Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Risk-Eye for the IT Security Guy

As the practice of IT security matures, the capabilities of security practitioners must improve in the area of risk management to keep pace with the growth of the security issues in IT industry. In particular, US Federal guidance in the form of National Institute of Standards and Technology (NIST) special publications, provide only introductory coverage of risk management methods. The Software Engineering Institute's Continuous Risk Management (CRM) process, a cyclic risk management paradigm, is tailored to the domain ...

Copyright SANS Institute
Author Retains Full Rights

AD

Risk-Eye for the IT Security Guy
(Focusing on IT Security Enterprise Risk Management)

Thomas Siu

February 4, 2004
GSEC Practical Version 1.4b (Option 1)

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Risk-Eye for the IT Security Guy
(Focusing on IT Security Enterprise Risk Management)
Thomas Siu
February 4, 2004

Abstract

As the practice of IT security matures, the capabilities of security practitioners must improve in the area of risk management to keep pace with the growth of the security issues in IT industry. In particular, US Federal guidance in the form of National Institute of Standards and Technology (NIST) special publications, provide only introductory coverage of risk management methods. The Software Engineering Institute's Continuous Risk Management (CRM) process, a cyclic risk management paradigm, is tailored to the domain of IT security to produce an enterprise risk management methodology suitable for Federal government organizations. This process builds upon the basics of the NIST guidance and adds the possibility of managing risks from diverse systems, providing the high-level perspective of security risks that is currently lacking. The resulting management-level processes are scalable from a small organization to a nationwide enterprise, providing a foundational practice for IT security planning. An enterprise risk management workflow model is presented to illustrate the 'big picture' of risk management, the key to developing a "keen eye" for IT security risks as a part of the overall IT management doctrine.

Introduction

This paper will describe an approach that will be generally compatible with the NIST risk assessment guidelines with the goal of defining a well reasoned process to how risks can be managed for IT security. This risk macro-management is termed Enterprise Security Risk Management.

The Federal Information Security Management Act (FISMA) of 2002 directs Federal agencies to,

> "…provide information security through risk assessment and implementing policies and procedures to cost effectively reduce risks to an acceptable level, while periodically testing and evaluating security controls to ensure effectiveness." [1]

This is a prescription for an IT security risk management program. Note the terms "cost effectively" and "acceptable level" as they apply to "reduce risks." A risk analysis method, as part of a risk management program, will help define what level of risk is acceptable, the cost of risk reduction, and how to make tradeoffs between risks. The Act also specifies that NIST will be tasked with providing the required mandatory standards pertaining to Federal information systems.[2] The NIST SP 800-30 Rev A "Risk Management Guide for Information Technology Systems" dedicates only about 3 paragraphs (out of 55 pages) to the concept of risk management[3], and is focused on a

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

monolithic, single-system, risk assessment approach. This guide also calls for, "…ongoing and evolving"[4] risk management processes, but stops short at describing cyclic or evolutionary practices in detail. Similarly, the SP 800-18 "Principles and Practices for Securing Information Technology Systems"[5] and SP 800-33 "Underlying Technical Models for Information Technology Security"[6] assign risk management as the title for what appears to be solely a risk assessment method. It is assumed that the NIST guidelines have the objective of assessing risks once during early stages of a system or project's lifecycle, identifying and applying controls to major risks, but never formally reviewing risks again. To move up to the next level of IT security risk management, the possibility of managing risks from dissimilar systems must be addressed. What is needed is an approach to gathering and managing risks from various subsystems in an organized and consistent manner, such that enterprise security risks have the same management visibility as enterprise projects. This need for managing risks on a macro-scale combined with the local-level focus of NIST guidelines with linear risk assessment leaves a gap in the practice of IT security risk management. Some critical enterprise wide risk management activities in that gap are:

- Making trade-offs between risks and opportunities provided by related or unrelated IT projects, with teams that may not have visibility into security risks outside their project or system.
- Assigning responsibility for certain groups or classes of risk, such as security risks that cross boundaries between physical security and IT security.
- Performing analysis of aggregate risks from multiple systems which may be a harbinger of a cascade failure, including root cause analysis.
- Managing risks in an impact timeframe that is shorter than the typical risk assessment process.
- Determining when a risk has become realized as a problem, and handling it as a problem and no longer as a risk.
- Rapidly integrating newly identified risks into the risk management focus.

Background

Risk management in the IT security field can look to many examples in other domains for raw material to build upon. In a recent article in IEEE Computer magazine, author Dan Geer labels IT security leadership as in interdisciplinary endeavor, and identifies several adaptable risk management methods from other fields. He makes a call to IT security practitioners to absorb risk-aware methods from other domains (such as reliability engineering, software quality assurance, biology, public health, investment banking, and insurance) and develop a vigorous hybrid risk management approach.[7] Cryptanalyst Bruce Schneier argues that security risks need to be managed just like real world risks, and organizations that manage risks better will perform better.[8] Upon investigation of literature available on software[9] and project risk management[10], a unique risk management approach was encountered in a paper by David Gilliam[11] that appears to be already a vigorous hybrid. This approach is the Continuous Risk Management (CRM)[12] program from the Software Engineering Institute at Carnegie Mellon University.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Risk Nomenclature in CRM

The CRM is a risk management approach hybridized from the software engineering and project management domains, and use of terminology is different from what is often used in the pertinent NIST guidelines for IT security.[13] To gain the clear understanding of how to use CRM in an IT security context, these definitions are offered:

- Risk is the potential for realization of an unwanted negative consequence.[14]

- A risk is <u>not</u> a problem.

