

White Paper

Information Security Risk Management Dynamics

Disclaimer

This is one of a series of articles detailing information security procedures as followed by the INFOSEC group of Computer Technology Associates, Incorporated, also known as CTA. These articles are copyright by Computer Technology Associates and may not be reproduced or used for profit without the expressed written permission of CTA or as included in contractual arrangements with clients of CTA.

For further details as to the process and the procedures followed, contact:

Computer Technology Associates, Inc.
INFOSEC Group
7150 Campus Drive, Suite 100
Colorado Springs, CO 80920
(719) 590-5100

Introduction

Purpose

The purpose of this document is to:

Establish an understanding of security terminology used in information security and risk management.

Describe a dynamic information security risk management model which can be used to create an acceptable balance between risk of loss and investment in security

Provide a set of key issues that must be addressed to enhance visibility of the existing security posture of an enterprise and to reduce and maintain risk at an acceptable level.

Scope

This document is intended for all personnel responsible for information security such as system owners, program managers, system developers, programmers, planners, technical engineers, or maintainers.

Background

For many companies information security and managing the risks associated with information and automated systems have always been concerns. Their response to these concerns has been evidenced in the way their systems are designed, configured, and operated.

However, changes in the business environment brought on by a rapid growth in technology puts many companies in a position where the presence of information security is now a key capability discriminator of the company and a highly desired assurance their customers want.

Global business competition within many customer bases, and threats from "others" who would like to see you fail, mandate more security consciousness within the business environment.

This being the case, a standardized process for documenting and managing information security risks across your enterprise is now needed to replace an undocumented process once performed on an informal basis to various degrees of rigor.

Information Security and Risk Management Terms

Information security and risk management have their own set of unique terms. The following terms are repeated many times throughout this document. Historically, the Government has driven the commercial interest for security. Rather than reinventing the wheel, we chose established Government definitions as the basis for a standard set of terms in the commercial arena. Many of the definitions are taken directly from the National Computer Security Center (NCSC) Technical Guide (TG)-004, *Glossary of Computer Security Terms*, the Department of Defense Directive 5200.28, *Security Requirements for Automated Information Systems*, or derived from Federal sources.

System

For the purpose of this document, the term "system" will consist of two mutually dependent components; the platform and the environment. The system's platform will consist of hardware, software, and firmware products used to input, process, store, and communicate information. The system's environment will consist of physical, procedural, and administrative aspects in which the platform operates. Both components will be viewed in their combined context - a "system".

Information Security

The degree to which measures and controls safeguard or protect an automated information system (AIS) against unauthorized (accidental or intentional) disclosure, modification, destruction of AIS and/or data, and denial of service. Security controls include consideration of all hardware and/or software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the AIS and for the data contained in the AIS. It includes the totality of security safeguards designed to achieve an acceptable level of protection, from safeguards designed to: a) protect system assets from unauthorized access; b) mechanisms which detect attacks and finally, c) reaction mechanisms designed to prevent asset loss in the event of successful penetration. (Department of Defense Directive 5200.28)

Confidentiality

The concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations. (NCSC-TG-004)

Integrity

The state that exists when data is unchanged from its source and has not been modified, altered, disclosed, or destroyed either accidentally or maliciously. (Department of Defense Directive 5200.28)

Availability

The state when data [or systems] are in the place needed by the user, at the time the user needs them, and in the form needed by the user. (NCSC-TG-004)

Accountability

Property that allows auditing of activities on an AIS to be traced to persons who may then be held responsible for their actions.

Threat

Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service. (NCSC-TG-004)

Two aspects of threats are their **likelihood** (the probability of the circumstance or event happening) and their **impact** (what happens if it does).

Controls / Safeguards

Protective measures and controls that are prescribed to meet the security requirements specified for an AIS. These safeguards may include, but are not necessarily limited to, hardware and software security features; operation procedures; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures, areas, and devices. (NCSC-TG-004)

Note: Synonymous terms for controls / safeguards are mechanisms and countermeasures. Differences between the four terms are academic. For the purpose of this document, all four may be used interchangeably. We will however, be making a distinction in whether or not they (controls, safeguards, mechanisms, or countermeasures) are technical (e.g., automated) or non-technical (manual) in nature.

