GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

An Overview of Practical Risk Assessment Methodologies
(Version 1.0, Dated 29 June 2003, Prepared By Ng Say Wee)

Abstract

This document provides an overview of risk assessment, its benefits and pitfalls, as well as when and how they can go about making use of risk assessment to improve the security of their organisation.

It also describes the following methodologies that are commonly used by security practitioners and consultants for risk assessment: -

a. Asset Audit
b. Pipeline Model
c. Attack Tree

Besides risk assessment methodologies, this document also provides an insight on risk assessment tools – their pros and cons, as well as the evaluation criteria or features to look out while selecting a risk assessment tool.

A working risk assessment template is also given at the end of this document to help the user kick-start their risk assessment.

© SANS Institute 2003, Author retains full rights.

Introduction - What is Risk Assessment?

Security is about managing risks. The moment you connect your computer to the Internet, you are exposing your computer to all kinds of attacks and risks from the Internet. The most secure computer is one that is never switched on and always locked up in a box and buried 200,000 metres under the seabed of the Atlantic Ocean. But this does not work in reality as today's world has become heavily dependent on information technology and communications to process, store and transmit information and deliver services to the people. In order to set up an infrastructure that is operational and secure, not only must one understand the business requirements, he must also know what are the risks and how to best secure them with the assigned budget. This would require a proper information security risk assessment to be conducted.

Risk assessment is about finding out what are the risks, where they are and matters most and how to mitigate the risks identified to an acceptable level for business to go on. It is a rather intensive process. Not only must the assessor find out all the systems, processes and people that are involved, he must also know what are the threats and vulnerabilities that are relevant. Risk assessment looks at all aspects of information security, which includes physical and environmental, administrative and management, as well as technical measures.

In a typical risk assessment, a risk assessment project plan, which identifies what will take place during each stage of the assessment process, the scheduled dates for each activity and the required resources, should be developed.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Types of Risk Assessment

Generally, there are 2 types of risk assessment, namely qualitative and quantitative risk assessment.

In quantitative risk analysis, numeric values (e.g., monetary values) are independently assigned to the different risk assessment components as well as the level of potential losses. When all elements (asset value, threat frequency, safeguard effectiveness, safeguard costs, uncertainty and probability) are quantified, the process is considered to be fully quantitative.

Qualitative risk analysis does not assign numeric values to the risk assessment components. It is scenario-based and the assessors/participants will go through different threat-vulnerability scenarios and try to answer "what if" type of questions. Generally, qualitative risk assessment tends to be more subjective in nature.

The following table shows the pros and cons of qualitative and quantitative risk assessments.

	Pros	**Cons**
Quantitative	The results are based on independently objective processes and metrics; which removes the amount of guesswork required and subjectivity. Great effort is put into asset value determination and risk mitigation. Cost/benefit assessment effort is essential; which may proves to be useful for management's decision making. The results can be expressed in management-specific language (e.g., monetary value, percentages, probabilities).	Calculations can be complex and time-consuming. Historically only works well with a recognized automated tool and associated knowledge base; thus may incur higher costs. Requires large amounts of preliminary work in collecting and quantifying the different risk analysis components. Generally not presented on a personnel level. Participants cannot be coached easily through the process.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	Pros	Cons
Qualitative	Simpler as there are any complex calculations. It is not necessary to determine the monetary value of assets; which can be quite tedious and in certain cases an impossible task as assessor and even system owner find it hard to give a value to intangible items such reputation and customer goodwill. It is not necessary to quantify threat frequency. It is easier to involve non-security and non-technical staff.	It is subjective in nature. Results and quality of the risk assessment depend solely on the expertise and quality of the risk management team. Limited effort to develop monetary value for targeted assets No basis for the cost/benefit analysis of risk mitigation.

Benefits of Risk Assessment - Why Conduct Risk Assessment?

Risk assessment requires the business owner to identify what are its information assets and what are their values to the organisation and its customers or business partners. Importantly, through risk assessment, the business owner will have a better overview and understanding of its risk exposure and whether existing controls are adequate. From the risks identified, the business owners are better informed of the types of risks the organisation is exposed to. This information will definitely be useful in management decision-making as the business owners can now assign the required resources that commensurate with the risk level. For instance, due to resource or time constraint, a decision can be made to resolve all the high risks first before attending to those medium or low risks. Besides helping the business owners to prioritise its resources, it can also provide the necessary guidance for allocating the organisation's budget more effectively and on where it matters most (or hurts most!).