Thinking about risks as 'potential problems' sets the stage for the manager or analysis team to make decisions to avoid such problems. If a risk has become a problem, it is too late for mitigation. Action is warranted right away for problems. If risk management has been successful, that action has been planned, rehearsed and budgeted.

The NIST SP 800-30 (Rev A) defines Risk as: Risk = Threat x Vulnerability[15]

CRM defines risk statements as: Risk = Condition (Probability) + Consequence (Impact)[16]

The CRM definition of risk used in this paper encapsulates the threat-vulnerability concept of NIST within the Condition variable, which is described later under Step 1. A general definition of risk management applied to IT security should be the disciplined approach to reducing the probability, impact, or timeframe of security risks associated with computerized data and network communications as a function of various threat sources. This is offered as a possible bridge of 'common language' (called for in a paper by Archie Andrews[17]) between IT security risk managers and project or program managers who are responsible for different parts of an IT system or environment. If IT Project managers are using CRM-like risk management methods, adapting the IT security risk terminology and semantics will help them gain an understanding of how security risks fit into the overall project or program risk scheme.

Thinking risk also involves determining the likelihood of a risk becoming a problem. The benefit to this perspective is like that ofa 'glass half-full' mentality, there is also the potential that the risk will *not* become a problem. This challenges the current conventional thinking that the presence of security risks is "bad." When projects are "running toward risk[18]" to be successful, IT security risks become manageable if they are, after focused analysis, viewed simply as 'potential' problems.

The CRM is a set of processes, methods, and tools to manage risks within a disciplined environment. It supports active decision making to:

- continually assess risks (what could go wrong)
- determine which risks are most important
- implement strategies or controls to deal with these risks
- assure (with measurement) that these strategies are effective

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The CRM Cycle

The CRM cycle consists of 5 sequential steps, accompanied by an ongoing effort of communication and documentation.

1. Identify- risk assessment activities creating a risk inventory
2. Analyze- comparison and ranking of risks
3. Plan- deeper analysis of risks and planned actions or tradeoffs, contingency planning as necessary
4. Track- management of the planned efforts, looking for risks becoming problems, status reporting
5. Control- decision making concerning disposition of risks in the inventory, ranging from retiring risks to executing contingencies

These risk components evolve through the 5-step cycle, which can iterate at any organizational business cycle frequency (daily, weekly, monthly, etc.). These steps are now described in more detail, from the perspective of an interdisciplinary team that creates a baseline risk inventory for a hypothetical virtual private network (VPN) system.

Figure 1: Basic CRM Diagram[19]

Step 0: Scope Determination, System Data Gathering, and Goals

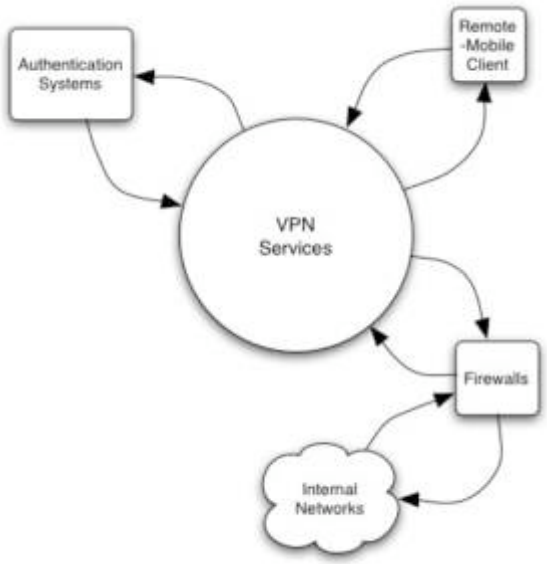
The CRM was designed to support software project management, but IT security risk management often applies to systems already in 'production environments' which often did not consider IT security requirements early in the system lifecycle. The objective of Step 0, though not formally part of the parent CRM process, is added to gather the pertinent information such that the risk assessment can proceed.

A useful and effective method to determine the scope of the assessments is done by building a context model. A simple context model[20] for the hypothetical VPN system is

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

provided in Figure 2. The large central circle defines the scope of the system and workflow from which you want to find IT security risks. The boxes around the circle that represent 'adjacent systems' that feed data or information in and out of the workflow.

Figure 2: Context Model



Deciding the scope of the assessment is done by moving these adjacent systems in or out of your circle (which becomes your scope boundary). It is extremely helpful later to have and understanding of what adjacent systems receive information from your system, but may be out of your scope. Now pertinent data concerning what is within scope of your effort must be gathered, such as host, server, software, types of information, user types (internal or external), network characteristics, general threat trees, and vulnerability information.

An additional Step 0 activity also involves setting goals. In a project sense, this means to identify the project goals, such that risks to obtaining those goals keeps the risks pertinent to the project. In using CRM in an IT security sense, this goal setting means gaining an agreement between all major stakeholders at their (and their organization's) risk tolerance level (or 'acceptable risk'). This may be difficult to do at first, but considering requirements like confidentiality, integrity, and availability will help with goal setting. After one iteration of the CRM cycle, all participants may have a stronger idea of their collective risk tolerance, and since the process is continuous, changes to organizational risk tolerance can be dealt with in the planning stages of subsequent cycles.