Vulnerability

A vulnerability is a weakness in system security procedures, system design, implementation, internal controls, that could be exploited to violate system security policy. (NCSC-TG-004).

Risk

The probability that a particular threat will exploit a particular vulnerability of the AIS or telecommunications system. (NCSC-TG-004)

Risk Management

The **total process** of identifying, measuring, and minimizing **uncertain events** affecting AIS resources. It includes risk analysis, cost benefit analysis, safeguard selection, security test and evaluation, safeguard implementation, and continuous security monitoring. (NCSC-TG-004)

Keys to the definition lie in the phrases "total process" and "uncertain events." "Total process" is the beginning to end (life cycle) totality of risk management. Risk management is just as concerned with the operation of a system as it is with its development. The concern is not only with the platform but also the environment in which it operates. Risk management isn't something you do once then move on to something else. Rather, it is a continual process (a "total process") through out the system's life.

In the AIS world, uncertain events are undesirable and akin to "undocumented features." In the context of the definition, an uncertain event equates to a risk (a probability that a particular threat will exploit a particular vulnerability of the system) and produces an unacceptable outcome. Continuing with the definition, we find that risk management identifies, measures, and minimizes those uncertain events or risks.

Risk Management Overview

Risk Management Basics

Risk management, information security, controls, threats, risks, vulnerabilities, and other security terms tend to intimidate people unnecessarily. The terms are unfamiliar, they sound complex, and may be perceived as a complication to doing your business. The prospect of a visit by security personnel may seem intimidating - almost invasive. In reality, risk management is an intuitive process; performed every business day by responsible developers, integrators, operators, and managers. Risk management may not be a process at the tips of our tongues and the terminology may be unfamiliar but we do it nevertheless.

A manager, regardless of discipline (software development, operations, or in this case security) will try to identify the variables most likely to influence the outcome of the task at hand. The successful manager **identifies** the variables, **understands** how they effect the task, and **uses** this knowledge to complete the task even without having total control of the environment. The process is not an exact science but an understanding of what can be controlled and what can't. The Risk Management Model, Figure 1, provides the first input to the process - identification of the variables and a visual insight into their interactions.

Components of the Risk Management Model

The risk management model is made up of various components. The ovals are variables affecting information security that your company can control, the rectangle represents the threat variable which, generally, cannot be controlled, and the diamond is the risk assessment decision.

The components of the risk management model are dynamic - always in a state of leveling themselves as changes in one forces changes in others. Components can be viewed as either separate states or assembled to reflect a "flow" where the effect of one influences the others. Risk management deals with the dynamics (flow) of the model. The following paragraphs describe the model components.

Information

The model begins with the information component. The primary focus of information security is protection of information. Data and the information derived from it are vital to business operations. Take away the information (loss of availability), corrupt it (loss of integrity), or worse, in the case of sensitive systems, unintentionally disclose the information (loss of confidentiality) and you will be unable to operate.

Information **must** be protected. **Information can't protect itself**. It relies on either the platform or the environment (and more preferably a combination of security controls present in both) for its protection.

Platform (Technical Controls)

The platform component includes computers, bridges, modems, disk drives, printers, terminals, network components, as well as the operating, executive, communications, and application software that govern how it will operate. Platforms have automated (technical) security controls that offer protection services to the information. Technical controls are provided by hardware and/or software and perform specific functions (some control access to information using userIDs and passwords, some perform an audit function, and so forth). These services are usually referred to as technical security controls in that they are automated and operate at a prescribed level of assurance. Once configured, the technical security controls occur typically without operator intervention and are generally transparent to the end user.

Environment (Non-Technical Controls)

The environment component surrounds the platform component. **The environment offers protection to the platform while the platform protects the information.**¹ Security controls within the environment (non-technical security controls) reinforce protection afforded by the platform. Physical, procedural, and administrative security mechanisms like back-up power, door locks, badge systems, policies, operational procedures, location, trusted users, and so forth, are all examples of security mechanisms present in the system's environment.

¹ For example, the system couldn't protect itself from fire or theft. This must be provided by non-technical controls such as fire protection and guard services present in its environment.