As a result of risk assessment, personnel within the organisation will become more aware of the risks to business operations and avoid bad practices that might be detrimental to the information security of the organisation. Besides raising personnel security awareness, it also provides a common platform for

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

reaching a consensus on which are the greatest risks and the steps needed for risk mitigation. The results of the risk assessment can also serve as an effective means for communicating risk findings and control recommendations to senior management.

Risk assessment pitfalls – What are the problems or obstacles in risk assessment?

A common complaint from the owners of system and infrastructure is that they do not have the time to do risk assessment. Even for those who may have the time, they often lament that they do not know how or where to start. Though there are a lot of guidelines on risk assessment and management, there is yet an industry common standard on risk assessment. Moreover, most of these guidelines have been deemed to be too general and high-level as they do not have enough details on the next-level of details on how-to and the steps needed to conduct a proper risk assessment. The popular and common approach is to outsource to external vendors who have the expertise and experience of conducting proper risk assessment, or at least better equipped with the know-how and in some cases tools for risk assessment. Outsourcing to professional external vendors will most likely be able to meet the need to conduct risk assessment on the organisation's systems and infrastructures, but it will be very costly if there are many systems, infrastructures and services that require risk assessment. More importantly, the owners may become over-dependent on the external vendor to make important business and risk mitigation decisions that could potentially affect the organization.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

When should risk assessment be conducted?

Risk assessment should be part of the organisation's internal processes for quality assurance and project management. As in any good security best practices, risk assessment should be conducted at the start of the system development life cycle during the feasibility study phase to understand the security needs of the system based on the business impact analysis. This risk assessment approach should be continued throughout the entire life cycle to help identify any new security risks and controls that need to be put in place to address those new risks identified. As in any other quality assurance, security should be treated as an important quality that need to be assured to have met the organisation's internal assurance standard or criteria before allowing the systems or services to go into production.

Risk assessment should be conducted whenever there is a need to find out where are the security gaps or risk exposure of the organisation. It should also be conducted when deciding whether the organisation or specific business function needs to implement certain controls. This is usually done based on its business needs for confidentiality, integrity and availability.

It is an industry best practice that an organisation should have internal security policies and standards that mandate certain security requirements, processes and procedures across the entire organisation. If it does not have one, risk assessment can be used to understand its security requirements, which can then be factored into the security policies and standards. Risk assessment can also be used to decide what are the details or information to be logged.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Risk Assessment Methodologies

As the saying goes, there is more than one way to skin a cat. This section looks at different methodologies that can be used for risk assessment. Security practitioners will have to decide the most suitable methodology based on their need and operating environment.

Asset Audit

The asset audit approach towards risk assessment looks at the assets the organisation has and determines if each asset is being protected adequately. Typically, an asset audit process will include the following steps: -

a. Information asset identification – Identifying all the data that the system being assessed stores, processes, transmits or has access to. The data can include program source code, backup tapes and customer information.

b. Data flow – Determines the means by which each information asset identified arrives and leaves the system.

c. Threat analysis – Determines the different threat mechanisms that can be used to acquire the information as the data

   - Enters the system
   - Is stored on the system
   - Leaves the system

d. Likelihood of threat occurrence – determines how likely each threat mechanism identified will happen

e. Impact Analysis – Assess the impact of data being disclosed, corrupted or destroyed or unavailable for a certain period of time

f. Safeguard identification – Selects the relevant safeguards or controls that needs to be implemented to protect the organisation's information assets. These controls can be technical (e.g. install personal firewalls on all remote users' computers) or non-technical (e.g. acceptable use policy or security awareness programs)

The asset audit approach is an easy-to-use and straightforward method for assessing risks by giving the reviewer and owners a direct approach of looking at all the information assets and their risk exposure. The people involved in the asset audit process also obtain a better understanding of how information flows in and out of, as well as, is stored on the system. With this knowledge and insight

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

of the system and the information flow, the reviewer can have a better picture of what and where are at risk and thus needs to be protected

Pipeline Model (A Craftsman-led Approach, By Dr David F. C. Brewer, http://www.gammassl.co.uk/topics/hot3.html)

Yet another risk assessment methodology, which may proves to be useful for seizing up the security of transactional systems [1].