Step 1: Identify- Risk Assessment

The objective of Step 1 is to develop a list of IT security risks for the system defined in Step 0. This also should include any procedural or management risks that would negatively impact the goals that have been set. To develop this list of risks, it is important to define a standard set of key attributes for each 'risk statement.' Clear risk statements are essential, no matter the source or type of risk, so that they can be compared directly between systems or projects.

A risk statement then identifies a condition and an associated consequence. It follows the format:

> Given the *CONDITION*, there is a possibility that *CONSEQUENCE* will occur.[21]

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The condition is a brief description of context, such as circumstances, observations, or situations that cause concern to the analysis team. The consequence is the major negative outcome of the conditions described.

Example Risk Statement 1:

> Condition: The users are connecting to the corporate network via VPN from remote locations using their personal home computers (vulnerability), which are not rigorously protected from external attack (threat).
> Consequence: An attacker who compromises a user's home computer via their ISP or home network may gain access to the sensitive corporate network. If this user has access to sensitive corporate information, that information is likely to be disclosed with dire consequences.

Good risk statements have the following characteristics:

- Clear and concise
- Understandable to all participants (avoid specialized jargon)
- One condition, one or more associated consequences
- Contextual information is helpful if it identifies the what, where, when, and how, if that background information is not in the risk statement

Example Risk Statement 2:

> Windows2000 Clients. Patch every 3 hours.

This is an example of a poor risk statement. Essential context information, as well as conditions and consequences of the potential risk are left to the imagination of the reader. This would complicate further comparison with other risks.

As a comparison for readers familiar with how NIST SP 800-30 defines risk statements (threat x vulnerability), the threat and vulnerability semantic is captured under the 'condition' section of the CRM risk statement. The consequence statement defines the specific problem that may occur, which focuses the risk statement on a general impact discussion. Note that the NIST SP 800-30 guidelines do cover impact in their analysis guidance but do not formally include it in the risk statement because it is included in the numerical value assigned to the threat variable.[22] In the CRM, the Condition/Consequence risk statement considers relative impact in Step 2. The Identification phase is focused on finding and defining as many security risks as possible. Because it is a cyclic process, any risks initially missed but discovered later can be folded into the process. As we will see later, impact of the risk will weigh in the prioritization of risks.

The CRM process by definition intends to manage a variety of risks, and so is quite liberal in recommending risk identification or risk assessment methods and activities. The objective of an initial baseline risk assessment is to obtain an inventory of security risks, each having a risk statement and contextual information. An IT project could perform different types of risk assessments during different iterations of the CRM cycle. Formal risk assessments may be necessary depending upon the circumstances, but

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

less formal methods may be equally effective, but less costly in terms of time. Since the process is continuous, new risks can always be added later. While the NIST SP 800-30 describes a single risk assessment method, other NIST guides point out that risk assessments can, "…be accomplished in a variety of ways depending upon the specific needs of the organization."[23] The CRM Guidebook lists and describes several risk identification techniques[24], all of which can be adapted to IT security risk assessment, and are deemed compatible with NIST guidance:

- Brainstorming (informal)
- Taxonomy-based questionnaires (formal)
- Goal/Question/Metric (formal)
- Checklists (informal)
- Failure Modes and Effects Analysis[25] (formal)
- Fault/Threat Tree Analysis[26] (formal)
- Probabilistic Risk Assessment[27] (formal)
- Lessons Learned of problems seen on other projects (both formal and informal)
- Voluntary reporting (informal)

To get a risk baseline for the example hypothetical VPN system, a straightforward security risk assessment is performed using a multi-disciplinary team in a brainstorming session using OCTAVE[SM28] threat tree analysis. This team will include IT security analysts to bring threat and environment perspective, a project manager to bring business impact perspective, software and hardware systems engineers who know what applications and tools the system employs, network and telecommunications representatives as needed, and a facilitator. The OCTAVE[SM] trees based upon network access, physical access, system problems, and other problems (natural disasters, etc.) are discussed in context of assets, actors, and outcomes. These threat trees are very helpful in identification of management and process-based security risks in addition to the technology based risks. The team works through the threat trees to build a list of risks. Each risk that is identified by the team is then distilled into a risk statement that includes the data described in this table:

Item	**Description**
Unique risk identifier	A unique identifier that helps to distinguish a risk from others in the enterprise. For example, it may have some designation of a locality, or system name, and then a numerical value.
Condition	A single condition that leads to the potential risk.
Consequence(s)	A number of adverse consequences that are postulated as directly related to the stated condition.
Context	Additional information that captures the original intent of the risk statement to help other personnel understand it as time passes. Can be circumstance or additional factors that are not in the Condition and Consequence statement. This may also be drawn from lessons learned in similar systems, or from known persistent threat sources.
Origin	The name of the person who will be able to explain conditions. Usually the person who identified the risk.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