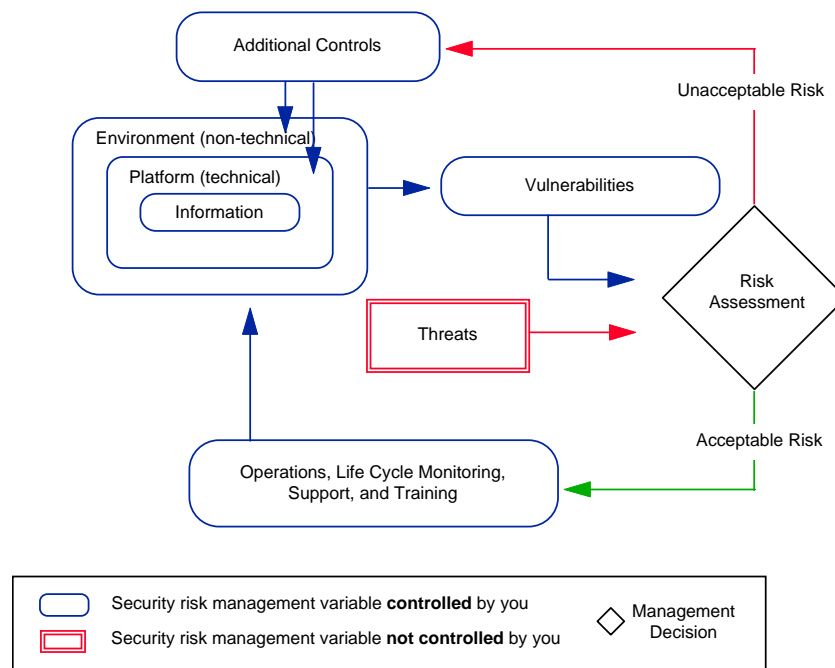


Figure 1. Risk Management Model.

Controls / Safeguards Functional and Performance Characteristics

All protective measures and controls can be functionally classified in one of three categories:

Protective Mechanisms—mechanisms designed to deny unauthorized access such as firewalls and password controls

Detection Mechanisms—mechanisms designed to detect attack attempts (alarms, sniffers, real-time scanners, etc.)

Reaction Mechanisms—mechanisms designed to react to an attack such as disconnecting access routes, isolating attack zones, shutting down services.

To fully understand the security posture of an enterprise, the performance characteristics of each of these mechanisms must be understood: how much time does the mechanism need for it to work? How reliable/available is the service? How secure is the mechanism? For example, if the response chain to an attack involves a manual process, how long the notification and reaction process takes determines the security posture of the organization.

A useful tool to analyze performance characteristics of mechanisms is performance matrices characterizing detection and reaction timelines against anomalous events such as bad password attempts, port scans, firewall breach attempts, DOS attacks, etc.

Vulnerabilities

Although the platform and environment offer security controls to protect information, their protection is not absolute; both can have weaknesses. Weaknesses in the environment and the platform are called vulnerabilities. Vulnerabilities are typically the difference between what the platform (or environment) is supposed to do and what it really does or how it really performs. Vulnerabilities are identified and reported through a variety of means such as security tests and evaluations (ST&Es), penetration tests, flaw hypothesis, trade sources, employee reports, audit reports, covert channel analysis, or by national computer emergency response teams (CERTs).

Threats

All platforms and environments have threats that seek to exploit or cause harm to the information. This inevitability is represented by the model's threat component. Some threats are natural, some are inherent

in the system design, some can be attributed to unauthorized personnel who want to break in and see the information, others are authorized personnel who make human mistakes. There are different categories of threats but the prime concerns are the likelihood that the threat will be realized and its impact on the confidentiality, integrity, or availability of the information. Threats change over time and should be periodically re-assessed. Table 1 illustrates the four threat types and examples of each that are relevant to information systems in general.

Table 1. Threat Types and Examples.

Threat Type:	Examples:
Human Intentional	Malicious intruder (hacker) Terrorism / attack Corporate espionage / competition Disregard for procedures Disgruntled employee
Human Unintentional	Curiosity seeker Untrained user Data entry error Programming or configuration error
Structural	Physical environment Hardware anomaly Software anomaly Power anomaly
Natural	Fire Wind Flood

Risk Assessment

The risk assessment component brings vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of safeguards together for examination. (Risk is the probability that a particular threat will exploit a particular vulnerability of the system.)² The risk assessment weighs known or perceived threats with known or perceived system vulnerabilities to determine the magnitude of risk present if and when the system is placed into operation. The results of the risk assessment are presented to the system owner in support of a certification decision. It is the responsibility of the owner to determine whether or not the risks are acceptable.

