

18. Dooley, Michael. Drescher, Alex . “IP Address Management Challenges in the Enterprise”. URL: http://www.ins.com/downloads/whitepapers/ins_white_paper_ip_address_mgmt_0104.pdf (3/23/2004)

19. Trofimoff, Michael. “Justifying the Business Value of IT Initiatives Connecting the Dots in a Chaotic World”. URL: http://www.ins.com/downloads/whitepapers/ins_white_paper_justifying_business_value_0703.pdf (3/23/2004)

20. Kapella, Victor. “A Framework for Incident and Problem Management” URL: http://www.ins.com/downloads/whitepapers/ins_white_paper_incident_management_0403.pdf (3/23/2004)

21. Fox, Christopher. Zonneveld, Paul A. ,IT Governance Institute. “IT Control Objectives for Sarbanes-Oxley”. URL: http://www.deloitte.com/dtt/cda/doc/content/IT_Controls_%20Sarbanes-Oxley%281%29.pdf (3/27/2004)

22. FRB- Federal Reserve System Board of Governors. “SR 95-51 (SUP) Rating the Adequacy of Risk Management Processes.“ November 14, 1995. URL: http://www.federalreserve.gov/boarddocs/SRLETTERS/1995/sr9551.htm (3/18/2004)

23. FRB- Federal Reserve System Board of Governors. “SR 98-9 (SUP) Assessment of Information Technology in the Risk-Focused Frameworks .“ April 20, 1998. URL: http://www.federalreserve.gov/boarddocs/SRLETTERS/1998/sr9809.htm (4/3/2004)