This basic risk statement format is important because later in the CRM cycle, new risks may be identified as work proceeds, independent of formal risk assessments. New risks will be added to the risk inventory and must be compared against those already in the listing. Teamwork is valuable in encouraging all personnel to bring forward new risks that they see beyond the horizon of immediate problems.[29] Each risk has a documented risk statement, including a condition and consequence. Unlike the NIST guidelines, which perform threat/vulnerability valuation analysis during the assessment phase, Step 1 is to identify risk and develop the risk statements. For the example VPN system, the risk listing includes:

ID: VPN-77-1 Origin: Stephan Hawking	Risk Statement- Condition: The users are connecting to the corporate network via VPN from remote locations using their personal home computers(vulnerability), which are not rigorously protected from external attack (threat). Consequence: An attacker who compromises a user's home computer via their ISP or home network may gain access to the sensitive corporate network. If this user has access to sensitive corporate information, that information is likely to be disclosed with dire consequences.	Context: Indentified through modeling of the workflow and from lessons learned via Industrial Security.
ID: VPN-77-6 Origin: Linux Pauling	Risk Statement- Condition: This VPN uses SSL and a web browser client. A commonly used web browser automatically caches the user credentials, without the user's knowledge. Consequence: The cached credentials can be used to reconnect to the network via VPN by an unauthorized user.	Context: Some users have reported using kiosks in airports or internet café's to check on corporate email via the VPN.
ID: VPN-77-14 Origin: A.T. Hunn	Risk Statement- Condition: Several corporate laptops have been lost, but not reported immediately. Consequence: A dedicated corporate spy could use information on the laptop to gain access to the network via the VPN.	Context: A secondary risk related to VPN-77-6

Now that a baseline set of risks have been gathered, the next step describes the analysis.

Step 2- Analyze

Once an inventory of IT security risks have been collected, the analysis process begins, which will result in the first general step of risk management, managing groups of risks. The objective of Step 2 is to assign ownership, categorize or group risks, and then

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

prioritize them. This information will drive the decision process in subsequent steps of the cycle.

Risk Attribute Analysis

The CRM defines 3 basic attributes to each risk statement:

- Probability- likelihood of risk becoming a problem
- Impact- loss or effect of the risk on the environment or system if the risk is realized
- Timeframe- time period when actions must be taken to mitigate the risk

It is beneficial to have your data from Step 0 available, since it permits the determination of the thresholds for the risk attributes. An example set of specific criteria are defined here using a 3-level gradient of risk exposure.

Attribute	**Level**	**Description**
Probability	Likely (High) Probable (Medium) Unlikely (Low)	*Likely* to become a problem, >70% probability *Probable*, 30-70% probability *Unlikely* to become a problem, <30% probability
Impact	Catastrophic (High) Critical (Medium) Marginal (Low)	Loss of complete functionality. Major damage or loss. Minor damage or loss.
Timeframe	Near term Mid term Far term	Within 1 day. Within 2 weeks. Beyond 1 month.

These attribute levels may be defined by the organization as a whole, or are set by the project team. The CRM Guidebook gives numerous examples of the use of binary, 3-level, 5-level, and n-level, including using quantitative values versus these qualitative criteria.[30] The essence of this analysis is that these criteria may need to consider what will work within the given organization, prescribed customer specifications, as well as the time available for the analytical work. The interdisciplinary team now reviews risks in the inventory. Values for Probability, Impact, and Timeframe are assigned to each risk statement based upon the pre-defined attributes. If a probabilistic risk assessment was performed, quantitative data are available to assign probability. Qualitative or experiential approaches are also satisfactory. In contrast, the NIST SP 800-30 embeds the concepts of probability within its approach to threat likelihood, and impact within the bounds of data confidentiality, integrity, and availability. Timeframe for action is used differently in the NIST guide, where minimizing the exposure window is used as for each risk based upon the calculated risk level.[31] The CRM intends to use the timeframe for action in the effort to rank risks against one another for priority.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

For the example VPN system, viewing the risk statements in context of the Step 0 goals will serve to help categorize the impact of the risk.

Categorization

Now the risks, which have their attributes assigned, are evaluated *en masse* to look for patterns or relationships between risks. The objective here is to condense the risk listing such that common cause may stand out, and duplicate risk statements can be combined. This permits the team to sort through what can be a large amount of data. Typical categories of risks often follow the OCTAVE[SM] threat trees, such as network-based risks, system risks. This categorization permits the decision to mitigate and track a group of risks as a set. The CRM Guidebook also notes that sometimes a risk is only seen when all the component (smaller risk) pieces are seen together.[32] In this case, a new summary risk statement is created, with a new unique identifier, keeping the worst case of the defined attributes from the component risk statements.

The aggregate or 'set of risks' concept is a level of abstraction that fits an enterprise risk management model, where they would be managed in aggregate as one risk. Examples of enterprise-based risk management sets could be:

- Remote access risks for mobile clients and computers.
- A class of complex and persistently vulnerable applications or operating systems.
- Entrepreneurial business areas where risk tolerance is high.
- Intercommunication between business partners in differing security environments.