Unacceptable Risks

Unacceptable risks require that something be done to either the platform (via technical controls), the environment (via non-technical controls), or preferably an economical combination of both to reduce overall risks to an acceptable level (you can never economically eliminate risk altogether). It's a business decision that says the benefit (greater safety of information) is worth the cost (a change in the platform or environment). When a risk assessment brings back an "unacceptable" verdict, program managers or developers re-visit the security requirements to ensure they've been implemented correctly, consider strengthening existing controls, or determine the need for additional controls. After corrective measures are taken, the system re-enters the Risk Management Model's flow for another round of testing for vulnerabilities and assessment.

Controls

Controls (often called safeguards, mechanisms, or countermeasures (CM)) are security mechanisms that are added to or modify the platform or the environment in an attempt to eliminate (mitigate) or decrease (minimize) vulnerabilities. Controls are protective measures implemented into the system to meet its security requirements. Controls may include, but are not necessarily limited to, hardware and software security features, operating procedures, accountability procedures, access and distribution controls, management constraints, personnel security, and security of physical structures, areas, and devices. The control component is an important player in the risk management process during all life cycle phases.

² Risk exists only in the presence of threats and vulnerabilities, e.g. if there are no threats, there is no risk. Likewise, if there are no vulnerabilities, there is no risk.

After controls are added or made more robust, their performance is tested in the “system” context and re-assessed to determine if vulnerabilities and risks still exist.³

Acceptable Risks

Acceptable risk doesn't mean that the system's security is without its faults. It means that the owner is sufficiently satisfied with the way information is protected by the system, that the risks are acceptable, and that he or she takes security responsibility for the system and allows it to be placed into operation. Acceptable risk implies that an economic balance between security and operations has been achieved.

Operations, Life Cycle Monitoring, Support, and Training

The operations, life cycle monitoring, support, and training component completes the model and ensures that the system security remains acceptable throughout the duration of its life cycle. It provides the feedback loop necessary to support continual assessments since the platform, environment, vulnerabilities, value of the information, and the organizational requirements evolve over time. It also ensures that re-assessments and training are provided on a recurring basis.

Visualizing the Risk Management Model Dynamics

A very important aspect of risk management is being able to visualize the dynamics of the model's components, how they interact, and relating their dynamics to the information security requirements of the system.

Practice walking through the model by mentally changing the sensitivity of the information, the technical and/or non-technical controls applied, the nature of the threats, the observed vulnerabilities of the system, your decision as to the acceptability of the risk, etc. After a little practice it becomes easier to visualize the dynamics.

A key to risk management is applying the most economic blend of technical and non-technical security controls necessary to provide an appropriate level of assured security to the information you're protecting. Neither the Risk Management Model nor this document will tell you how much is enough when it comes to security. There is no global textbook answer.

Developing a Risk Management Mindset

Risk Management is an “Acquired” Taste

It may sound odd but risk management is an acquired taste; similar to acquiring a taste for certain foods. The taste is acquired through practice. You can read all of the textbooks in the world but you won't be able to put risk management to work unless you incorporate it as a natural way of doing business. Four things you need to do to get going are:

Develop an understanding and appreciation for the dynamics in the risk management model.

Develop a risk management mindset. Learn to ask the right questions.

Get the answers to your questions.

Assess the results.

The mindset is intuitive and can best be built by asking essential information security-related questions and getting the answers. All of the questions are straight forward but often overlooked when it comes to information security. When you get a negative answer, it will automatically give you another set of related questions to ask.

Table 2 contains 17 questions that will definitely break the ice and gather essential information you need to assess and manage the risk in your system. This list of questions is repeated in Attachment 3 in an expanded form to assist your risk management efforts. It can be completed and attached to the Worksheet as supporting material.

³ Assuming the threat stays the same.

Table 2. Risk Management Questions.

