SECURITY RISK ANALYSIS AND MANAGEMENT

<A white paper by: B. D. Jenkins, Countermeasures, Inc.>

Risk Analysis helps establish a good security posture; Risk Management keeps it that way.

Security measures cannot assure 100% protection against all threats. Therefore, risk analysis, which is the process of evaluating system vulnerabilities and the threats facing it, is an essential part of any risk management program. The analysis process identifies the probable consequences or risks associated with the vulnerabilities and provides the basis for establishing a cost-effective security program. Risk management is the process of implementing and maintaining countermeasures that reduce the effects of risk to an acceptable level.

The risk analysis process gives management the information it needs to make educated judgments concerning information security. The procedure identifies the existing security controls, calculates vulnerabilities, and evaluates the effect of threats on each area of vulnerability.

In most cases, the risk analysis procedure attempts to strike an economic balance between the impact of risks and the cost of security solutions intended to manage them. At the basis of selecting cost-effective protective measures is the assumption that the cost of controlling any risk should not exceed the maximum loss associated with the risk. For example, if the potential loss attributable to a risk is estimated to be $100,000, the cost of the protective measures intended to prevent that loss should not exceed that amount. In other cases, however, the decision to implement (or not implement) countermeasures may be driven by the importance of the system or its data or by mandates as opposed to its cost.

In either case, the sum of averted risks must be considered where a single remedy will reduce several risks. The analyst must also consider the use and interaction of multiple remedies. One remedy may improve or negate the effectiveness of another.

These considerations form the basis for determining which protective measures are the most appropriate. After having evaluated the loss of each risk, assessments can be made about the funds that can be allocated to lessen the estimated annual losses to an acceptable level. With information on loss before and after the application of controls, cost evaluations will indicate which countermeasures are most cost-effective. When identifying the protective measures that should be implemented, consideration should be given to the greatest risks first. The risk analysis methodology selected (including the quantitative cost analysis methods) will likely suggest the use of cost indicators or common denominators that function to identify the most cost-effective security solutions. The following cost indicators provide a basis for comparison among protective measures:

- The payback period necessary to recover the costs attributable to a protective measure

- The expected annual cost avoidance (the reduction in potential loss) attributable to a protective measure (the amount of cost avoidance realized after the countermeasure is installed and has achieved payback)

- The amount of expected loss reduction provided the counter-measure is implemented

Security policy requires the creation of an ongoing information management planning process that includes planning for the security of each organization's information assets.

Risk management is an ongoing, proactive program for establishing and maintaining an acceptable information system security posture.

Once an acceptable security posture is attained [accreditation or certification], the risk management program monitors it through every day activities and follow-on security risk analyses. In many cases, the rules, regulations, or policies that govern the information security program will stipulate when a follow-on risk analysis must be done.

The risk management steps include:

- Assign and track corrective actions, as necessary, to reduce residual risk to an acceptable level.
- Continuously monitor the security posture

A security risk analysis is a procedure for estimating the risk to computer related **assets** and loss because of manifested **threats**. The procedure first determines an asset's level of **vulnerability** by identifying and evaluating the effect of in-place **countermeasures**. *An asset's level of vulnerability to the threat population is determined solely by countermeasures [controls/safeguards] that are in-place at the time the risk analysis is done.*
Next, detailed information about the asset is used to determine the significance of the asset's vulnerabilities. This includes how the asset is (or will be) used, data sensitivity levels, mission criticality, inter-connectivity, etc. Finally, the negative impact [**expected loss**] to the asset is estimated by examining various combinations of threats and vulnerability areas.

The highlighted words in the above paragraphs point out the more important terms associated with security risk analysis. That is, assets, threats, vulnerability, counter-measures, and expected loss. *If you understand how these various "things" relate to each other you will understand the rationale behind a security risk analysis.*

How do we know what our potential losses will be if we do not do an analysis? Should we spend the time and money to implement one or more countermeasures if manifested threats are unlikely? Is the status quo acceptable?

A *security risk analysis* defines the current environment and makes recommended corrective actions if the residual risk is unacceptable. Risk analysis is a vital part of any ongoing security and risk management program. The risk analysis process should be conducted with sufficient regularity to ensure that each agency's approach to risk management is a realistic response to the current risks associated with its information assets. Management must then decide on whether to accept the residual risk or to implement the recommended actions.