Prioritization

Not all risks in the inventory will be within the capability of an organization to completely mitigate. The purpose of prioritization is to sort out the most important risks for action. Using the assigned values of Probability, Impact, and Timeframe, the classes of risk, as well as the singular risks, are ranked against one another. Each risk statement then gets an ordinal risk value (1, 2, 3, etc.). Typical ranking guidelines involve first addressing the risks with Near timeframe and High impact values. A risk will get a lower value or may be eliminated if it is already being addressed. The organization will have to determine if the Top 5, Top 10, or Top "N" risks will be moved further into the cycle. If the baseline has been completed on an earlier cycle, new risks are then compared against the current top risks, and they group is re-ranked. Now the 'big-picture' of the risks has been formed. Note that the NIST SP 800-30 also performs prioritization, but of mitigation actions, not of risks.[33] This is understandable in the context of a single system, where all identified risks might require an applicable control implementation.

The following example risk statement from Step 1 is provided with risk analysis data completed[34]:

ID: VPN-77-1	**Risk Information Sheet**	**Date Identified:** Jan 12, 2004

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Priority:	**Risk Statement:** Condition: The users are connecting to the corporate network via VPN from remote locations using their personal home computers (vulnerability), which are not rigorously protected from external attack (threat). Consequence: An attacker who compromises a user's home computer via their network may gain access to the sensitive corporate network. If this user has access to sensitive corporate information, that information is likely to be disclosed with dire consequences.		
Probability: Medium			
Impact: Major	**Timeframe:** Near term	**Origin:** S. Hawking from the Incident Response team.	**Assigned to:**
Context: Based upon an incident last year reported by Industrial Security.			
Action Plans: (watch, accept, research, mitigate)			
Contingency Plans and Trigger:			

Step 3- Plan

Now that the list of top risks have been defined, three tasks must be completed in the planning phase. The objective of Step 3 is to assign of responsibility, determine of risk handling approach, and define actions. In assigning responsibility, the team is making the determination that the risk lies within the responsibility of the organization. If another organization is responsible for the risk, it is transferred. Otherwise, the part of the organization that can best handle the risk is delegated to handle the risk. Application security risks, for example, would be assigned to an applications group.

Once the group has determined that the risks are within their responsibility, four common handling approaches are given:

Approach	**Description**
Research	We don't know enough about the risk to know what to do about it. Investigate the risks enough to make an informed decision.
Watch	Monitor the risk for early signs of trouble, or 'triggers' that may impact the Probability, Impact, and Timeframe. Usually done for risks which have significant impact, but low probability.
Accept	Do nothing. The risk will be handled as a problem if it occurs, and the organization will accept the consequences. Contingency plans in this context address risks that are watched or accepted.
Mitigate	Eliminate or reduce the risk by taking actions that: • Reduce Impact, such that it is tolerable • Reduce probability, making it less likely

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

	• Extend Timeframe, permitting more time to deal with the risk

An action plan for a particular risk may involve more than one action item. For example, risks of mobile computing devices may require both research and acceptance, followed by subsequent mitigation later in the cycle. These actions need to be defined for the systems taking into account the priorities of the goals (from Step 0) as well as the timeframes for implementation and how the risk fits into the overall picture of the system. Action plans are the foundation of the IT security planning called for in the FISMA protection guidelines referenced in the introduction of this paper, which assume that mitigation decisions will be made for all risks. It should be noted that risk mitigations may also add new IT security risks to the system. This is another justification for a continuous process of risk management, such that new risks are always addressed in context of the risk baseline. Our example VPN's number one risk is then described:

<table>
<tr><td>Priority:
1</td><td colspan="3" rowspan="2">Risk Statement:
Condition: The users are connecting to the corporate network via VPN from remote locations using their personal home computers (vulnerability), which are not rigorously protected from external attack (threat).
Consequence: An attacker who compromises a user's home computer via their network may gain access to the sensitive corporate network. If this user has access to sensitive corporate information, that information is likely to be disclosed with dire consequences.</td></tr>
<tr><td>Probability:
Medium</td></tr>
<tr><td>Impact:
Major</td><td>Timeframe:
Near term</td><td>Origin: Stephan Hawking from the Incident Response team.</td><td>Assigned to: Steve Employment on the Client Services team.</td></tr>
<tr><td colspan="4">Context: Based upon an incident last year reported by Industrial Security.</td></tr>
<tr><td colspan="4">Action Plans: (watch, accept, research, mitigate) Mitigate: Restrict VPN services to the minimum essential to reduce impact. Deploy personal firewalls to home user's systems to reduce probability. Watch: Evaluate IDS on the VPN gateway to determine if immediate response needed.</td></tr>
<tr><td colspan="4">Contingency Plans and Trigger: Problem will be evident if traffic from remote clients exceeds the currently measured levels by 20%.</td></tr>
</table>

In comparison, the action planning phase of the NIST SP 800-30 is covered under "Mitigations."[35] The 'risk avoidance' and 'risk limitation' used by this NIST guide correspond most closely with CRM mitigation actions in Step 3. The difference in semantic is that in the NIST guides, all actions are considered 'mitigation', whereas in CRM a risk acceptance decision is distinct from the risk mitigation decision. The NIST guide then delves deeply in various managerial, operational and technical controls, which is much more of localized sub-system scale than the CRM, which is focused on a system or enterprise management scale.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Note the use of the term Contingency Plans in the context of CRM is quite different from that used by NIST[36], where contingency planning is attributed to recovery from outages or disasters. In the CRM, contingency plans are proposed actions that are in reserve for when a particular risk (usually the Top "N") become problems. In a sense, if the top security risk becomes a problem that has system outage as an impact, the two perspectives merge.