1	Are company employees or contractor personnel assigned responsibility for ensuring that security is adequate and for day-to-day security management?
2	Is the sensitivity of the information in the system and its criticality to the company documented? Are there types of information that require special protection?
3	Are system threats identified and documented? Are they assessed in terms of likelihood and impact?
4	Are the technical and non-technical controls for the overall system and its internal and external interfaces documented? (What is it supposed to do?)
5	Have the security requirements been developed, integrated, or configured into the platform and environment?
6	Is there a graphic or verbal description and inventory of the overall system? Does the description show where the safeguards have been placed? (What precisely are we talking about when we refer to "the system"?)
7	Has the system been tested to ensure it actually does what it was supposed to do? (What are my <u>actual</u> vulnerabilities?) Are the system's security controls as strong as they need to be? Are <u>they</u> secure?
8	Have knowledgeable company developers, integrators, testers, and/or security personnel signed off on the system's security? Have knowledgeable non-company personnel who input, process, transport, manipulate information on the system, or protect its environment acknowledged their responsibilities?
9	Have the security risks of operating the system been documented?
10	If the risks have been found to be <u>unacceptable</u> , have additional controls been identified? Have the controls been assessed in terms of their cost to implement and benefit in reducing risk? (What will it cost to reduce the risk?)
11	If the risks of operating the system are found to be <u>acceptable</u> , has formal approval been granted to continue with the development, advance to the next milestone, go into production on an interim basis, or go fully into production?
12	Is a procedure in place to identify, report, and correct possible breaches in security in a timely manner?
13	Are security administrators trained to ensure they know what they are responsible for and how to perform their duties?
14	Are users trained to ensure they know and carry out their security responsibilities?
15	Is there a recurring training program for administrators and users so that they stay proficient in their security responsibilities?
16	If something goes wrong with the system is there a plan to get back up and running?
17	Is the system's security posture monitored to ensure that the risks of operation remain acceptable throughout its life cycle?

Figure 2 illustrates how the risk management questions relate to the components of the Risk Management Model.

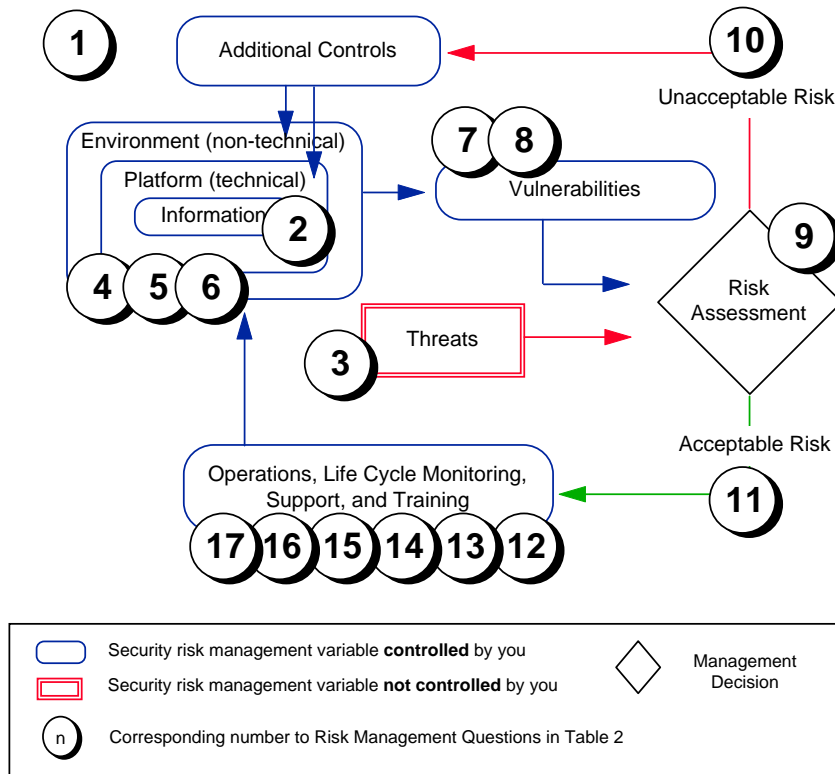


Figure 2. Relating Key Questions to the Risk Management Model.