Believe it or not, YOU do one or more risk analyses every day of your life! Every time you cross the street or pull out onto the highway you do an analysis of the threats, vulnerabilities, and in-place countermeasures, and decide if the risk of asset loss is acceptable. If it is, you proceed. If not, you may put one or more additional countermeasures in-place and analyze the risk again.

In order to discuss security risk analysis concepts we must first establish a baseline of the related terms. Then, we must define how the terms relate to each other and how they are used to analyze risk.

Risk Analysis Terminology

Asset - Anything with value and in need of protection.

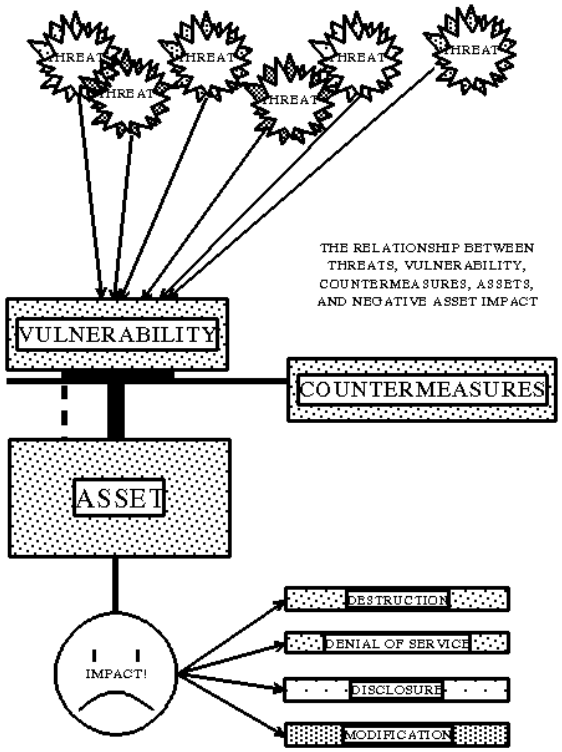
Threat - An action or potential action with the propensity to cause damage.

Vulnerability - A condition of weakness. *If there were no vulnerabilities, there would be no concern for threat activity.*

Countermeasure - Any device or action with the ability to reduce vulnerability.

Expected Loss - The anticipated negative impact to assets due to threat manifestation.

Impact - Losses as a result of threat activity are normally expressed in one or more impact areas. Four areas are commonly used; Destruction, Denial of Service, Disclosure, and Modification.



How "Things" Work Together

A security risk analysis is an examination of the interrelationships between assets, threats, vulnerabilities, and countermeasures to determine the **current** level of risk. The level of risk that remains after consideration of all in-place countermeasures, vulnerability levels, and related threats is called **residual risk.** Ultimately, it is the residual risk that must be accepted [as is] or reduced to a point where it can be accepted.

The relationship between the elements of a risk analysis is illustrated in the graph at left. Any given threat in the population of threats is poised to take advantage of system vulnerabilities, countermeasures

reduce the level of vulnerability, the asset is what needs to be protected, and the impacts are the result of threat activity through residual risk.

Doing The Analysis

Although the same "things" are involved in a security risk analysis, many variations in the procedure for determining residual risk are possible. Likewise, the metric for expressing residual risk can vary from good/bad or high/low to a statement that a certain amount of money will be lost. But, in the end, any security risk analysis should indicate (1) the current level of risk, (2) the likely consequences, and (3) what to do about it if the residual risk is too high.

What risk analysis methodology is best? Which one will produce the desired results with the least cost and time? Should the procedure be qualitative?, quantitative? automated? manual?, or some combination of these?

All risk analysis methodologies enable system users to compare possible losses to their agency with the cost of countermeasures (a.k.a. safeguards or controls) designed to protect against those losses.

To be useful, a risk analysis methodology should produce a quantitative statement of the impact of a risk or the effect of specific security problems. The three key elements in risk analysis are; (1) A statement of impact or the cost of a specific difficulty if it happens, (2) A measure of the effectiveness of in-place countermeasures, and (3) A series of recommendations to correct or minimize identified problems.

How many people will be needed? For how long? How much experience must they have, what type, and what impact will their experience [or lack thereof] have? Will the results suffer from inaccuracies, inconsistencies in the information obtained? What are the advantages of automation?

Planning for information security and risk management begins with identifying the information assets, data sensitivity, values, in-place countermeasures, applicable threats and their frequency of occurrence, system (project) configuration. This information is later used to calculate vulnerabilities and risks. The computer or network risk assessment process consists of nine separate, but interrelated steps. The following paragraphs provide a description of what's involved in these 9 steps.

Identify and Valuate Assets

The first step for all risk assessments is to identify and assign a value to the assets in need of protection. The value of assets is a significant factor in the decision to make operational tradeoffs to increase asset protection. The essential point is to list all things that could be affected by a security problem. These include: *hardware, software, data, people, documentation, and supplies.*

An assets' value is based on its cost, sensitivity, mission criticality, or a combination of these. When the value is based on something other than cost, it is usually converted to money using a standard equivalency table. The asset value will be used later in the assessment process to determine the magnitude of loss when threats occur.

Identify Applicable Threats

After identifying the assets that require protection, the threats to those assets must be identified and examined to determine for loss. This step involves the identification and description of threats in the threat population that seem appropriate for the system or network being assessed, and estimating how often they are likely to occur. These include: *unauthorized access, disclosure of information, denial of service, access points, misconfigured systems, software bugs, insider threats, as a minimum.*

Threat Definition

A threat is a potential force that could degrade the confidentiality (compromise), accuracy (integrity), or avail-ability (denial of service) of the system or network. Threats can be human (intentional or unintentional) or environmental (natural or fabricated). Two axioms apply for threats:

Axiom 1: The same population of threats exist for all systems and networks.
Postulation: The population of threats is infinite in number and variety. Any given threat in the population will occur at an undetermined and uncontrolled frequency. Only the likelihood of threat occurrence varies between systems and locations. For example, the threat of an earthquake exists for both a system located inside Cheyenne Mountain, Colorado and one located in Oakland, California, but the likelihood of an earthquake occurrence varies greatly.

Axiom 2: The frequency of occurrence of a threat cannot be altered.
Postulation: Apparent alteration to the frequency of occurrence of a threat is, in reality, altering the *impact* of threat occurrence through countermeasures. Countermeasures reduce the level of vulnerability to the manifested threat, not how often the threat occurs. To say that countermeasure implementation alters threat frequency is to say that using an umbrella will alter how often it rains.

Applicable Threats

Determining which threats apply is an involved process that entails research of historical records, mathematical formulas, and empirical conclusions. In the end, however, both if and when a threat will occur is always an educated guess.

Threat identification, usually on a form, includes a title, a brief definition, and written rational for the inclusion of the threat in the assessment process. A written justification for the estimated frequency of occurrence must also be provided.

Identify/ Describe Vulnerabilities

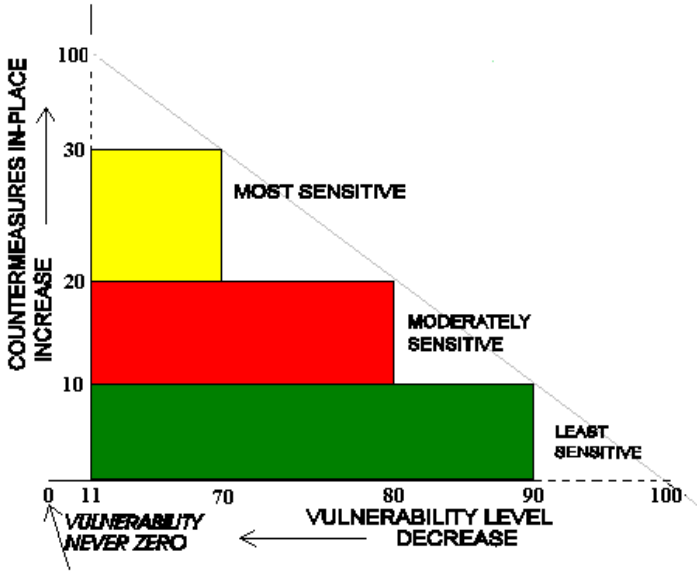
The level of risk is determined by analyzing the interrelationship of threats and vulnerabilities. A risk exists when a threat has a corresponding vulnerability, but even high vulnerability areas are of no consequence if no threats occur.

Vulnerability Definition

A vulnerability is a condition of weakness. A condition of weakness creates an opportunity for exploitation by one or more threats. The following axiom applies for vulnerabilities:

Axiom 3: The level of vulnerability decreases as countermeasures increase.
Postulation: The level of vulnerability to threats is reduced by the implementation of countermeasures. Some countermeasures have a greater propensity to offset vulnerability than others. The level of vulnerability and the relative value of each counter-measure said to reduce it can be expressed numerically.

Axiom 3 is illustrated in the following graph:



Pair Threats and Vulnerabilities

A threat is any action with the potential to cause a negative impact. If there were no threats to computer systems, there would be no need to be concerned about computer system vulnerabilities. By linking or pairing threats with vulnerabilities the potential for threat occurrence evaluation is tailored to any particular environment.

Determine the Impact of Threat Occurrence

When the exploitation of a vulnerability occurs, the asset suffers an impact (loss). The losses are categorized in impact areas titled Disclosure, Modification, Destruction, and Denial of Service.

Disclosure

This is a confidentiality issue. Greater emphasis is placed on this impact area when sensitive or classified information is being processed.

Modification

When an asset is changed from its original state by the effect of threat manifestation it is called Modification. This is of special concern when a threat might modify the content of a database, say, in a computer aboard one of NASA's Shuttles.

Destruction

In this case the asset is damaged beyond practical use by threat activity. Emphasis is placed on this impact area when the complete loss of an asset is a more important concern than its modification or temporary non-availability.

Denial of Service

This impact is emphasized when threats are more likely to cause a temporary loss of capability than total destruction of modification.

By emphasizing one or more impact areas in the evaluation process, management can focus their resources on reducing the impact in the area that concerns them most.

In-Place Countermeasures

Credit must be given for **all** in-place countermeasures. Identifying in-place countermeasures is part of the up front data gathering process in any risk analysis process. Countermeasures can be categorized as *Technical* or *Administrative* with sub categories of each type as follows:

Preventive
This type countermeasure is designed to prevent damage or impact from an action or event from occurring.

Detective
These countermeasures provide some type of notification that something has gone wrong.

Corrective
Some countermeasures have the ability to correct identified problems, such as the loss of a bit in a word.

Countermeasure Definition

Countermeasures are the protection measures that reduce the level of vulnerability to threats. For recommendation purposes, they come in two flavors; required and discretionary. Both types of in-place countermeasures are identified as part of the initial data gathering activity. The following axiom applies to countermeasures:

Axiom 4: All countermeasures have inherent vulnerabilities.

Postulation: A vulnerability level of ZERO can never be obtained since all countermeasures have vulnerabilities themselves. For this reason, vulnerability can never be zero, and thus risk can never be totally eliminated.

Required Countermeasures

All countermeasures in this category can be traced to one or more written rules or regulations. The sensitivity of data being stored and/or processed on a system or network, and its mode of operation, determine which regulations apply. This, in turn, determines the required countermeasures.

Discretionary Countermeasures

This type of countermeasure is elective in nature. In many cases the required countermeasures will not reduce the level of vulnerability to a level acceptable to the Designated Accreditation Authority (DAA). In such cases, managers may choose to implement this type of countermeasure to adjust the level of vulnerability to an acceptable level.

Determine Residual Risks (Conclusions)

Residual risk refers to the level of risk that remains after giving credit for the in-place countermeasures. Based on the nature of countermeasures, as defined in Axiom 4 above, there will always be residual risk. The issue becomes one of determining whether or not the residual risk acceptable.

The residual risk takes the form of conclusions reached from the assessment process. The conclusions must identify:

(1) Areas which have a high vulnerability coupled with a likelihood of threat occurrence, and

(2) All required countermeasures that are not in-place.

The results of these steps provide the input needed to begin the selection of additional countermeasures.

Identify Additional Countermeasures (Recommendations)

Once the residual risk has been determined the next step is to identify the most effective and least costly way to reduce risk to an acceptable level. *An operational trade-off must be made any time additional countermeasures are implemented.*

Tradeoffs can take the form of cost, convenience, time, or a mix of these. The following axiom applies to reducing risk:

Axiom #5: An acceptable level of vulnerability can be obtained through the implementation of countermeasures.
Postulation: There exists a mix of countermeasures that can achieve any arbitrary level of vulnerability. By adding countermeasures, the vulnerability level can be adjusted to

a level commensurate with the sensitivity level of the information being processed or importance of the Project.

For discretionary countermeasures, this step also includes an assessment of the value of one countermeasure over others. This usually takes the form of a Return on Investment (ROI) calculation but may also be based on which is quickest and easiest to implement.

Required Countermeasure Recommendation

Required or mandated countermeasures that are not in-place are the first recommendation.

Discretionary Countermeasure Recommendation

The second recommendation usually identifies the discretionary countermeasures needed to further reduce the risk level.

Prepare a Risk Analysis Report

The risk analysis process helps to identify the information assets at risk and attach a value to the risks. Additionally, it identifies protective measures that minimize the effects of risk and assigns a cost to each countermeasure. The risk analysis process also determines whether the countermeasures are effective. After the analysis is complete, a report documenting the risk assessment must be prepared.

The biggest challenge in writing a security risk analysis report is to bridge the gap between risk analysis jargon and information management can understand and use for decision making. As a rule, management will focus on summary information and only use technical details if they are needed to support a decision or make a choice between recommendations.

The risk analysis report serves as the vehicle for presenting to management the findings of the risk analysis process and recommendations for information security. It provides company or agency management with the information needed to make intelligent and well-informed decisions related to security issues. The report should be forwarded to the agency or company head for prompt review, approval, and action.

The report should include only summary information. The working papers and detailed analyses that support the findings and Recommendations outlined in the report should

be maintained for reference purposes and as a resource for future risk analyses. The report and its related documentation should be considered sensitive information and be protected accordingly. They are not intended for general distribution. An acceptable risk analysis report outline is provided as Attachment (1).

The amount of effort involved with each of the above steps will vary greatly based on the size and complexity of the "Project" being analyzed. The first step is often critical in that the **scope** of the Project needs to be accurately defined. In other words, where does the Project start and end?; what components (individual computer systems, networks, etc.) are included in the definition of the "Project?"

The report's technical details should include, as a minimum:

- Vulnerability levels
- Applicable threats and their frequency
- The use environment
- System connectivity
- Data sensitivity level(s)
- Residual risk, expressed on an individual vulnerability basis
- Detailed Annual Loss Expectancy calculations

So, which methodology for security risk analysis is best; qualitative?, quantitative?, or hybrid? Should the process be manual or automated? The most basic function of any security risk analysis process is to determine, as accurately as possible, the risk to assets. Of course, the procedure for determining the risk can be complex or simple, depending on the asset and on the analysis methodology used. The amount of risk can be expressed as good/bad; high/low (qualitative), as a calculated metric (quantitative), or a combination of the two (hybrid).

The process of data collection, analysis, and preparing a security risk analysis report involves many steps. It is time consuming, expensive, and more often than not, a collateral duty for the person(s) charged with getting it done. Moreover, the requirement to do a security risk analysis is cyclic in nature, e.g., initially, then once every one to three years.

There is little doubt that an automated risk analysis methodology is less demanding on the user in terms of time and experience. The concepts and implementation of most commercial automated methodologies contain the expertise and have undergone the scrutiny of both government and commercial users.

In contrast, manual methods are often less formal and require the user to interpret and execute numerous, and sometimes complicated, steps. This increases the likelihood of error or omission and makes repeatable results difficult to obtain.

After establishing what is to be protected and assessing the risks these assets face, it is necessary to decide how to implement the controls that protect these assets. The controls and protection mechanisms should be selected to adequately counter the vulnerabilities found during risk assessment and to implement those controls cost effectively.

The controls that are selected represent the physical embodiment of the security policy. Because these controls are the first and primary line of defense in the protection of assets, they must be selected wisely. If the major threat to the system is outside penetrations, implementation of biometric devices to authenticate regular system users would be unnecessary. On the other hand, if the major threat is unauthorized use of computing resources by regular system users, rigorous automated accounting procedures should be established. Another method of protecting assets is to use multiple strategies. In this way, if one strategy fails or is circumvented, another strategy comes into play to continue protecting the asset. Using several simpler strategies can often be more effective than one very sophisticated method. For example, dial-back modems can be used in conjunction with traditional logon mechanisms. Many similar approaches can be devised to provide several levels of protection for assets. However, those planning security strategies must keep in mind exactly what needs to be protected and cautiously avoid unneeded mechanisms and methods.

Some Significant Countermeasures

If the system itself is not physically secure, nothing else about the system can be considered secure. With physical access to a machine, an intruder can halt the machine, bring it back up in privileged mode, replace or alter the disk, plant Trojan Horse programs, or take any number of other undesirable actions.

Critical communications links, important servers, and other key machines should be located in physically secure areas. Some security systems, require that the machine be physically secure. Care should be taken about who has access to the machines that seem or are intended to be physically secure. Custodial and maintenance staff often have room keys. If machines cannot be physically secured, care should be taken about trusting those machines. Sites should consider limiting access from nonsecure

machines to more secure machines. Allowing trusted access from these kinds of hosts is particularly risky.

Several simple procedures can be used to detect most unauthorized uses of a computer system. These procedures use tools provided with the operating system by the vendor or tools publicly available from other sources.

System monitoring can be done either by a security analyst or by software written for the purpose. Monitoring a system involves looking at several parts of the system and searching for anything unusual. Monitoring system use must be done on a regular basis. Picking one day out of the month to monitor the system is not recommended because a security breach can be isolated to a matter of hours. Only by maintaining a constant vigil can security violations be detected in time for prompt reaction.

Risk analysis aids in developing a security strategy and provides the basis for establishing a cost-effective security program that minimizes the effects of risk. Preparation of the risk analysis report marks the completion of the risk analysis process or cycle. After the report is forwarded to the program manager and approved, the planning process necessary to establish the technical and procedural protective security measures identified in the report should begin. The successful implementation of a security program depends on management involvement. This involvement includes planning for the security of information assets. The planning process identifies needs, establishes priorities, implements objectives, obtains resources, and secures commitment to the security plan, which includes a contingency plan for information resources services resumption.

An implementation plan and a schedule for instituting the proposed protective security measures must be developed. Additionally, ways to implement the objectives must be identified. The plan should assign security responsibilities to management; to information security function personnel; and to the owners, users, and custodians of information. The success of the security program depends on the proper assignment of security responsibilities.

The risk analysis process should be conducted with sufficient regularity to ensure that the approach to risk management is a realistic response to the current risks associated with its information assets. Consequently, the security plan may require reassessment and interim updates should significant changes in security issues occur.

All information resources determined by management to be essential to the critical mission and functions, and whose loss would have an unacceptable impact, should have

a written contingency plan that will provide for the prompt and effective continuation of critical functions in the event of a disaster. The contingency plan should be tested and updated at least annually to ensure that it is valid and current.

The owners of information play a major role in the development and implementation of the contingency plan. For example, the owners of information, in cooperation with the custodians, should address the following issues in the contingency plan:

a) Critical applications, technical support services, and assignment of priorities to jobs.
b) Data files and programs that should be backed up and stored off site
c) Assurances that the backup schedule is adequate
d) Assurances that all required documentation stored off site is current and complete, including data, programs, user documentation, and paper supply
e) Arrangements for processing at an alternate location if the primary site is rendered inoperable
f) Detailed plans for transition to the alternate processing site and for later resumption of normal processing

Contingency planning includes procedures and actions to recover from losses ranging from minor temporary outages to comprehensive disaster recovery planning in preparation for catastrophic losses of information resources. Onsite backup is employed to have readily available current data in machine-readable form in the production area in the event operating data are lost, damaged, or corrupted, without having to resort to reentry from source material. Offsite backup or storage embodies the same principle but is designed for longer-term protection in a more sterile environment, requires less frequent updating, and provides additional protection against threats potentially damaging to the primary site and data.

Data and software essential to the continued operation of critical agency functions should be backed up. The security controls over the backup resources should be as stringent as the protection required of the primary resources.

B. D. Jenkins is the designer and developer of the widely accepted BUDDY SYSTEM Automated Risk Analysis and Management software. He has made several significant contributions to the information security knowledge base over 18 years as a security practitioner. He can be contacted at 1-800-242-8339 or email to bjenkins@buddysystem.net.

Attachment (1) Example Format

The following is an example security risk analysis report format:

Cover sheet with report title, date, and preparer's ID
Table of Contents
Executive Summary

1. *Introduction*
    - *1.1 Purpose*
    - *1.2 Scope*
    - *1.3 Background*

2. *System Description*
    - *2.1 Overview*
    - *2.2 Hardware*
    - *2.3 Software*
    - *2.4 Communications/Network environment*
    - *2.5 Sensitivity*
    - *2.6 Criticality*

3. *Methodology Used*
    - *3.1 Data collection*
    - *3.2 Data analysis*
    - *3.3 Reporting and risk management*

4. *Conclusions*
    - *4.1 High vulnerability areas*
    - *4.2 Significant threats*
    - *4.3 Measure of compliance (required countermeasure's)*
    - *4.4 Most significant vulnerability(ies) due to paired threats*

5. *Recommendations*
    - *5.1 Rationale*
    - *5.2 Required countermeasures (relate to documents)*
    - *5.3 Discretionary countermeasures*
    - *5.3.1 Cost benefit analysis*
    - *5.4 Prioritization*

Appendices as necessary to support the report with technical information
Graphic representations where practical and beneficial to the reader.