Now that the risk baseline is completed, and actions are assigned, the typical IT security plan is prepared based upon these actions. In the risk information sheet, the action plans are entered.

Step 4- Track

This is the phase where CRM goes beyond the coverage of NIST guidelines. Tracking is the phase of the process where data are managed to ensure that the actions defined in the Planning phase are being executed. The objective of Step 4 is to collect timely, accurate, and relevant risk data, then compile and report the tracking data. The tracking effort will drive decisions about risk management. When a risk action is 'watch,' the specific risk metrics are tracked to look for a trigger that it may be turning into a problem.[37] Additionally, trend analysis of risks, such as an ongoing comparison of the Top Risks, number of risks open and closed, and stoplight charts are useful tools to identify when a risk is about to become a problem, or when a risk should be retired.

The collection of data pertaining to security risks should rely principally upon status reports. Ongoing reports of risk mitigations will be needed and can be applied to the tracking process. The frequency of data collection should be specified in the action planning phase. An example indicator would be to track risk exposure over time, where risk exposure is derived from the Probability and Impact indicators from the initial risk analysis. The values of these indicators can change rapidly in the IT security domain, so tracking activities need to be on a frequency that meets the local environment's need.

Compilation and reporting in CRM are essential inputs to the Control phase. The compiled data can be correlated as summaries of risk mitigation plans, or risk status, or trend summaries. Risk mitigation plans often involve specific progress reports, and should be presented in a way that management can see if an effort is on track or not. Risk status summaries are most effective in IT security if they keep the risk management effort focused on what is likely to be the biggest security problem. Risk summaries are often presented in a chart format, and when coupled with stoplight charts are helpful in reporting risk status to senior management. Trend analysis is achieved by observing where risks have been in successive iterations of the CRM cycle. These 'patterns over time' are achievable only with a continuous risk management paradigm, and may lead to the identification of new risks in a particular type of project.

Step 5- Control

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The final phase of the CRM cycle, the objective of the control function is to analyze the status reports, make decisions on upcoming events, then execute the control decisions. This is the point when all decisions are made with adequate information, in a timely manner, and with effect.

Some of the control function analysis involves viewing the top risks and data from the Tracking function in cause-and-effect loops. Additionally, cost-benefit analysis, PERT charts for risk dependencies, and mitigation status reports are tool to support this analysis. In essence, Step 5 is the top level control function, something that IT security managers could be performing frequently.

Decisions about risks can be made at this point. Some decisions about the risks in the Top "N" are[38]:

- Close the risk. Trend data shows that the risk is becoming increasingly unlikely, or it is no longer cost-effective to track this risk. Lessons learned data are reported.
- Replan the risk. The mitigation plan does not appear to be working effectively.
- Invoke the contingency. The risk is about to become a problem as based upon trigger indicators.
- Continue tracking and maintain current plan. All is going as expected.At this point, the cycle returns to Step 1.

Ongoing risk identification can be performed either formally or informally and added to the risk baseline. Analysis activities prioritize the new risks with respect to other risks, taking into consideration the execution of planned actions (watch, accept, research, mitigate).

In Figure 3, the workflow diagram presents the basic CRM process, supported by data flow in a clockwise manner. The first iteration defines the baseline risk inventory. As the cycle continues, new risks are added, closed risks are retired, and risks that become problems are moved to the problem realm via contingency efforts.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