In this approach, risks are assessed on a pipeline, which is the system constituent that is responsible for processing a certain type of transaction. Each pipeline is made up of five components, as follows: -

a. active processes – all the software that make the transaction happens

b. communication processes – responsible for sending/receiving messages (data) over the networks

c. stable data processes – responsible for inserting stable information into the pipeline

d. enquiry processes – responsible for extracting information from the pipeline

e. access control processes – responsible for controlling human access to the pipeline

The security requirements for each pipeline are derived from the security policy of the organisation. Each pipeline is reviewed according to the five components to determine whether the security requirements are met and if not what are the gaps that need to be addressed.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Attack Trees [2]

Attack trees are a variation of fault trees. Attack trees provide a methodical way of describing the security of systems based on who, when, how, why and with what probability an attack will happen. The top of the attack tree or its root node represents the ultimate goal of the attacker and the branches and leaf nodes show the different ways of attaining the goal. The following steps describe how an attack tree can be built: -

a. Identify all the threat agents that might attack the system. These would include dishonest or disgruntled employees, script kiddies, users, administrators, competitors, etc.

b. Explore and consider the ultimate goal or goals of each threat agent. Each goal will then be the root node of each attack tree.

c. Identify all the possible ways in which the threat agent could use to attain the goal; the attack methods then become the second level goals that come under the root node.

d. For each second level goal, consider whether there is the next level of details or ways of attaining the sub-goal. This process is repeated until each of the leaf nodes on the attack tree are a single and specific defined method.

e. Review and evaluate each attack path to determine the likelihood of each method being used to attack the system, assess its business impact if the ultimate goal was attained by the attacker and what countermeasure can be used to stop the attack.

The attack tree method of risk assessment may not be suitable for a novice security reviewer who may not have enough experience and knowledge to have the insight needed to identify all the different attack methods that would be used by different attackers.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Besides the above risk assessment methodologies, which have been used and proven to be effective and practical, there are also other popular risk assessment methods developed and used in the security industry:

a. OCTAVE – Operationally Critical Threat, Asset and Vulnerability Evaluation (http://www.cert.org/octave/methodintro.html)

b. Risk Management Guide for Information Technology Systems, Developed by National Institute of Standards and Technology (NIST), SP 800-30, January 2002.

c. Guide to BS7799 Risk Assessment and Risk Management

NIST had also published a self-help guide for risk assessment - Security Self-Assessment Guide for Information Technology Systems, SP 800-26, November 2001 (http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf). It provides a quick and low-cost method of assessing the security within an organisation through a series of self-assessment questionnaires.

Risk Assessment Tools

Typically, risk assessment is rather manpower-intensive, especially if it involves the entire organisation and all its critical information and information systems. There are many commercially available tools, which attempt to ease the tasks. The criteria given in the following tables can be used to evaluate and select a risk assessment tool that meet the operating need of the organization [9].

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Methodology

Selection or Review Criteria
Is there a description of the underlying methodology?
Is the methodology based on mathematical principles?
Does the methodology support the policy of the organization?
Does the tool examine physical, environmental, procedural, and human interaction with the computer system being analyzed?
What standard is it based on?
Are there any copyright requirements with the standard?
Does the methodology support both qualitative and quantitative results?
What is the formula for calculating risk?
What is the approach to risk calculation? ▪ Asset-based ▪ Scenario based ▪ Modular approach ▪ Systemic approach
Does the tool rank the level of risks?
Does the tool recommend control(s) to mitigate an identified risk?
Does the tool rank the priority of control implementation?
How many threats, vulnerabilities and controls are included in the tool?
How are the lists/databases of threats, vulnerabilities and controls kept up-to-date?

Reporting

Selection or Review Criteria
Are the results of the analysis well presented?
Are the reports comprehensive?
Are the reports useful?
Does the tool rank the results in priority order (e.g., from high to low)?
Does the tool provide advice for safeguard selection?
Does the tool provide iterative safeguard selection?
Does the tool provide cost benefit analysis?

Documentation

Selection or Review Criteria
Is there a manual describing the tool in over-all terms?
Is the documentation thorough?
Is the documentation easy to use and maintain?
Will the documentation be kept up-to-date by the developer?
Does the documentation meet the organization's standards?

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

History and Security Features

Selection or Review Criteria
Does the tool document participants in the analysis?
Does the tool control access to risk analysis data (e.g. logon/password encryption)?
Does the tool provide an audit capability?

Utility and Ease of Use

Selection or Review Criteria
Is the tool user-friendly, eg. Is the User Interface - how intuitive/appealing is the user interface?
Is it easy to interpret the risk results?
Does the tool offer useful options (eg data management routines, on-line help facility, etc.)?
▪ Are there online help functions?
▪ Does it have online instructions on what's next to do?
▪ How easy is it to input information?

Training and Technical Support

Selection or Review Criteria
Is installation support provided?
Is on-site training available?
Is training in usage of the tool provided as part of the installation support?
Will the developer provide future maintenance and ongoing product support?
Does the developer have the personnel and financial resources to provide adequate product support?
Are there any local support?
Does the developer plan further enhancements to the product?
What is the cost for providing future system enhancements?
Will the developer provide modifications to the product if requested?
How frequent is the software update and/or upgrade?
How are the software updates/upgrades sent to the users?
How easy it is to perform the software update/upgrade?

Hardware and Software Requirements

Selection or Review Criteria
Is the minimum hardware configuration compatible with the requirements of the organization?
Can the tool be readily modified to operate on other hardware configurations?
Can the tool be readily modified to operate on other hardware configurations?
Is the operating system the same as that utilized by the user?

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

COST

Selection or Review Criteria
What is the licensing scheme?
How much for purchase of additional licenses?
What services are provided as part of the basic purchase price? ▪ Installation ▪ Licensing ▪ Training ▪ Maintenance ▪ Modifications ▪ Software Updates
Is there a charge for multi-installation usage?

Most of these commercial risk assessment tools, such as XiSec RA tool, Vectra Corporation's Virtual Security Auditor and COBRA's Risk Consultant, are based on qualitative risk assessment approach as compared to Maximus Consulting's Security Risk Control, which attempts to use quantitative approach towards risk assessment.

The software complexity also differs among these tools. Certain tools, such as XiSec RA tool, tend to adopt a more simplistic approach, which requires more human inputs and analysis or judgement. Others like Maximus Consulting's Security Risk Control, tend to be more detailed in their risk assessment approach and thus making the software more complex. Most of these tools can potentially be customised (at a cost) to suit the varied security needs of different organisations. For instance, the tool can take in your organisation's security policies and standards such that the risk assessment can be done and benchmarked against the internal security policies and standards, instead of basing on general security standards or best practices. One common emerging trend among these tools is that they are aligned to ISO 17799 as a baseline for security standard.

Having and using the tools is one thing, but being able to analyse and make sense out of the results produced by the tools is a totally separate thing. These tools are not designed to be foolproof and end-user friendly, as it often requires a lot of technical expertise, human judgement and heavy involvement from different groups across the organisation. A major strength of these tools is that they help to reduce the amount of paper work and manual data collection and collation. The tools will also reduce the amount of guesswork required and lower the chances of inconsistencies among different security practitioners assigned to conduct risk assessment, with their built-in knowledge-base or databases of threats, vulnerabilities, risk levels and controls.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Sample Risk Assessment Template

The sample risk assessment template provided in Annex A is intended to be a working template for conducting risk assessment. The template can be used in the following few steps: -

a. Information asset identification and classification – All the information assets that fall under the scope of the risk assessment are identified as the first step. The owners of these information assets will need to assign the appropriate security classification for each information asset that commensurate with its value to the organisation. The effort taken to classify the information assets will prove to be worthwhile during the business impact analysis phase.

b. Threat Assessment – The threats on each information asset and the likelihood of their occurrence are identified and determined during this phase.

c. Business Impact Analysis – Through a series of questions, the reviewer will assess the possible impact to business, based on the business need for Confidentiality, Integrity and Availability.

d. Risk Determination – Using NIST's risk determination matrix, the risk exposure of each information asset is calculated by considering both the likelihood of threat occurrence and business impact.

Of course, the actual risk assessment does not end here. With the identification of the risks and their level of severity, the owners of the information asset have to decide how they would like to manage the risks to a level that is acceptable. They can choose to mitigate the risks by implementing the appropriate controls; transfer the risks, e.g. to an insurance company, or accept the risks, e.g. if the risk is within their risk threshold or in the absence reasonable risk mitigation measures.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Conclusions

Despite its problems and pitfalls, risk assessment is a very important component of the organisation's overall approach and strategy towards security management. It should be built into the organisation's internal processes for system development life cycle as well as quality assurance to ensure that adequate security has been designed and implemented cost-effectively in places where it matters most. Though risk assessment requires skills, time and strong management support, at the end of the day it might really be worthwhile as the effort put in helps to save the day for the individuals who are responsible for security and the continuing survival of the organisation.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

[1] A Craftsman-led Approach, By Dr David F. C. Brewer (http://www.gammassl.co.uk/topics/hot3.html)

[2] Modeling security threats, Bruce Schneier, Dr Dobb's Journal, December 1999 (http://www.counterpane.com/attacktrees-ddj-ft.html)

[3] Information Security Risk Assessment – Practices of leading organization, United States General Accounting Office, November 1999. (http://www.gao.gov/special.pubs/ai00033.pdf)

[4] Threat and Risk Assessment Working Guide (ITSG-04) , Communications Security Establishment, Government of Canada, January 1996. (http://www.cse-cst.gc.ca/en/services/publications/itsg/ITSG-04.html)

[5] A Guide to Security Risk Management for Information Technology Systems (MG-2) , Communications Security Establishment, Government of Canada, 1996. (http://www.cse-cst.gc.ca/en/services/publications/itsg/MG-2.html)

[6] A Guide to Risk Assessment and Safeguard Selection for Information Technology Systems (MG-3), Communications Security Establishment, Government of Canada, January 1996. (http://www.cse-cst.gc.ca/en/services/publications/itsg/MG-3.html)

[7] Security Self-Assessment Guide for Information Technology Systems, SP 800-26, National Institute of Standards and Technology, November 2001 (http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf)

[8] Risk Management Guide for Information Technology Systems, Special Publication 800-30, National Institute of Standards and Technology, January 2002. (http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf)

[9] Guide for Selecting Automated Risk Analysis Tools, National Institute of Standards and Technology, October 1989. (http://csrc.nist.gov/publications/nistpubs/500-174/sp174.txt)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Annex A - Sample Risk Assessment Template

Name of IT System _____

Name of System Owner _____

Brief Description of the System _____

Date of Implementation _____
(DD/MM/YYYY)

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

1 INFORMATION ASSET IDENTIFICATION AND CLASSIFICATION

List all the information stored in, processed and transmitted by the system. Classify the information (Top Secret - TS, Secret - S, Confidential - C, Restricted - R, Public - P).

Details of Information (Stored, Processed or Transmitted by the system)	Information Classification (TS, S, C, R, P)

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2 THREAT ASSESSMENT

1. For each of the identified information asset, what are the means by which the information arrives and leaves the system?

2. Where is the information stored? How is it stored?

3. What are the threats or mechanisms that can be employed by an attacker to acquire the information as it
   - enters the system,
   - is stored on the system and
   - leaves the system?

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

4. What is the likelihood of the threat occurring? This may include a description of existing controls (technical, management, operational).

Threat Assessment Table

Details of Information (Stored, Processed or Transmitted by the system)	Description of where the information is stored, how it is stored, arrives and leaves the system.	Description of the threats or mechanisms that can be employed by an attacker to acquire the information as it - enters the system, - is stored on the system and - leaves the system.	Likelihood of Threat Occurrence (High – H, Medium – M, Low – L)

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3 BUSINESS IMPACT ANALYSIS

The following self-assessment questionnaires will help in determining the security need for data confidentiality, integrity and availability. Grade the information security need in terms of their confidentiality, integrity and availability (High, Medium, Low).

Data Confidentiality Need Determination

		Need for Data Confidentiality (H, M, L)
1 Confidentiality of Information		
How would you classify the level of confidentiality of data handled in the system?	[ ] Unclassified [ ] Restricted [ ] Confidential [ ] Secret	
2 Consequence of Unauthorised Disclosure		
What is the consequence to the organisation if data are disclosed to unauthorised party?	[ ] None at all [ ] Some negative impact, but manageable [ ] Significant negative impact, with grave consequences	

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Data Integrity Need Determination

		Need for Data Integrity (H, M, L)
1	**Consequence of Unauthorised Modification** What is the consequence to the organisation in the following situations:	
(a)	Unauthorised data modification occur during data transmission or at storage in the system	[ ] None at all [ ] Some negative impact, but manageable [ ] Significant negative impact, with grave consequences
(b)	Unauthorised deletion of data from the system	[ ] None at all [ ] Some negative impact, but manageable [ ] Significant negative impact, with grave consequences
(c)	Unauthorised data are added to the system	[ ] None at all [ ] Some negative impact, but manageable [ ] Significant negative impact, with grave consequences

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Data Availability Need Determination

		Need for Data Availability (H, M, L)
1	**Maximum Tolerable Downtime**	
	In the event of a total disruption of the services and information provided by the application system, how long can operations affected be sustained via manual or other means?	[ ] About 1 month [ ] About 1 week [ ] Between 1 to 3 days
2	**Estimated Dollar Loss**	
	What is the estimated financial loss for the period of tolerable downtime in the event of total system failure?	[ ] Less than $30,000 [ ] Less than $1,000,000 [ ] $1,000,000 and above
3	**Public Impact**	
	What is the severity of the impact on the public in the event of total system failure?	[ ] None at all [ ] Some negative impact, but manageable [ ] Significant negative impact, with grave consequences

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

4 Consequence of Unavailability

What is the consequence to the organisation in the event of a system failure or the data cannot be accessed?	[ ] None at all [ ] Some negative impact, but manageable [ ] Significant negative impact, with grave consequences

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Impact Analysis Table

Details of Information (Stored, Processed or Transmitted by the system)	Information Classification (TS, S, C, R, P)	Business Impact due to Loss of Data Confidentiality (H, M, L)	Business Impact due to Loss of Data Integrity (H, M, L)	Business Impact due to Loss of Data Availability (H, M, L)	Overall Business Impact (H, M, L)

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

4 RISK DETERMINATION

Use the following risk-level matrix[1] for risk determination: -

Threat Likelihood	**Impact**		
	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*

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)

[1] Risk Management Guide for Information Technology Systems, Special Publication 800-30, National Institute of Standards and Technology.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Details of Information (Stored, Processed or Transmitted by the system)	Likelihood of Threat Occurrence (High – H, Medium – M, Low – L)	Overall Business Impact (H, M, L)	Risk Level (H, M, L)

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Project Leader:	User Owner:
Name:	Name:
_____	_____
Designation:	Designation:
_____	_____
Signature & Date:	Signature & Date:
_____	_____

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Threat Examples [2]

Physical and Environmental Threats

- bomb attack
- earthquake
- environmental contamination
- fire
- flooding
- hurricane
- lightning
- airborne particles/dust
- air-conditioning failure
- failure of power supply
- power fluctuation

Equipment and Software Threats

- malicious software (e.g. viruses, worms and Trojan horses)
- hardware failure
- misrouting or rerouting of messages
- software failure
- traffic overloading
- transmission errors
- failure of communication services

Human and Personnel Threats

- theft

[2] Annex A Example Lists of Threats and Vulnerabilities, Guide to Risk Assessment and Risk Management

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- willful damage
- network access by unauthorised persons
- user error
- maintenance error
- masquerading of user identity
- misuse of resources
- operational support staff error
- traffic overloading
- use of software by unauthorised users
- use of software in an unauthorised way
- use of network facilities in an unauthorised way
- unauthorised/illegal use of software
- unauthorised/illegal import and export of software
- staff shortage
- eavesdropping

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.