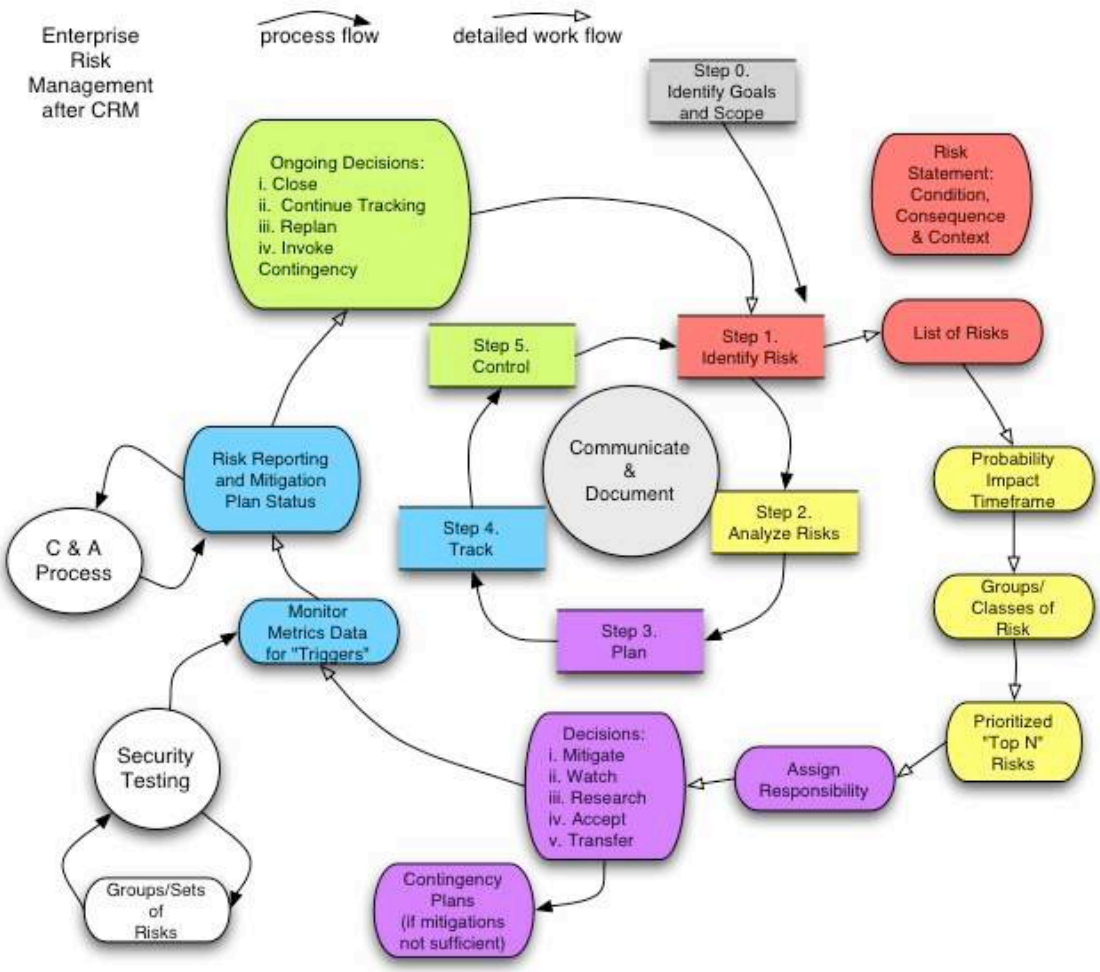


Figure 3: The overall workflow model is depicted.

Enterprise Risk Management

The use of the term enterprise here connotes an entire Federal agency, which may be geographically and functionally dispersed nationwide or globally. Risk assessments are unlikely to be conducted at this level, but risk management should be essential. The objective of CRM at this level is to collect the Top "N" (5%, for example) of the most pressing IT security risks from all of the enterprise systems (e.g. enterprise IT systems, infrastructure, etc.), analyze them in aggregate, and derive strategic decisions that balance the opportunity vs. security risks. A basic approach to achieve this is straightforward:

1. Define which systems are 'enterprise' (also called major) systems. This could be a collection of IT infrastructure and applications that support a strategic capability of the Federal agency.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

2. Allocate resources for risk assessments of sub-systems that make up or support the major systems. Create risk baselines. These risks are managed in 'child' CRM cycles pertinent to the scope of these sub-systems.
3. Define what percent of the top risks, such as 10-15%, in the condition/consequence format, are reported upward from the baseline risk listings of sub-systems. They should also report risk closure/retirement as well as when a risk becomes a problem.
4. Correlate these Top Risks of major systems risks into an enterprise risk inventory. At an enterprise level, track and control the "Top Enterprise N Risks."
5. Assign responsibility for actions that cross boundaries, usually residing with senior management. This permits enterprise systems managers to see what security risks they bring to the shared environments.

Typically the Chief Information Security Officer (CISO) will be the decision-making authority in this scenario, but a key role in this effort is the need for an Enterprise Security Risk Manager or Chief Risk Officer. As described by Tom DeMarco in The Deadline[39], this risk manager is to track and analyze these risks with no expectation of a "can do" attitude, which should keep the decision makers appraised of the realistic impacts of the risks. The person in this role needs to have both the technical and people skills to balance various interest with strategic demands in coordinating enterprise-wide risk management.[40]

The CRM is also easily scoped down to cover a specific installation or business group, which would collect the Top "N" risks from its subsystems. Since the risk statement format is simple and commonly structured, it can be understood in comparison to risks from dissimilar environments. There are likely to be hundreds of risks; only the collective Top Risks should get attention in this cyclic view.

Conclusion

The NIST risk management guidelines offer a linear, waterfall assessment method. The NIST SP 800-30 and SP 800-53 call for 'ongoing' risk management, but to apply them in an iterative manner would require an unacceptable time interval between iterations (several months). As IT security risks are as volatile as the Internet, adapting a solid continuous risk management model permits a comprehensive and up-to-date view of the IT security risk inventory. In this context, the CRM is a superior methodology, due to its speed of identification, analysis, and action planning. Top risks are evaluated with respect to each other, risks that are realized are managed as problems, and new risks are rapidly integrated into the cycle. Using the CRM approach will also align IT security management more closely with conventional IT systems and project management, hopefully bringing security requirements earlier into project lifecycles.

This discussion has covered CRM only in a brief summary form in the context of IT security practice. The CRM guidelines and methods are significantly more detailed and comprehensive than presented here, and the reader is encouraged to explore the

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

wealth of options opened by the CRM method. Further research that is necessary in this field would involve:

- Development of a taxonomy-based questionnaire as a tool for rapidly identifying top IT security risks for a system.
- An analysis of appropriate skill sets for risk managers, analysts, and assessors.
- Correlating the Software Engineering Institute's OCTAVE[SM] and OCTAVE-s risk assessment methods within the context of the CRM.
- Improving the understanding of quantitative risk as a function of inherently unquantifiable elements, notably threat and vulnerability.
- Reviewing the literature for common risks seen over a particular year and redefining them in terms of the condition and consequence statements.

The intent of CRM is to manage the making of tradeoffs between varying types of risks and opportunities. IT security risks portend great opportunities behind potentially debilitating impacts. Continuous processes will keep our 'risk-eye' focused on the Top "N" risks, no matter the pace of change or discovery.

---

[1] Federal Information Security Act of 2002 (Title III of E-Government Act, Public Law 107-347); Section 3544. http://csrc.nist.gov/policies/index.html - fisma2002
[2] Ibid. Section 11331.
[3] Stoneburner, Gary; Goguen, Alice; Feringa, Alexis; "Risk Management Guide for Information Technology Systems." NIST Special Publication 800-30, October 2001, DRAFT Revision A, January 2004, p.6. http://csrc.nist.gov/publications/drafts/SP800-30-RevA-draft.pdf
[4] Ibid, p. 40.
[5] Swanson, Marianne; Guttman, Barbara; "Generally Accepted Principles and Practices for Securing Information Technology Systems." NIST Special Publication 800-14, September 1996, p.19. http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf
[6] Stoneburner, Gary; "Underlying Technical Models for Information Technology Security"." NIST Special Publication 800-33, 2001, p.18. http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf
[7] Geer, Dan; "Risk Management Is Still Where the Money Is" *IEEE Computer* Volume 36, Number 12, December 2003.
[8] Schneier, Bruce; Secrets and Lies: Digital Security in a Networked World, John Wiley & Sons, 2000, p 385.
[9] DeMarco, Tom; Lister, Timothy; Waltzing with Bears: Managing Risk on Software Projects, Dorset House, 2003, p.10.
[10] Project Management Body of Knowledge, Chapter 11 "Project Risk Management"; Project Management Institute, Upper Darby, PA, 1996, p. 111.
[11] Gilliam, David; "Managing Information Technology Security Risk," International Symposium on Software Security 2003, Tokyo, Japan. http://www.yonezaki.cs.titech.ac.jp/Workshop/isss2003/slides/Gilliam.pdf (November 2003).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

[12] Dorofee, Audrey; Walker, Julie; Alberts, Christopher; Higuera, Ronald; Murphy, Richard; Williams, Ray; Continuous Risk Management Guidebook; Software Engineering Institute, Carnegie Mellon University, 1996.
[13] The CRM guidebook must be purchased from the SEI. For additional open source information on CRM, consult http://crm.nasa.gov/.
[14] Rowe, William D.; An Anatomy of Risk, Krieger Publishing, 1987.
[15] Stoneburner, *et. al.*, p. 28.
[16] Dorofee, *et. al.*, Discussion of risk exposure, p. 42.
[17] Andrews, Archie; "Security Program Management and Risk"; June 2, 2003, p.3, http://rr.sans.org/rr/papers/5/1061.pdf/
[18] DeMarco, *et. al.*, p. 9.
[19] "Risk Management Paradigm;" The Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA (12 Jan 2004) http://www.sei.cmu.edu/programs/sepm/risk/paradigm.html
[20] Robertson, James; Robertson, Suzanne; Complete Systems Analysis: The Textbook, The Workbook, The Answers; Dorset House, 2000, p.123.
[21] Dorofee, *et. al.*, p. 32.
[22] Stoneburner, *et. al.*, p. 28.
[23] Ross, Ron; Stoneburner, Gary; Katzke, Stuart; Johnson, Arnold; Swanson, Marianne; "Recommended Security Controls for Federal Information Systems." DRAFT NIST Special Publication 800-53, October 2003, p.5.
[24] Dorofee, *et. al.*, p. 29.
[25] Kinetic, LLC; "FMEA Methodology"; 2001; http://www.fmeca.com/ffmethod/methodol.htm (Feb 4, 2004).
[26] The OCTAVE^{SM} method is a useful threat tree method, summarized here: https://rimr.tatrc.org/OCTAVEImplementationGuide/vol18/appendixe.html (Feb 4, 2004)
[27] Stamatelatos, Michael, PhD; "Probabilistic Risk Assessment and Procedures Guide for NASA Managers and Practitioners;" August 2002. http://www.hq.nasa.gov/office/codeq/doctree/praguide.pdf
[28] Alberts, Christopher; Dorofee, Audrey; OCTAVE^{SM} Method Implementation Guide Version 2.0, June 2001. http://www.cert.org/octave/omig.html
[29] Dorofee, *et. al.*, p. 24.
[30] Ibid, p. 43.
[31] Stoneburner, *et. al.*, p. 29.
[32] Dorofee, *et. al.*, p. 49.
[33] Stoneburner, *et. al.*, p. 31.
[34] Dorofee, *et. al.*, p. 146.
[35] Ibid, p. 31.
[36] Swanson, Marianne; Wohl, Amy; Pope, Lucinda; Grance, Tim; Hash, Joan; Thomas, Ray; "Contingency Planning Guide for Information Technology Systems." NIST Special Publication 800-34, June 2002, p.2. http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf
[37] Dorofee, *et. al.*, p. 79.
[38] Dorofee, *et. al.*, p. 98.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

[39] DeMarco, Tom; The Deadline: A Novel About Project Management; Dorset House, 1997.
[40] Pundmann, Sandra; Kobel, Bill; "Send In the Chief Risk Officer," Optimize Magazine, September 2003, http://www.optimizemag.com/issue/023/culture.htm.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced