Växjö University

School of Mathematics and Systems Engineering

Reports from MSI - Rapporter från MSI

Intrusion Management

Fredrik Ohlsson

Jun
2006

MSI
Växjö University
SE-351 95 VÄXJÖ

Report 06117
ISSN 1650-2647
ISRN VXU/MSI/DA/E/--06117/--SE

Abstract

Information security is tasked with protecting the confidentiality, integrity, and availability of an organizations information resource. A key aspect in protecting these resources is developing an understanding of the threats, vulnerabilities, and exposures that they face by using Risk Management.

The objective of Risk Management is to identify, quantify and manage information security risks to achieve organizations objectives through a number of tasks utilizing key Risk Management techniques. Risk Management is a process that ensures that the impact of threats exploiting vulnerabilities is within acceptable limits and at an acceptable cost.

With the increased complexity of modern dynamic networks, traditional defence mechanisms are failing and as a result cyber crime is on the rise [FBI03]. This puts organizations and corporations at risk as the defences are ill-fitted and weak [KBM04].

No information system can be absolutely secure, especially large and complex systems. Embedded security works for isolated, dedicated systems with few users but does not offer cost effective security, and even worse does not always handle security based on a real threat (this is manly due to it inherent inflexibility). A military strategy within the field of information operations suggests a method of information superiority bases on the OODA-loop. This theses propose a method of information security protection based on a combination of risk management techniques and information operation (foremost the OODA-loop). This is in order to ensure a cost effective and a viable future for information security in large and complex systems, where the war at least at present time is lost to the "black hats", a term often used to describe a menaced hacker.

Preface

This Masters thesis was conducted at Växjö University in Sweden. This thesis is based on previous work commenced by FMV in a project that has as a goal to secure "Network Based Defense" strategy and implementation, NBF.

The thesis aims to describe, at a conceptual level a method of network supervision from a security point of view (i.e. command and control systems). This network supervision is based on Risk Management, Intrusion Detection System (IDS) technology, information operations strategies, the OODA loop, decision support and a flexible and highly competent organization.

Or as history states it:

"War is the realm of uncertainty; three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty. A sensitive and discriminating judgment is called for: a skilled intelligence to scent out the truth." — Carl von Clausewitz [CLAUS]

Table of Contents

1 Introduction

There are different ways to approach information security. Very simplified, there are two basic approaches. A static approach that relies heavily on user rules and regulations and static IT-environments that does not change often and therefore can be scrutinously analyzed and protected, usually by border protection. The static approach, again simplified, regards an asset in need of protection as binary; either secure or insecure.

Another, perhaps more modern approach is to utilize a dynamic approach based on risk management. This approach does not regard assets in a binary manner, instead tries to analyze the asset and its environment in its full diversity of available security threats and protection mechanisms. The real world of course uses a combination of the two approaches, usually where the first approach is used as a security baseline [ISACA05] for an organization and the second approach is used to evaluate if further protection is needed (that is more protection than that of what the baseline is offering) and if so what kind of protection.

Risk management is a popular tool for today's information security professionals and is therefore frequently put to practice. There are many different methodologies and standards available on the market today. In order to unify all the available standards and methods offered today there exist an international standardization effort regarding risk management in an ISO/IEC project, conducted by ISO/TMB/WG Risk Management.

1.1 Background

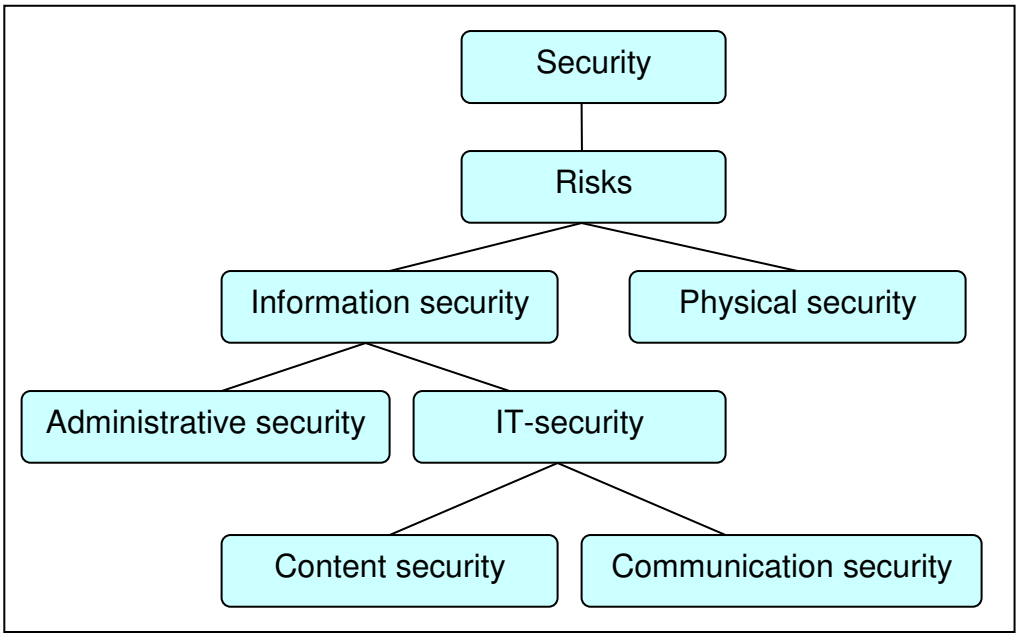
According to Bruce Schneier [SCHN04], the problem with supervision and security in a networked world has always been of keen interest for the research community. The industry has in the past; in collaboration with the research community tested new ideas and evaluated strategies for defense mechanisms. This has been a profitable cooperation and the traditional defense mechanisms are now mature and well understood. By defense mechanisms it is understood mechanisms such as firewalls, encryption, authentication and router-filters, amongst others.

The vast explosion in network development in the last decade has unfortunately left the security research and security industry behind with the result that defenses has once again decreased. The give-and-take relationship between researchers/security industry and network industry has been altered and the security industry has unfortunately been left behind. The reason for this explosion around network development research is foremost the consumer demand for functionality instead of security in today's operating systems and network devices.

With the focus swinging back to security in the last couple of years the funding for research and industry has increased and the security field now have a chance to balance this relationship back to equilibrium. In order for the security field to manage this task, old habits and trails of thought have to be broken in order to se new solutions not based on traditional security methodology and technology. The Security field has to look towards other more mature fields within the research community, such as military strategy, quality methodologies, administrative security (for example policy's, rules, personnel and organization) and physical security among other fields, in order to draw experience and influence towards the information security field in order to advance the field further.

Lately a higher degree of focus has to be directed towards the administrative side of security. IT-security has in the past largely focused on technology to solve defense issues with varying results. Today security personnel largely spends their time with both IT-security (technical aspects) and administrative security in acknowledgement of the fact that users within organizations rarely understand the way that IT-security work and therefore a need for steering (management) and policy emerges.

Information security is within this thesis interpreted as defined by the international information security standards ISO/IEC 17799:2000 [ISO17799]. That is, information security is a management issue composed of both physical security, IT-security and administrative security.



Picture 1.1: describing the different fields encompassed by security according to ISO/IEC 17799:2005

1.2 Problem description

1.2.1 Motivation for Risk Management

Traditional network security has a static approach towards defense. Risk Management on the other hand analyzes threats, evaluated and graded threats according to the principles stipulated by risk management [GUSTH00]. Traditional security leads to static defense mechanisms such as firewalls and Virtual Private Networks (VPN) with static rules that clearly dictate which network traffic is allowed and which is not. This is regardless of the generation [CISSP] of the firewall technology as firewalls are based on the concept of clear boundaries between an inside of a network and an outside that contain the threats towards the network. In today's complex and integrated network world the concept of a clear boundary is no longer relevant. The defense mechanisms must therefore be concentrated elsewhere.

Modern networks are extremely dynamic. By this I mean that the networks aren't based on just one protocol nor does the network only allow single protocols to access the networks such as only HTTP traffic through a single access point. Instead the modern

networks allows virtually any protocol to flow freely through the network and there aren't any single access points from the network to other networks any longer (modems access other networks from inside the network as does VPN connections). There also exist a multitude of different network architectures (autonomous, add hoc or sensor networks for example).

Network integration is also a major problem in today's networks where the boundaries between networks are slowly eradicated. Modern networks are tightly integrated to Internet, supplier/contractor networks and customer networks and so on. Between theses networks there traditionally doesn't exist any, or limited protection. The consequence of this tightly coupled integration is often that if one organization is struck by an incident, the incident spreads to the other integrated organizations. There exists a need for protection and supervision inside and between organizations.

Another downside to perimeter defenses is the fact that encryption is becoming more and more popular today. Even in advanced generation four firewalls [CISSP] which have a proxy function called statefull inspection; of all the packages that flow through the firewall, the statefull inspection is hindered by encryption as the network packages makes no sense to the state full inspection. **This theses call for a more dynamic approach to network defense**. I call this approach Intrusion Management.

1.2.2 Motivation for OODA-loop

The OODA-loop is a military strategy used to describe conflicts or strategies that deal with the types of conflicts that go under the names "fourth generation warfare", "low intensity warfare", or as favored by the American strategist and inventor of the OODA-loop, Col. John R. Boyd "highly irregular warfare" [BOYD86] [MTP00]. The purpose of the OODA-loop is to gain information superiority, that is to have a thought out and agreed upon strategy on how to handle a problem before your enemy does resulting in information superiority. Information superiority can be defined in a number of ways. The simplest definition could be: "the capability to collect, process, disseminate an uninterrupted flow of information, while exploiting or denying an adversary's ability to do the same"[JCF96].

The Swedish military's definition according to a doctrine document specifying Information Operations (IO) is: "Information superiority over an adversary is a matter of success. Information superiority is obtained by gathering and analyzing information, protection of one's own information gathering process and to hinder other party's information gathering processes. Information superiority is not a static condition; it is created, exists and disappears locally over both time and space. Actions demands reactions; in an everlasting lapse of time."[FMVIO]

The American counterpart's definition is: "Information superiority, a condition that allows commanders to seize, retain, and exploit the initiative. It facilitates more effective decision making and faster execution. IO involve constant efforts to deny adversaries the ability to detect and respond to friendly operations, while simultaneously retaining and enhancing friendly force freedom of action. When expeditiously exploited, IO provide a potent advantage that facilitates rapid military success with minimal casualties. Effective IO and information management allow commanders to take advantage of opportunities, while denying adversary commanders the information needed to make timely and accurate decisions or leading them to make decisions favorable to friendly forces."

[DOA03]

1.2.3 Problem description

The purpose of this thesis is to present a method of combining the information advantage strategies from the OODA-loop, Information Operation, and Information Warfare with the risk management dynamic way of treating information security. The potential gains for information security are:

- Cost effectiveness
- Dynamic protection, in terms of configurations and mechanism
- Better equipped protection mechanisms compared to today's static protection
- Information superiority regarding to information operation/warfare

1.3 Structure of the paper

The first part of the paper is an introduction to the subject with motivation. The next part of the paper describes the methodology and the theory behind Intrusion Management. The last part of the paper describes the merge of risk management with the OODA-loop.

1.4 Delimitations

The delimitations regarding this thesis are foremost the depth and detail in which this thesis has been pursued. Adjacent field handled in this thesis such as network theory concerning the different networks discussed within this theses are not described in greater detail as they are not directly concerned with security. This means that prerequisite services such as communication between components, integrity of the information is guaranteed, and that all parties are controlled by access control mechanisms, are assumed to be in place.

The depth of the thesis is limited as far as architecture, policy and rules, and design is concerned by the fact that the theories are submitted as general theories and not dependent on the underlying technical architecture. The specific security mechanisms used to protect the fictive company is also pointless and will only result in a complex discussion based on personal preferences instead of keeping the overall goal in focus; the merger between risk management and information operations strategies (and the OODA-loop).

Decision Support algorithms or search methods are also not discussed, although important to the overall functionality if the Intrusion Management system it has no immediate implication on the security issues that this thesis is based upon.

2 Methodology

I have chosen to use exploratory research as my research methodology because a problem has not been clearly defined. Exploratory research helps determine the best research design, data collection method and selection of subjects. As I have used exploratory research as my methodology and as such used work performed by secondary researchers (such as reviewing available literature and/or data, research conferences or qualitative approaches such as informal discussions with purchasers, colleagues, friends, and management) have been the methodology used.

This thesis is based on previous work commenced by FMV in a project that has as a goal to secure "Network Based Defense" strategy and implementation, NBD. This work started during 2004 and is continuing today with a theory validation phase and will move on to an implementation phase once the validation has been confirmed. The validation is performed by other people than the theory workgroup. My assignment was to specify a Risk Management approach to Intrusion Management. This was performed by studying literature and research within various fields in order to create a hypothetical defense strategy for NBD. An effort was also made analyzing national and international laws, regulation and standards.

Adjacent work has been performed regarding IT weapon taxonomy, IDS technology evaluation, and linkage/integration to international military Command and Control systems (NATO) by WM-data, FOI, AerotechTelub and Ericsson Microwave Systems.

I would like to thank the following people for their input and support: Dan Gorton at Handelsbanken, Stefan Burström at Ericsson Microwave Systems, Martin Karresand at FOI, Krister Gustavsson at FMV, Ola Flygt at VXU.

The work is loosely based on multiple reports authored by me to FMV, and the design in this thesis bears very little resemblance to the delivered design to FMV.

3 Theory

I have made a literature study in the field of network theory, information security, information operations, information warfare, intrusion detection theory and military strategy in order to combine these theories into a defense methodology. This literature study was conducted through search engines on the Internet as well as in books and discussions with colleagues.

3.1 What can network security learn from military history

As stated by Bruce Schneier [SCHNCR] “Military strategists call it “the position of the interior.” The defender has to defend against every possible attack. The attacker, on the other hand, only has to choose one attack, and he can concentrate his forces on that one attack. This puts the attacker at a natural advantage. Despite this, in almost every sort of warfare the attacker is at a disadvantage. More people are required to attack a city (or castle, or house, or foxhole) than are required to defend it. The ratios change over history - the defense's enormous advantage in WW I trench warfare lessened with the advent of the WW II blitzkrieg, for example -- but the basic truth remains: all other things being equal, the military defender has a considerable advantage over the attacker.

This has never been true on the Internet. There, the attacker has an advantage. He can choose when and how to attack. He knows what particular products the defender is using (or even if he doesn't, it usually is one of a small handful of possibilities). The defender is forced to constantly upgrade his system to eliminate new vulnerabilities and watch every possible attack, and he can still get whacked when an attacker tries something new...or exploits a new weakness that can't easily be patched. The position of the interior is a difficult position indeed.

A student of military history might be tempted to look at the Internet and wonder: "What is it about warfare in the real world that aids the defender, and can it apply to network security?"

Good question. The defender's military advantage comes from two broad strengths: the ability to quickly react to an attack, and the ability to control the terrain.

The first strength is probably the most important; a defender can more quickly shift forces to resupply existing forces, shore up defense where it is needed, and counterattack. I've written extensively about how this applies to computer security: how detection and response are critical, the need for trained experts to quickly analyze and react to attacks, and the importance of vigilance.

The defender's second strength also gives him a strong advantage. He has better knowledge of the terrain: where the good hiding places are, where the mountain passes are, how to sneak through the caves. This provides the defender with an enormous advantage. He can modify the terrain: building castles or surface-to-air missile batteries, digging trenches or tunnels, erecting guard towers or pillboxes. And he can choose the terrain on which to stand and defend: behind the stone wall, atop the hill, on the far side of the bridge, in the dense jungle. The defender can use terrain to his maximum advantage; the attacker is stuck with whatever terrain he is forced to traverse.

On the Internet, this second advantage is one that network defenders seldom take advantage of: knowledge of the network. The network administrator knows exactly how his network is built (or, at least, he should), what it is supposed to do, and how it is

supposed to do it. Any attacker except a knowledgeable insider has no choice but to stumble around, trying this and that, trying to figure out what's where and who's connected to whom. And it's about time we exploited this advantage. Think about burglar alarms. The reason they work is that the attacker doesn't know they're there. He might successfully bypass a door lock, or sneak in through a second-story window, but he doesn't know that there is a pressure plate under this particular rug, or an electric eye across this particular doorway. McGyver-like antics aside, any burglar wandering through a well-alarmed building is guaranteed to trip something sooner or later.

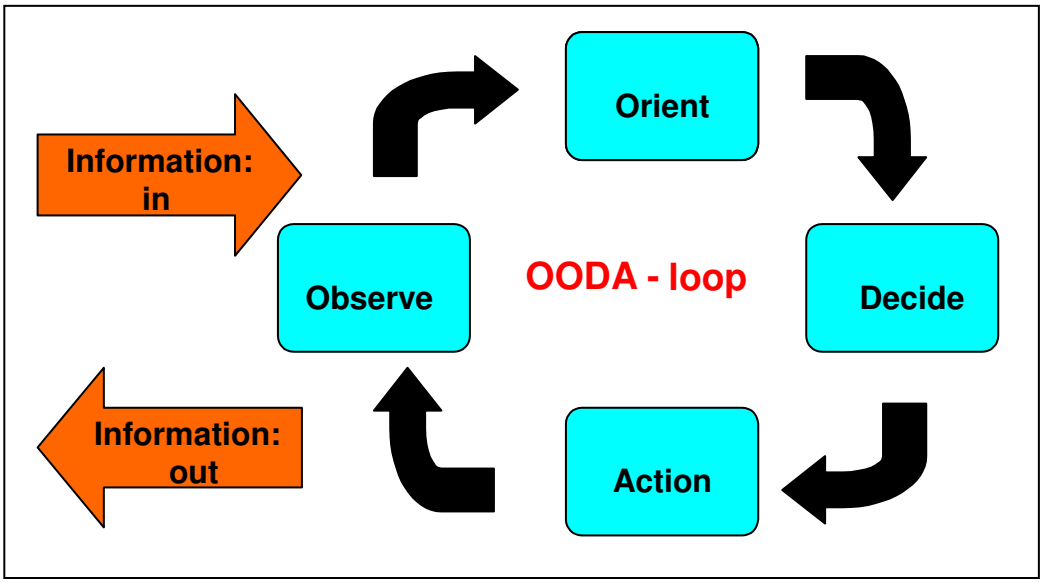
Traditional computer security has been static: install a firewall, configure a PKI, add access-control measures, and you're done. Real security is dynamic. The defense has to be continuously vigilant, always ready for the attack. The defense has to be able to detect attacks quickly, before serious damage is done. And the defense has to be able to respond to attacks effectively, repelling the attacker and restoring order.

This kind of defense is possible in computer networks. It starts with effective sensors: firewalls, well-audited servers and routers, intrusion-detection products, network burglar alarms. But it also includes people: trained security experts that can quickly separate the false alarms from the real attacks, and who know how to respond. This is security through process. This is security that recognizes that human intelligence is vital for a strong defense, and that automatic software programs just don't cut it.

It's a military axiom that eventually a determined attacker can defeat any static defense. In World War II, the British flew out to engage the Luftwaffe, in contrast to the French who waited to meet the Wehrmacht at the Maginot Line. The ability to react quickly to an attack, and intimate knowledge of the terrain: these are the advantages the position of the interior brings. A good general knows how to take advantage of them, and they're what we need to leverage effectively for computer security."

3.2 Introduction to the OODA-loop

The OODA-loop can be described as a process containing four mayor blocks; *observe-*, *orient-*, *decide-* and *action*.



Picture 3.1: Description of the four blocks in the Security Management process

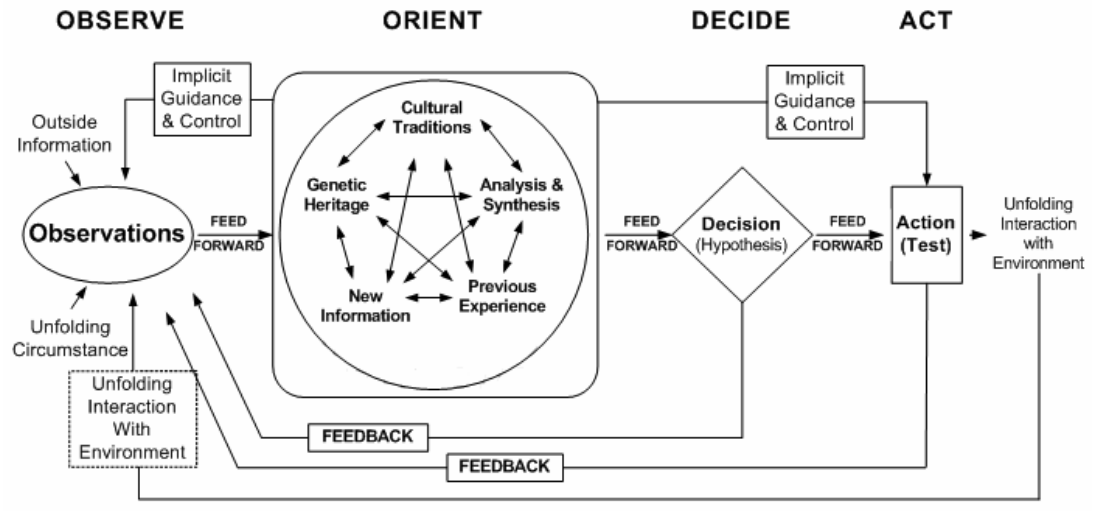
The OODA-loop has the responsibility to *detect* threats towards confidentiality, integrity, and availability. The Intrusion Management system also has to be able to take *actions* in order to eliminate, restrict or prevent incidents before they occur, fast enough and to a predefined acceptable (or risk evaluated) level before these threats pose a serious threat towards the organization.

The Intrusion Management system must have the capability to (amongst other things):

1 Identify penetration attempts, fraud, and conscious interruptions towards the availability of services
2 Plan and realize measures in order to eliminate or minimize damage
3 Plan, implement, risk evaluate defenses for new threats (for example: vulnerabilities, not installed patches or hot-fixes, virus, trojans, and worms) reported from both internal and external threat organizations such as CIRT, CERT or intelligence agencies.
4 Capability to proactive plan and increase the security level based on a risk evaluation.
5 Create a foundation for a risk analyses and decisions regarding information security and the capability to guarantee function to uphold confidentiality, integrity, and availability to a predefined risk evaluated, and agreed upon level.
6 Create and assist with information gathering to information operations and information warfare (business intelligence).
7 The capability to perform and risk evaluate decisions regarding both technical and organizational issues.

The OODA-loop is not a cyclic loop such as the Demming wheel [DEMM] of "PDCA" of quality, for an example. The Observe-Orient part of the loop is continuous all the time, as is the Decide-Act phase if needed. It does not have to be a perfect cyclic course of events.

The OODA-loop in detail reveals a more complex model [CWR03]:



Picture 3.2: Description of the OODA-loop in grater detail

Observe and orient: The observation is made without prejudice. The object that is observed is interpreted based on the interpreter's mental state (upbringing, culture, education, experience, ethics/moral, etc), that is once orientation. The orientation decides what is observed. The observed object is also expected to be in constant change. The orientation is an adaptation to the observed reality. What is observed depends on the orientation, new information, and an analysis and synthesis of the environment (to see what can't be seen with the naked eye). According to http://www.belisarius.com/ "In order to accept a model, the present mental model must be given up and destroyed in order to accept a new model"

Decide and Act: A decision is made based on a hypothesis of the observed reality and expected future development. Actions therefore change the observed reality and as a consequence our observation.

On a more practical level, in order to support the intended information security capabilities, we need to introduce a decision support system and capabilities to take and drive decisions fast enough. Decisions have to be made in co- ordinance with other interested parties because the decision can have devastating consequences for the overall functionality and availability. The visibility to se what consequences a decision can have for the functionality is very important and needs to be simulated and trained.

The speed in which decisions are handled can be improved by introducing automation. Automation has the ability to speed up the time for the decision but is a sword of Damocles [DEMOC]. Too much automation can lead to a pre defined decision based on the automation logic. Instead the automation logic should firstly be used to control defense mechanism configuration level in order to implement quick system changes. The upside of automation is that decisions can be made locally. The expected network load and processing power in the Intrusion Management system is not negligible in a large system.

4 Intrusion Management

4.1 Overall description of protection needs

Intrusion Management will demand new strategies for handling confidentiality, (integrity) and availability. Current strategies are based on a world where Intrusion Management system have contained and dedicated systems, and where the security strategies are based upon the two fundamental security strategies: *to minimize the exposures to threats and containment of information* (both logical and physical). Intrusion Management works in an environment concept of service oriented networking, and multiple network architectures, where completely new and different security protection is needed.

Service oriented networking means different things to different people, based on their own background and experience. In this concept, service oriented networking is defined by two primitives; service orientation or based, and real-time networking. The information will be distributed and available to anyone who needs the particular piece of information in order to solve a dedicated task. The new protection needed within the Risk Management process is largely based upon logical protection and the complemented physical protection, is therefore down prioritised within the scope of this document. The physical protection is as important as the logical protection but is not explored within the scope of this thesis.

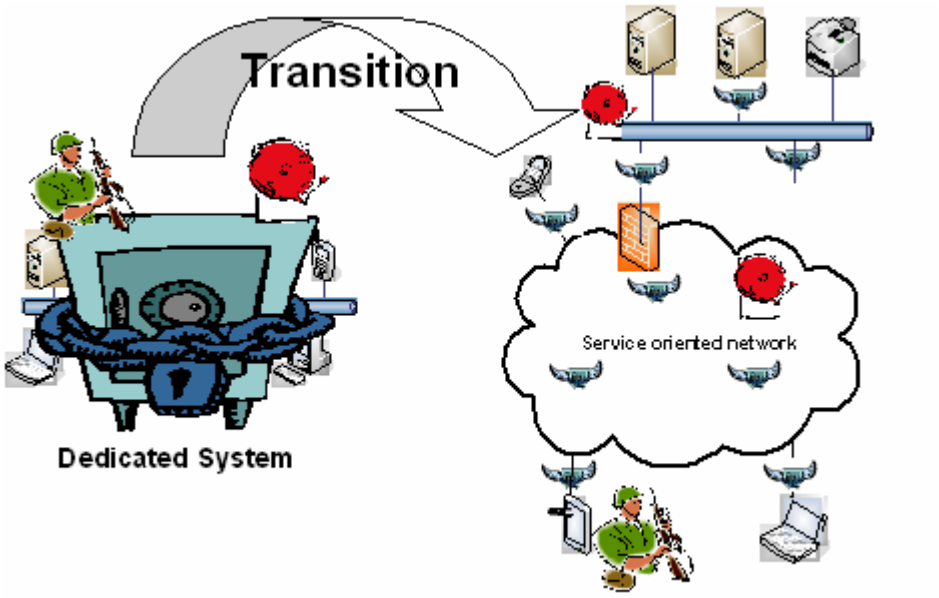


Figure 4.1: Picture describing the transition between a dedicated system to a service oriented network.

Figure 1 shows how a designer should look upon a service oriented network, specifically looking at security issues. The system and its protection moves from a contained and dedicated source out into a network where the system is just one of all the systems within the network and should be available to anyone in need of the systems, at any time and at any place. The information flows “freely” between different services in

the network and the protection strategy is to look upon the information protection value as “small information safes” flowing inside the network, instead of a large safe protecting the whole network.

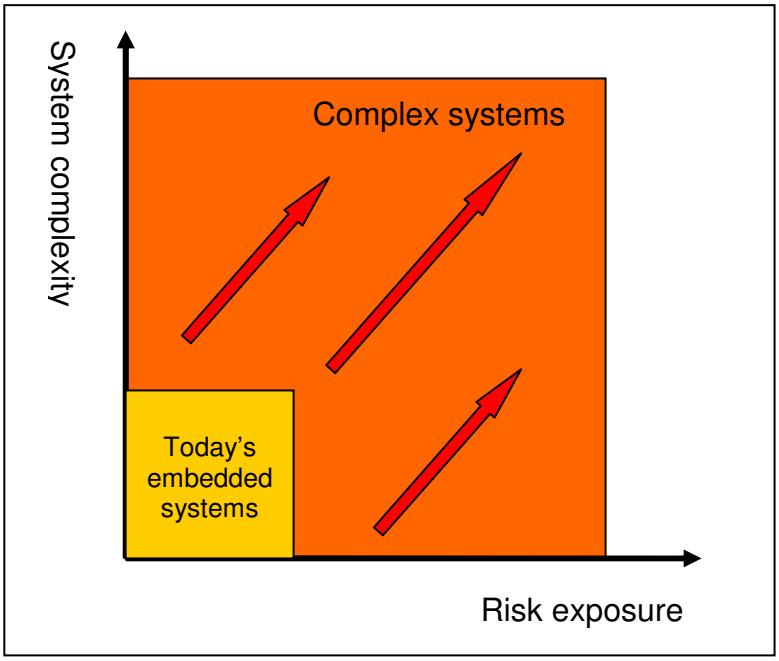


Figure 4.2: This picture describes the area of risk exposure between today’s embedded systems with a small area of exposure compared to Intrusion Management with a large are of exposure.

A comparison between physical protection and logical protection isn’t always obvious, most of the time both types of protection are required. In a service oriented network most of the protection will be based on the logical aspect of security because of the downgraded importance of physicality and locality. The type of protection needed is based upon a proportion between the threats and the risk of damage, which combined in a risk assessment, will result in the most cost effective and best suited protection for the task.

4.1.1 Risks

In order to discuss Risk Management as a process one has to look at risks and categorize them into understandable groups. IT risks are made up of threats that utilize vulnerabilities in IT systems that lead to an exposure in the IT system.
Risks, according to an adoption of Gustav Hamilton theories, can be calculated out of:
Total risk = Threat x Vulnerability x Asset value [GUSTH00]

Faced with risk, organizations have four basic choices regarding protection strategy:

- Terminate the activity that causes the risk increase
- Transfer the risk to another party (i.e. insurance)
- Reduce the risk by the use of appropriate control measures or mechanisms
- Accept the risk

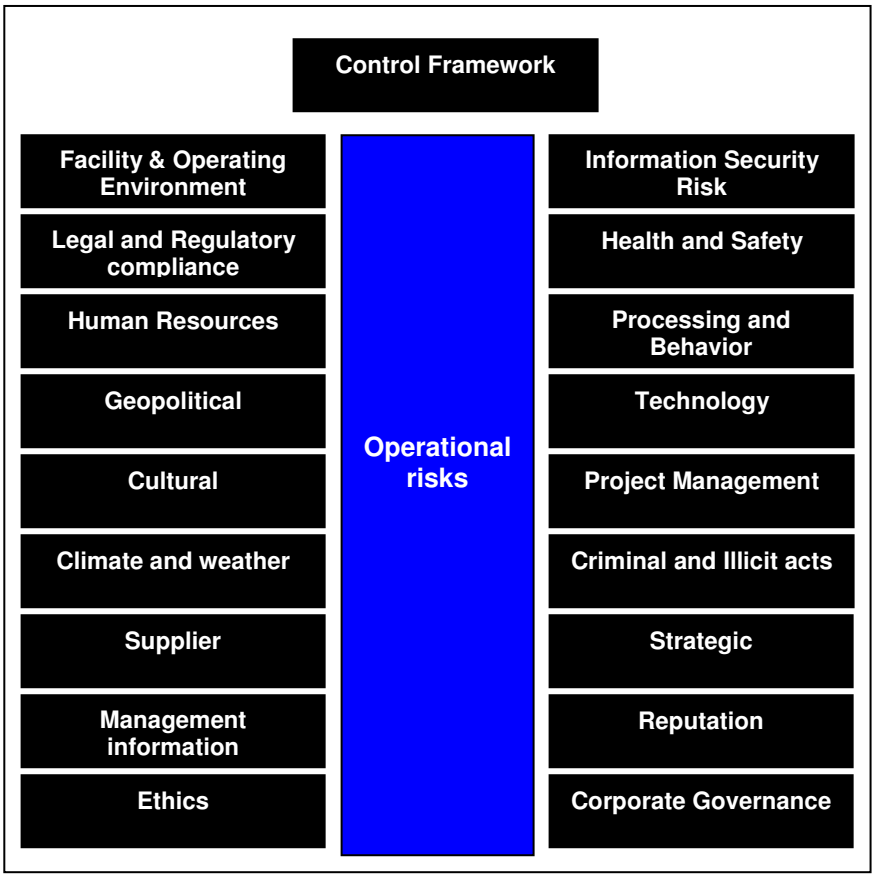


Figure 4.3: Picture describing organizations different risk areas, based on part of the WM-data risk management model. The model is an attempt to categorize different threats into different groups in order to try to create similar solutions (to minimize or remove the threat) to a group of threats

4.1.2 Risk Management

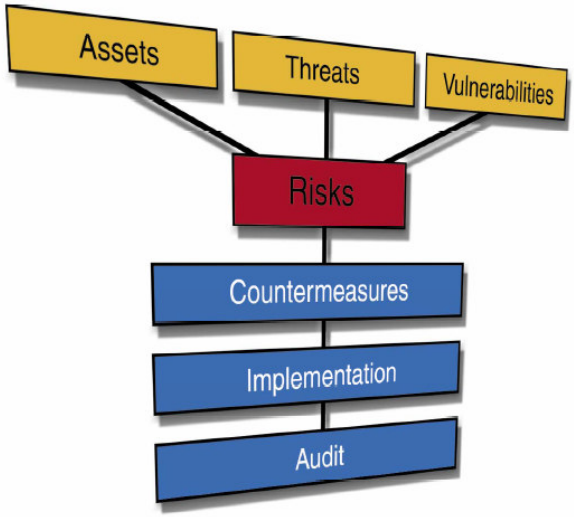


Figure 4.4: Picture describing the overall Risk Management process. The Assets are exposed to a number of threats that leads to system vulnerabilities. All of this categorized as Risks. When the risk has been analyzed countermeasures to minimize or eliminate the exposure should be implemented and audited for effectiveness. Implementation of course does not only mean technical countermeasures but also administrative, and organizational.

Risk assessment is nothing new [GUSTH00], but the Intrusion Management architecture in it self raises the demands based on the objective operation in order to support the business objectives with adequate functionality and an adequate security level. Risk Management is not a new concept in any line of business. Risk Management has been used in many different contexts (for example accreditation, financial risk calculations or for insurance purposes, just to name a few) but has historically been used mainly in a pre-emptive way. Risk Management is used beforehand, in order to identify and quantify different threats.

The challenge proposed is to use Risk Management in real time over a much grander scale.

A direct effect on risk management within any field is the grand scale of Intrusion Management in it self. The risk management process will encompass everything within Intrusion Management and therefore become a large process in it self. It is most likely that not all components in a complex system such as Intrusion Management will be evaluated theoretically as plausible safe or secure. The Intrusion Management system will complement the evaluation by subjecting a good foundation for the risk evaluation process. This is done by offering tools for reducing risks and damage. A decision support system for guiding and helping in the decisions needed in order to be effective within the security area is also needed.

Under operational support, the Decision Support System (DSS) needs to be constantly aware of its own operational abilities and availability. This is in order to be constantly aware of all abilities that are accessible to the Intrusion Management system over both time and space. This doesn't necessary mean only network based abilities such as CND, CNR, CNE or CNA (Computer Network :Defense, Response, Exploitation, and Attack) [DOD36001], but also business operational abilities, environment issues and safety. These abilities are governed by different policies, rules and regulations. Abilities do not only have to realm within the business or operational environment but can also be within the public sphere such as fire brigade, medical or the police service. Intrusion Management functionality will therefore vary depending on the state of the alerts (compared to the US military's DEFCON-levels that define the state of emergency; DEFense CONditions).

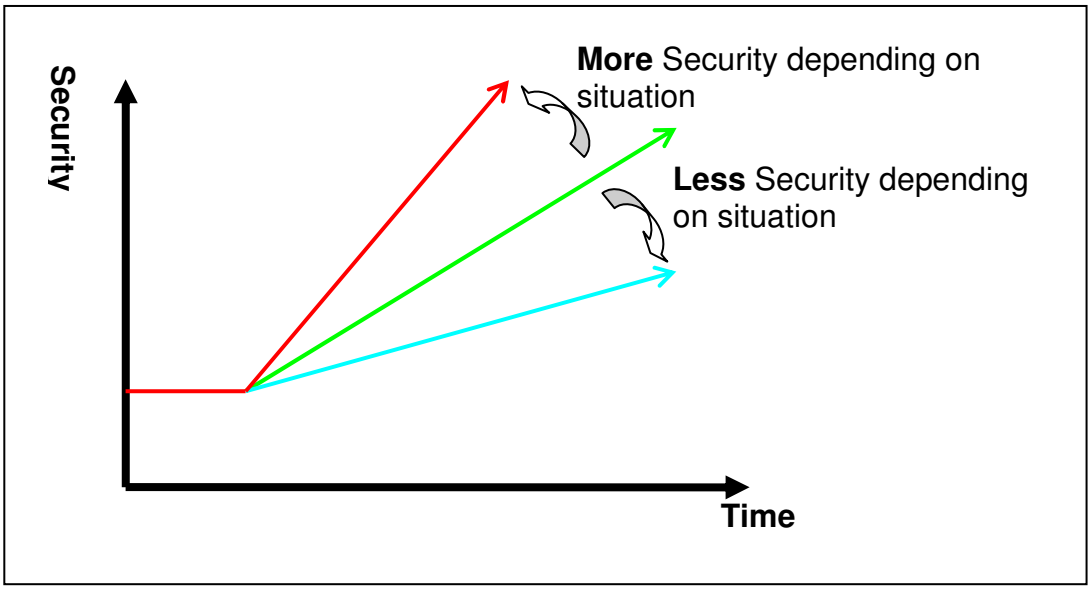


Figure 4.5: Picture depicting the different security levels needed in a dynamic system depending on time and Security emergency levels (DEFCON).

4.1.3 Competence within Intrusion Management

The Risk Management process is not only technical in its nature but on the contrary, demands specific competences, routines, rules and regulations in order to secure the correct competence of Intrusion Management and the right to swiftly make decisions as time is a critical factor. The Risk Management process is depending on: technology, processes and organization, as do most other management processes. These three fundamental requirements will be given different importance depending on the time and situation. As an example, the Risk Management system will never be delivered in a complete state. In fact the Risk Management system will never be completed as it has to evolve and change constantly, over time in order to be as effective as possible and to reflect changes in technology, organization and challenge.

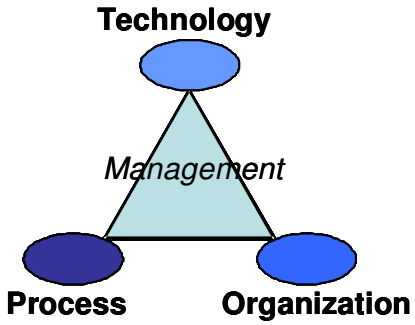


Figure 4.6: The Systems & Security Management tripod

Different competences, and a very basic description of their needed to support to the Risk Management process are among others:

- Executive in charge of the decision making process, a highly competent person to make decisions based on protection needs and objectives

- Manager in charge of business objectives and strategy, to manage and prioritize the business objectives
- Business Intelligence personnel, to support the decision making process with business intelligence analyses
- Configuration and Quality Management, to manage and prioritize configurations and quality of Intrusion Management system in an ever changing environment.
- Information Security Management, to manage and prioritize security issues in the business.
- System Security specialists, to manage and prioritize specific systems that might be vital, or not to the objectives
- Social scientists/sociologist, to manage and analyze social issues regarding different alternatives before a decision
- Network and systems specialists, to analyze and prioritize changes to the network and systems
- Developers, to analyze and input system development issues
- Penetration testers, to analyze and give expert advice on vulnerabilities and risk
- Statistical competence (anomaly analyst) to support the decision making with statistics
- Simulation experts, in order to support the decision making with possible scenario outcomes
- Contemporary social and environmental expert, in order to analyse outcome of decisions based on the consequences for the world around us

The decision making process within Risk Management is the core complexity of the Risk Management process of the Intrusion Management system. Input to the Risk Management process is not only limited to the business objective but dependent on relevant input from a global perspective.

The executive in charge of the decision making within Risk Management will have to prioritize between all different inputs which demand a very broad understanding from a very diverse field of different inputs. The prioritization and decision making will indeed demand a lot from the executive in charge as information overload is a very possible threat. Technical support systems will ease the decision process but is limited in its ability to support the executive.

4.1.4 Rapid information reclassification

In today's dedicated systems information classification decisions based on prioritization, confidentiality, integrity, and availability is possible. These classifications are in turn based on legislation, policies, guidelines and common sense. The person responsible for creating the particular piece of information is trusted to make the classification decision based on the fact that that person can make an intuitive guess about; one who will need to access the information in the future and why, and two the actual threats towards the information. The security protection is then implemented into the technical system.

Because of service orientation; on demand and real-time networking, the Intrusion Management system must be able to reclassify information very fast, because of the

complexity of analyzing the information need for a particular piece of information. In fact the Intrusion Management system must be able to reclassify the information as fast as a particular user needs the information, because this information demand from the user can be critical in order to accomplish the business objective. It will be impossible to build security protection that protects the information regardless of the classification and the physical locality of the users demanding it, **therefore the need for Risk Management and rapid reclassification is vital in service oriented networks**.
Another problem with information classification in the Intrusion Management system is the initial classification. When a user is faced with a classification decision an intuitive decision about who the receiving users are and where they might be (both physically and over time) just isn't possible.

Strategies and proposed algorithms regarding rapid reclassification based on risk analysis can be found in recent intrusion detection research [JVA04].

4.1.5 Risk Management and Policy development

One of the greatest benefits of Risk Management is the fact that it supports a small static core of information security policy, with complementing guidelines and rules if needed. Risk Management enables every document to be more specific and thus create a security baseline for the business objective (security baselines define the lowest level of information security demands for an organization, defined by ISACA in CISM Review Manual 2005). The policy and control documentation could be kept small, concrete and specific as to avoid confusion and the Risk Management system could automatically handle all security matters not specified in the policy thus creating a dynamic approach to information security. This means that the Intrusion Management system should be able to get feedback regarding the status of the security safeguards covering everything from usefulness, integrity, safety, and costs to name just a few benefits. This will lead to better (faster and more cost effective) overall management controls.

4.1.6 Risk Treatment

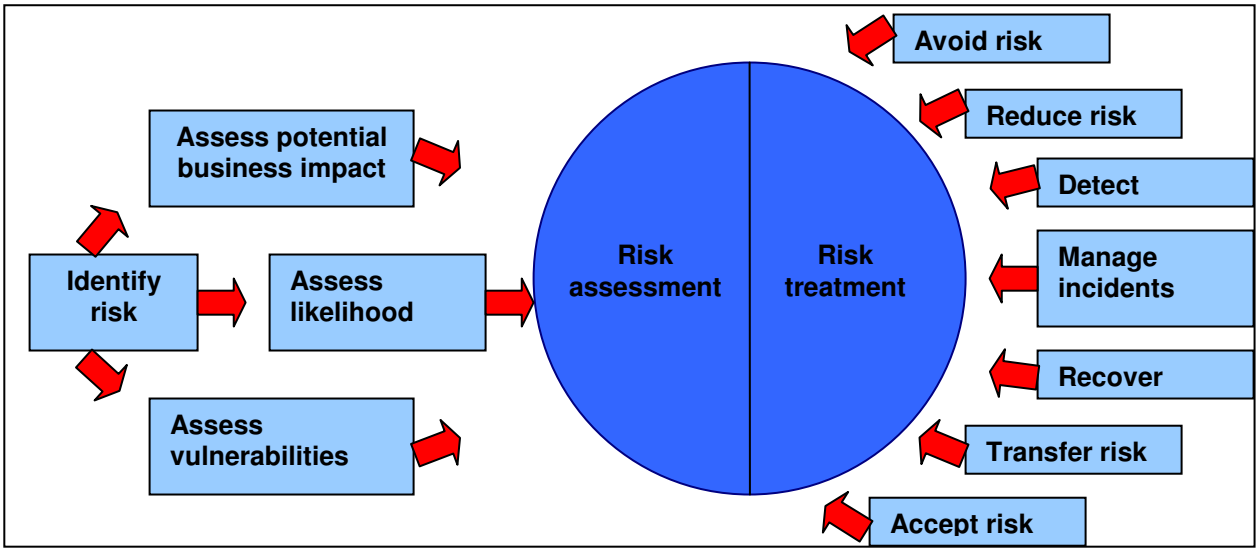


Figure 4.7: Picture showing different treatments to risk [AS\NZS]

Once risk has been identified, existing countermeasure can be evaluated or new

countermeasures are designed to reduce vulnerabilities to an acceptable level of risk. Controls can then be evaluated to determine if the countermeasures are effective. Countermeasures can be actions, devices, procedures, or techniques. Controls can be any combination of element that provides assurance of the effect of the countermeasures. The strength of a control can be measured in term of its inherent or design strength and the likelihood of its effectiveness.

Risk Management is a continuous and dynamic process to ensure that changing threats and vulnerabilities are addressed in a timely manner.

Formalized risk mitigation strategies exist within the methods and standards that exist covering Risk Management [AS\NZS].

5 Description of the Risk Management process

The Risk Management process can be described in many ways and in varying detail. In this thesis the Australian and New Zealand standard called AS\NZS 4360:2004 is chosen, as it will likely be the future international Risk Management standard.

On a high abstraction level the Risk Management process is divided into three major parts concerned in the **Risk Assessment process**. These three steps are:

- Identifying Risk
- Analyzing Risk
- Evaluating Risk

In practical implementations a fourth step is usually included, the Risk Treatment step, that makes up a complete process.

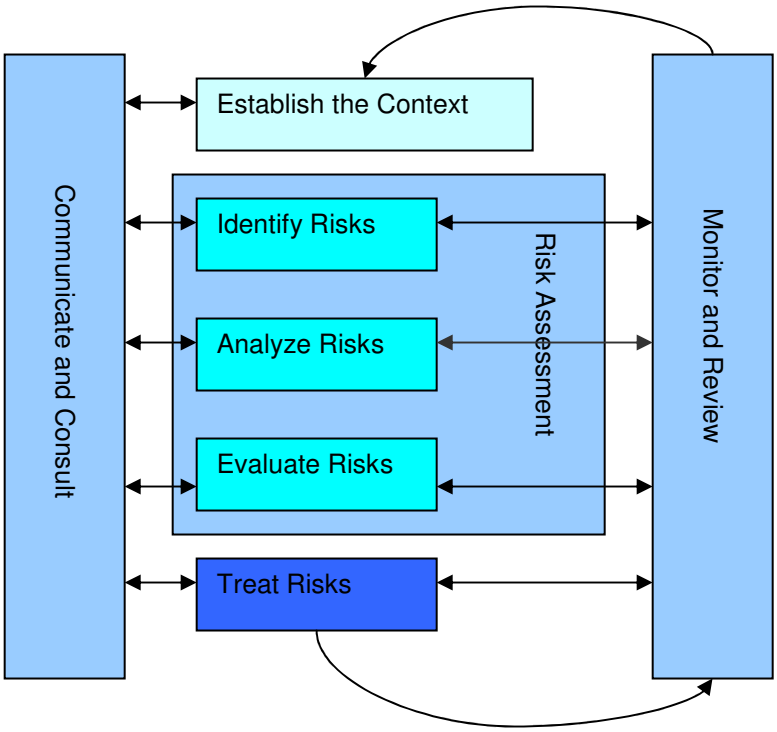


Figure 5.1: Picture describing the Risk Management Process at a high level.

Preceding the process an establishment of the context for the process has to take place and two supporting functions are usually added that work throughout the whole process. A Monitoring and Review function has to ensure that the management plans are constantly relevant. The other function is the Communication and Consult function that ensure that all the interested parties engaged in the process understand the basis on which decisions are made and why particular actions are required.

5.1 Establish the Context

Establishing the context defines the basic parameters within which risks must be managed and sets the scope for the rest of the management process. The context includes the organization's external and internal environment and the purpose of the risk

management activity.

Establishing the context is concerned with understanding the background of the organization and its risks, scoping the risk management activities being undertaken and developing a structure for the risk management tasks to follow. This step is needed in order to:

- Clarify the organizational objectives
- Identify the environment in which objectives are pursued
- Specify the main scope and objectives for risk management, boundary conditions and the outcomes required

5.2 Identify the Risks

This step seeks to identify the risks to be managed. Comprehensive identification using a well structured systematic process is critical because a risk not identified at this stage may be excluded from further analysis. A risk is associated with:

- A source of risk or hazard
- An event or incident
- A consequence
- A cause for the risk or hazard
- Controls and the level of effectiveness
- When and where could the risk occur

5.3 Analyze the Risks

Risk Analysis is about developing an understanding of the level of the risk and its nature. It provides an input to decisions on whether risks need to be treated and the most appropriate and cost-effective risk treatment strategies. Risk analysis involves consideration of the source of risk, their positive and negative consequences and the likelihood that those consequences may occur. Risk is then analysed by combining consequences and their likelihood.

The process of analysis will often commence with a simple qualitative approach that gives a general understanding. Where greater detail or understanding is required, more focused and robust investigation may be needed. It is inappropriate to assume that qualitative is superior to quantitative analysis. There is a multitude of analysis types available including, but not limited to:

5.3.1 Qualitative

Qualitative analysis uses words to describe the magnitude of potential consequences and the likelihood that those consequences will occur. These scales can be adapted or adjusted to suit the circumstances, and different descriptions may be used for different risks.

Qualitative risk valuation methods are judgmental or qualitative in its nature. Independent decisions are made based upon business knowledge, executive management directives, historical perspectives, business goals and environmental factors.

Qualitative analysis may be used:

- as an initial screening activity to identify risks which require more detailed

analysis;

- where this kind of analysis is appropriate for decisions; or
- where the numerical data or resources are inadequate for a quantitative analysis.

5.3.2 Semi-qualitative

In semi-quantitative analysis, qualitative scales such as those described in Qualitative analysis are given values. The objective is to produce a more expanded ranking scale than is usually achieved in qualitative analysis, not to suggest realistic values for risk such is attempted in quantitative analysis. However, since the value allocated to each description may not bear an accurate relationship to the actual magnitude of consequences or likelihood, the numbers should only be combined using a formula that recognizes the limitations of the kinds of scales used.

Care must be taken with the use of semi-quantitative analysis because the numbers chosen may not properly reflect relativities and this can lead to inconsistent, anomalous or inappropriate outcomes. Semi-quantitative analysis may not differentiate properly between risks, particularly when either consequences or likelihood are extreme.

5.3.3 Quantitative

Quantitative analysis uses numerical values for both consequences and likelihood using data from a variety of sources. The quality of the analysis depends on the accuracy and completeness of the numerical values and the validity of the models used. Quantitative risk analysis is therefore considered more precise but at the same time more complex [ISACA05].

Consequences may be determined by modelling the outcomes of an event or set of events, or by extrapolation from experimental studies or past data. Consequences may be expressed in terms of monetary, technical or human impact criteria, or any of the other criteria. In some cases, more than one numerical value is required to specify consequences for different times, places, groups or situations.

5.4 Evaluate the Risks

The purpose of risk evaluation is to make decisions, based on the outcome of risk analysis, about which risks need treatment and treatment priorities. Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. The objective of the organization and extent of opportunity that could result should be considered.

In some circumstances, the risk evaluation may lead to a decision to undertake further analysis.

5.5 Treat the Risks

Risk treatment involves identifying the range of options for treating risks, assessing these options and the preparation and implementation of treatment plans. Risk can have both negative and positive outcomes. The treatments must be able to handle both opportunities and negative outcomes. Options for risk treatment includes, among other plausible options:

- Avoidance of the risk
- Changing the likelihood of the risk

- Changing the consequences of the risk
- Sharing the risk
- Retaining the risk

6 External requirements

The Risk Management process (including the Decision Support System - DSS) needs to be fed a lot of input information from the rest of the Security Management process (identification, collection and analysis-phase) and other services in order to make sensible risk assessments and decisions. Additional contribution of information sources is probably also needed in order to make assessments or decisions as correct as possible. Additional information needed could be, among other tings:

- Analysis of current social and environmental issues
- Analysis of current security threats and security issues
- Business or military objectives and strategies
- The manager in charge of the Intrusion Management system
- Business intelligence information
- General SecOp information
- Public authority information; such as information from the fire brigade, medical and police services
- Media and global press

The Risk management process objectives are expected to change over time. This means that the network based services and security services are expected to change with the changing objectives. On one particular time in space availability might be the capability in demand from the network. As a new objective or changes to risk assessment decisions comes, different capabilities are in demand in the network such as integrity and safety for an example.

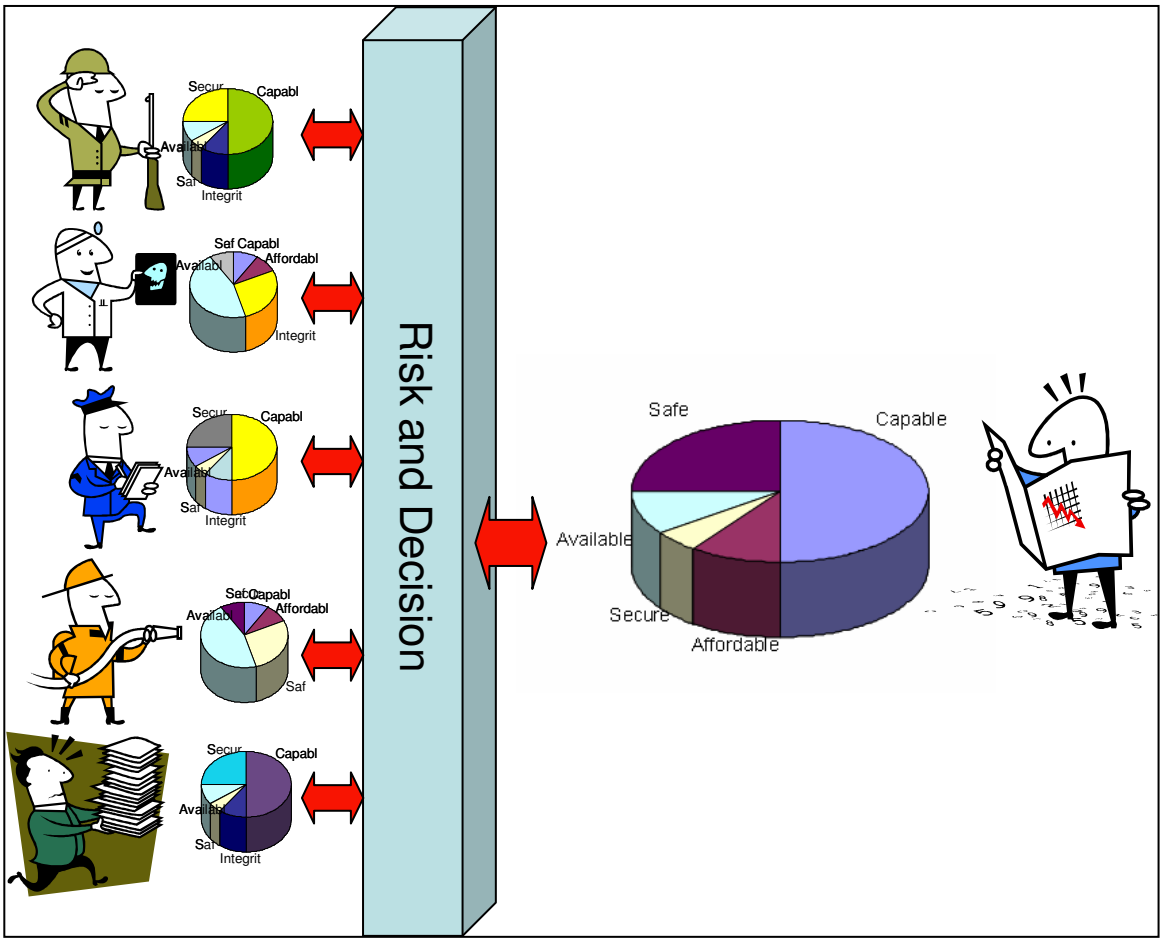
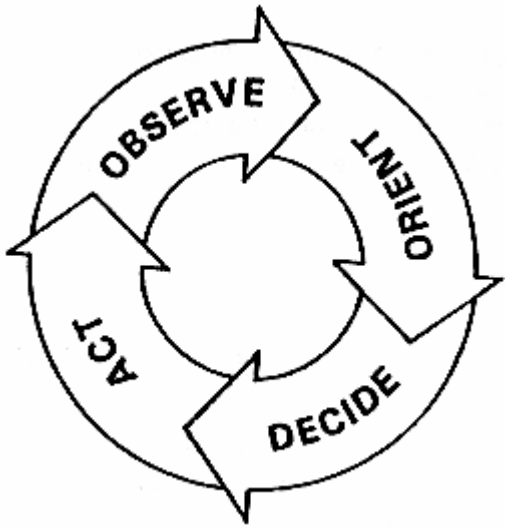


Figure 6.1: The picture describes the different needs for capability in the network as risk assessment changes or new business objectives are prioritised.

Based on all inputs sources to the Risk Management process, the decision process is very complex indeed. Considering that external sources of information are needed such as civilian agencies and business partner and even competitors, the complexity of the decision is overwhelming. All these civilian agencies and businesses all have their own agenda and therefore prioritization of the resources needed instead of prioritizing the common good. A "tragedy of the commons"[HAR68] where all the finite resources are all used up because all the individual parts in, for example competitors, are not interested in the common good for the system as a whole but instead maximizing its own gain, is an inherent risk. All different prioritizations have to be normalized and correlated in order to make them into one decision that becomes a business objective. This is especially important in times of crisis or disaster.

7 Architecture and proposed design



Picture 7.1: The OODA-loop revisited

The architecture described in this section is structured around the OODA-loop where the four distinct components of the OODA-loop are specified individually. These specifications are given as proposed method of implementing the Intrusion Management utilizing today's technology.

7.1 Observe

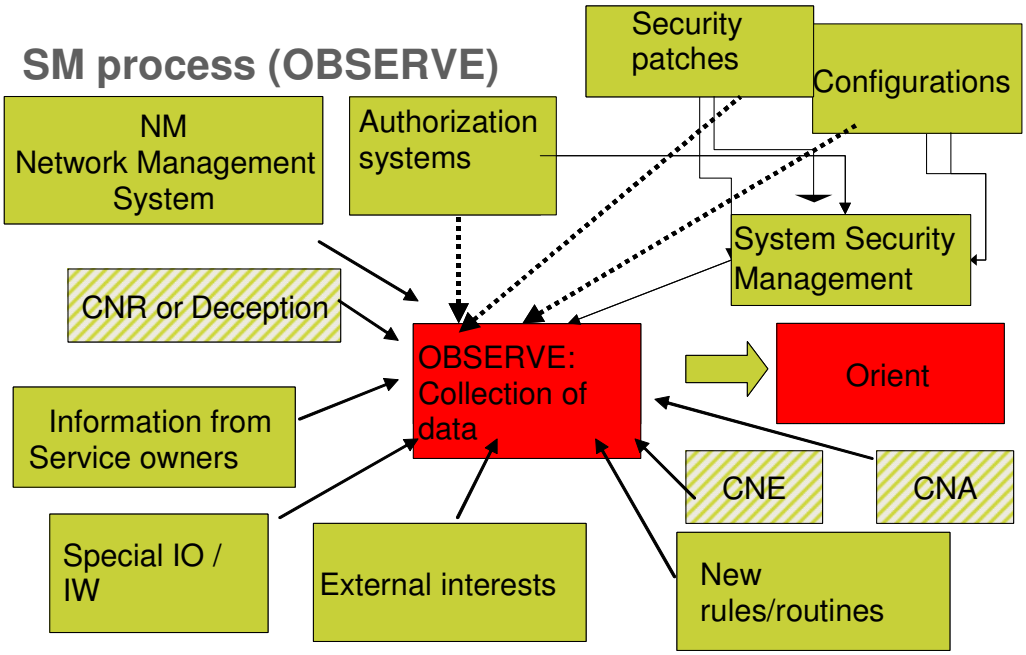


Figure 7.2: describing some of the different input sources to the Intrusion Management system

The collection of data to the Intrusion Management system serves many purposes. The collection process is both an internal and an external process. The collection process should also be able to handle single stand alone nodes in the network and collection of nodes for larger collection purposes. The collection should also be able to handle

information representatives through proxy functionality in order to transport data via alternative, or specific, dedicated encrypted connections. The reason for utilizing representatives as communication partners is that the data has to be communicated in an acceptable data format. Data also has to be collected manually and hand fed into the Intrusion Management system. There might also be a need for conversions from analogue signals to acceptable data formats. Examples of analogue signals might for instance be intelligence information that might not be available in a digital format.

The information gathering functionality has to discover encroachment or intrusions towards the system, DDOS and DOS attacks (DDOS and DOS = Distributed Denial of Service and Denial of Service attacks), attempts to affect system credibility, and also identify weaknesses to the system. The gathered information is, amongst other things, used in:

- IDS [BRACE] functionality such as sting comparisons with attack profiles and anomaly detection
- Decision basis for planning IO and IW activities (IO=Information Operations, IW=Information Warfare)
- Code integrity testing
- Command and Control systems over networks and services

The gathered information shall in itself or in combination with other information build information value that should be used for analysis and correlation (after data condensation).

A fundamental issue regarding multiple information sources is that multiple sources adds information value, and hinders an attacker to use individual system components for an attack without being discovered. The gathered information value over multiple systems is also greater than the individual parts processed individually.

7.1.1 Reasoning around the purpose of information gathering

The purpose of information gathering has many purposes and is executed through many different input sources. The information gathering, amongst other, purposes are:

- System integrity, information collection regarding code integrity testing from systems and services (applications)
- In order to created situation overviews and basis for analysis and decisions by gathering, amongst other input, network topologies, services dependencies, assignments dependencies, prioritized functionality, prioritized goals or operations in the network, network intelligence, signal intelligence, human intelligence, GPS data, logical and physical map regarding cables and telecom equipment, operator network, and routing
- Information in order to string compare and anomaly detect (that is IDS functionality) compared with general log information such as system logs, SNMP traps and logs, network traffic, routing, organization information, business assignments, authentication and authorization systems, application and service logs.
- In order to identify and localize external and internal attacks
- Identify the current threats and weaknesses towards the systems such as CERT information, SPAM information etc.

7.1.2 Reasoning regarding attack profiles versus anomaly detection

Intrusion detection focuses on attack detection. That is primarily performed by detecting attacks based on how network attacks are performed today, by using attack profiles. This paints a well defined threat picture for the information gathering process. The main problem regarding threat profiles is that it will not detect attacks that are not pre defined. This leads to situations where we won't be able to predict early warnings regarding attacks. That is we won't be able to detect attacks that haven't been pre defined and are unknown.

Traditional intrusion detection is defined and therefore limited to its operating environment. The operating environment that intrusion detection is tailored for is commercial environments and not general available environments. This means that input sources (information gathering) is tailored towards the most commercial viable input sources on the market today and this therefore where intrusion detection functions best.

This poses a threat to highly secure environments such as dynamic networks (highly movable networks created based on network functionality) where encryption is used as confidentiality functionality. This means limitation to intrusion detection functionality in networks based on peer-to-peer [PTPNET] architecture, ad hoc [LEVGJB] architecture, etc. This also means functionality limitation to the choices of services and applications viable on the commercial market today. There are however other options viable that have capabilities to support better and earlier attack detection such as systems based on historical positioning data coupled to services and physical networks.

7.1.3 Data ownership and data protection

A data ownership discussion must observe information classification, laws, rules and standards in order secure responsibility of the communicated information and the protection needs of the information. The individual information parts have meriting protection needs of themselves, but pooled information might have a higher information value than its individual parts; therefore a higher need for protection than the classified individual information parts protection needs.

7.1.4 Formats regarding gathered information

Individual systems generate information from the operating system and upwards. That is system logs and logs from services and applications. Some systems today even have predefined log and attack detection and alarms. There exist indirect system alarms such as network management systems, firewalls, routers etc. These systems have limited functionality to generate logs and alarms today already.

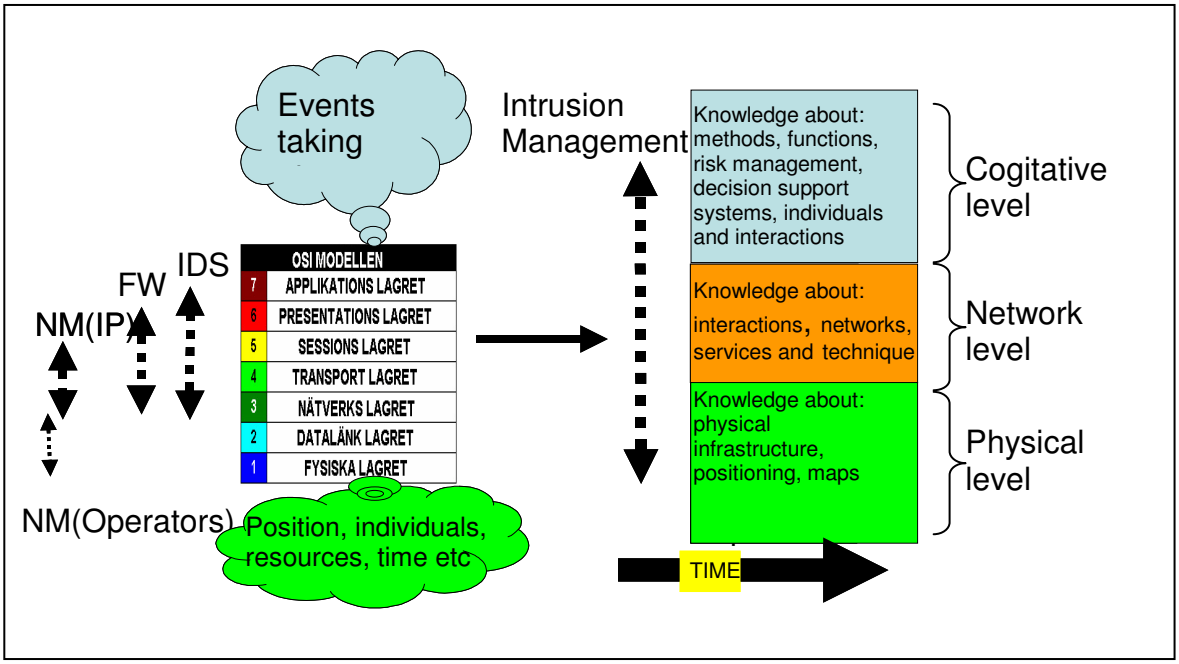
Information gathering is based on the collection of information both dynamic and on demand. In order to manage all this information in a simple and viable manner only a few information formats has to be agreed upon. This can be achieved by using broker services such as proxys for example in order to format the information into a standardized format but it also has the added value of security (that is nodes and network equipment that is administrated through a broker service and not directly over the network). The amount of information can also be minimized in order to keep the bandwidth low regarding administrative information over the network through local data condensation.

Another important format issue is the limitation regarding centralized time. Time is usually out of synch between different systems. When intrusion detection information is

correlated, synchronized time is an absolute security demand.

When regarding the information needs in order to detect an attack, the risk of only regarding information that is generated as a direct consequence of the attack is imminent. Analysis if the information regarding the point of attack is performed and with regards to this information, signatures or objects are identified to match or to find anomalies against the presumed attack. This line of reasoning only leads to part of the needed information though. This means that during an attack most of the efforts are concentrated to covering the attacker's tracks. That is to create an attack that isn't identified by the objects that are under surveillance (an attack performed "under the radar").

Asymmetric information gathering is therefore essential in order to use as much leverage as possible in order to identify an attack. Information security is not only composed of technical countermeasures but also by administrative issues, personnel issues, methods and physical countermeasures. Regarding information security as a point of reference a model consisting of three layers and a timeline can be constructed.



Picture 7.3: describes where different techniques operate in an OSI-model. The picture also describes the fact that Intrusion Management spans from the lowest levels of the OSI model up to a cogitative level.

The picture above describes a model where Intrusion Management manages to collect information from a multitude of sources, through all layers of the OSI model up to even a cognitive level. If one layer is affected by an attack, all other layers are affected as well, both over time and space. An attacker must therefore manipulate more objects in order not to be detected. One relies easily that given enough objects to manipulate, located over different space and has to be attacked under the same time, the chances for an attacker is significantly reduced. An attacker must, in order not to be detected, manipulate the whole system in order to succeed which is significantly harder.

In order to gain access to all information sources, from all levels of the model there is an amount of manual labor involved, foremost from the Risk Management perspective and the Decision Support System. Control must always be kept regarding business

operations, services, consumer's interactions, physical and logical infrastructure. Situation based security depends therefore on knowledge regarding how and when things in the system interact with each others, under different circumstances. All things together the model describes a system which shows interactions over the mental, logical and physical plane in a way that an attacker has a very hard time to predict.

7.1.5 Anomaly detection

One important part of information gathering is with regards to normal and un-normal network behavior (i.e. anomaly detection). In this case information gathering is based on gathering enough information in order to determine what type of behaviors deviates from normal network flow. This demands advanced analysis capabilities and large storage facilities in order to keep the relevant information in order to determine what "normal network flow" is.

7.1.6 Available concepts with today's technology

There exist systems today that offer parts of the above described functionality. Most systems today offer sub components of the joint capability asked for in the Intrusion Management system. Some systems offer parts of the functionality but have limitations in themselves that make them inappropriate. Examples regarding functionality are:

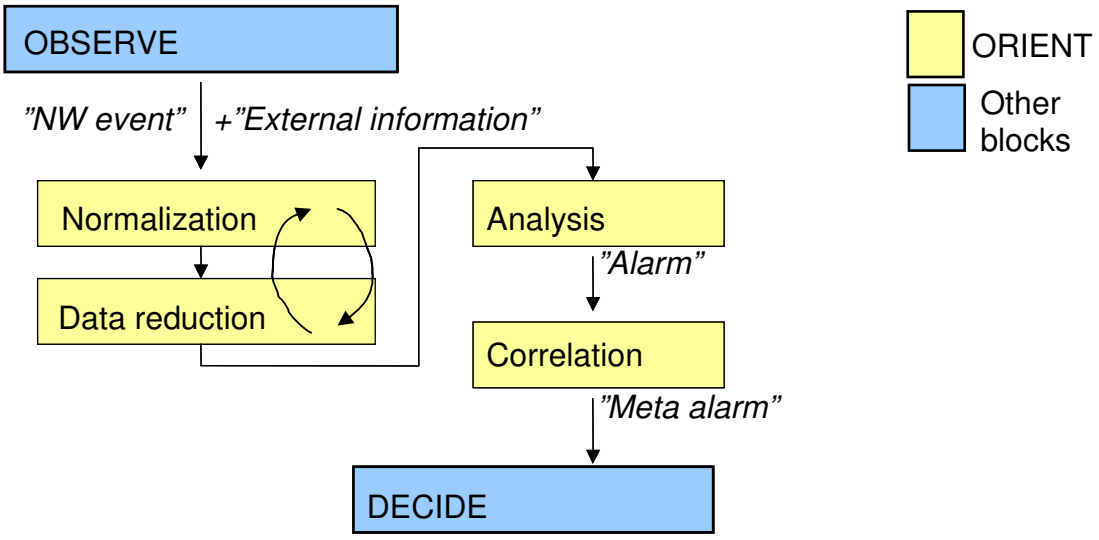
- Transport of large amounts of collected information might cause an internal Denial of Service attack due to the finite limit of bandwidth resource.
- Support for modern network topologies such as peer-to-peer, autonomous, or add-hoc networks have no support in commercial viable products on the market today.
- The field of combining different sources of information and information types is still immature and only commercial applications are usually supported. Advances have been made recently in IDS system coupled to network management systems.

Most information gathering systems today are dependent on the host systems that they collect information from. For example system logs, SNMP or configuration files. There is software that allows indirect information gathering by analyzing how systems react to different input, examples of the lateral is NMAP.

IDS technology is today built around two concepts, node-, or network based. Network based IDS technology can perform a correlation and an analysis before data is passed on, which results in lower network load. The downside to this technology is its incapability to handle encrypted network traffic, and the fact that the information gathering nodes must be places in architectural strategic places around the network in order to function well. Node based IDS technology on the other hand functions well in encrypted networks but in order to correlate events in the network between different nodes they have to be coordinated which in turn creates network load. Both methods have advantages and drawbacks, but they create a strong contender in combination with each other.

7.2 Observe and correlation of information

This section of the thesis focuses on the OODA-loop process block called Observe. The observe block can be broken down into the following components.



Picture 7.4: showing the four parts involved in the ORIENT process block from the OODA-loop.

The orient process block has for clarification reasons bee divided into two parts. Normalization, data reduction or data condensation, and analysis make up the first part. The second part consists of alarms, correlation and meta-alarms.

The analysis part of the orient block is comprehensive and therefore motivates a strong IT-support. Depending on the definitions of analysis, and where the analysis processing is carried out, the CPU and network load many vary greatly.
When regarding different aspects around evaluating algorithms for correlation and aggregation are, amongst other tings:

- Management of data conflicts
- Robustness
- Detection capabilities
- Time complexity
- Memory complexity
- Reliability
- Scalability

7.2.1 Normalization, correlation and aggregation

This part describes analysis algorithms which basically can be divided into two categories; misuse detection and anomaly detecting. Both algorithms are built around the same concept, equality. In misuse detection the equality are used. In anomaly detection whatever is left after the equality has been taken out, is used. Similar algorithms are therefore used in both cases, mainly inspired from data mining. Before the data can be analyzed it has to be transformed into a uniform format by the normalization process.

In order to compare (analyze) the collected data it has to be transformed into a uniform format, this process is called normalization. First of all, all scales and grades regarding sensor data (information gathering) have to be transformed into the same scale before it can be used. This is a sensitive process as it is divergence in the data from a defined normal that is sent to the analysis.

The next step is data reduction and condensation. Intrusion detection systems usually gather large amount of data, especially if multiple collection nodes are used. The data therefore needs to be reduced. This is usually done by reducing the least valuable data to the analysis. A lot of data, over multiple nodes, contains redundant information that is entries that are alike. These posts can be merged into a single post. Entries that are relative equal to each other can also be merged. The difficulty is deciding the boundaries for the equality and making sure that sequence of the events are not destroyed. Keeping the sequencing can be done by using a technique called condensation instead of reduction. Condensation can be compared to no-loss compressing of data. Sequencing and time stamping information is added to the information.

Both normalization and condensation is difficult in network environments that are dynamic in its nature.

7.2.2 Analysis

The detection of intrusions is the task of analysis algorithms, divided into misuse and anomaly detection algorithms. Most commercial IDS systems today use miss use detection algorithms which detect, with great certainty and little risk of inaccurate detection all known attacks. The downside is that they only detect know attacks. Considering an adversary which is both well funded and well informed, the chances of finding an exploitable error in software is good and therefore undetectable by misuse detection algorithms.

In order to detect new types of attacks anomaly detection algorithms are used. These are constructed around the concept of divergence from a predefined normal state. The divergence is then classified as attacks depending on a certain probability. These algorithms have a higher error rate, regarding both false alarms type 1 (false negative) and missed real attack attempts, type 2 (false positive) [BRACE]. Both false alarm errors cause a degenerate decrease in security because either the alarms are ignored, or drowns in an overwhelming flood of alarms.

7.2.3 Distributed systems

Regarding distributed systems more challenges are introduced. Controlling and updating the rules governing the algorithms cause difficulty. Automated update routines are needed (compare with antivirus update routines). Trust issues between the nodes also case problems. In order to detect attacks that spread across multiple nodes, the nodes must cooperate and be able to warn each other when there is an imminent threat towards them. Automated protection should also be included in the protection. There are multiple solutions to trust issues regarding distributed networks [BRACE]. Solutions regarding attacks and warning between nodes are proposed by the common Intrusion Detection Framework [PSSSW]. IEEE has a parallel working group [IDWG].

7.2.4 Capacity

All information has to pass the analysis part of the Orient block of the OODA-loop. The information will be made up from many different forms of media, amongst other printed media, intelligence information, networks information, verbal or digital storage media. The information has to pass through the analysis in order to maintain continuous control over the system and therefore detect anomalies that might point to an attack.

A design specific detail is the demand that the algorithms need to be self stabilizing. That is, if the analysis functionality needs to reboot for any reason, the algorithms need to shut down and restart in a secure manner. This creates a challenge as multiple functions are dependant on each others (i.e. when two autonomous networks reconnect to each others). More on self stabilization, robustness and fault tolerance can be found in [Tel00], [Lynch97] and [Mullen93].

7.2.5 Analysis with regards to Alarms, correlation and Meta alarms

This section discusses the linking between multiple IDS's in order to create a larger meta IDS with extended detection capabilities regarding complex attacks in larger network environments.

When regarding intrusion detection systems and extended IDS functionality problems occur such as:

- An overwhelming amount of alarms
- An overwhelming amount of false alarms
- The degree of detection is low when regarding new and stealth attacks

To make the situation even more complex, the use of heterogeneous IDS created a problem of results interpretation from the total value of all individual results (that is different report and presentation standards available). A large part of the problem here is due to the fact that different suppliers categorize and name attacks differently. The argument to be made here is that heterogeneous IDS information has synergy effects in forms of more complete results, but the different IDS systems results has to be correlated. Adding to complexity if the fact that more information than IDS information has to be regarded, information such as intelligence information, business intelligence information, network management information, contemporary social and environmental studies from Internet and newspapers for example. This means that the personnel working with the Intrusion Management system need to be very competent and highly skilled.
This chapter therefore discussed different options for, and problems regarding correlation methods, alarms and meta alarms.

Research within intrusion detection with regards to correlating alarm information is primarily taking place at the Internet Engineering Task Force (IETF), called Intrusion Detection Message Exchange Format (IDMEF). The model is centered on XML and a classification of alarm attributes. When regarding research in the field of alarm correlation the following external information might be of interest according to [DG03]:

- Information regarding the attacked infrastructure
- Information regarding the known weaknesses in the infrastructure
- Information about the ongoing attack
- Information regarding if the attack can be verified after the attack has occurred, called post mortem analysis.
- Information regarding the priority of the attacked system
- Information regarding the attacks visibility (that is what percent of the systems that should have seen the attack, actually did se the attack)
- Information regarding the current security level

Intelligence data will raise the quality of the correlated information. As intelligence data, in it broadest definition, we will include off-line information such as newspapers, list server information, system administrator reports, network management reports, etc (The information quality, objectivity and trustworthiness is not factored in to the overall judgment). If the IDEMF standard is to be governing, all this information needs to be translated to XML in order for the correlation to take place.

When different sources of information and analysis methods are used the information needs to be correlated. The correlation is expected to aid in the decision support and reduce the amount of false alarms. The overall expected result of this is better use of automated counter strike abilities.

Research regarding alarm information over heterogeneous environments is an active field of research [DG03]. In common when regarding this research is the need for a joint alarm format and a joint attack classification system (There exist attempts of attack classification but are in parts confidential. For the sake of the argument we will presume that there exists a classification scheme) [K03]. Correlation is then often hierarchical in its nature. First alarms are correlated in the individual sensors, then on a central level. It is common to correlate alarms individual alarms against meta alarms that contain a volume of already matched alarms. If an alarm is not positively matched, a new meta alarm is created. Meta alarms are therefore a way to capture all alarms that belongs to the same attack.

When analyzing the current research field regarding the correlation of alarms [DG03] and [JVA04] the following principle algorithm is found [DG03]:

- Create an alarm according to a pre defined standard format
- Store the alarms in a database
- Correlate alarms that belongs to the same attack type (remove duplicates)
- Correlate alarms of different attack types
- Raise the correlation information quality by correlating with external information
- Create security breach scenarios and identify the attacks next phase (prevention)

7.3 Decide

This section will comprehensively discuss the decision support system (DSS) within the Intrusion Management system. Decision is the third block of the four blocks in the OODA-loop. Different implementations of decision support systems will not be discussed in this thesis due to the fact that this thesis concentrated on security issues and not different methods or algorithms associated with decision support.

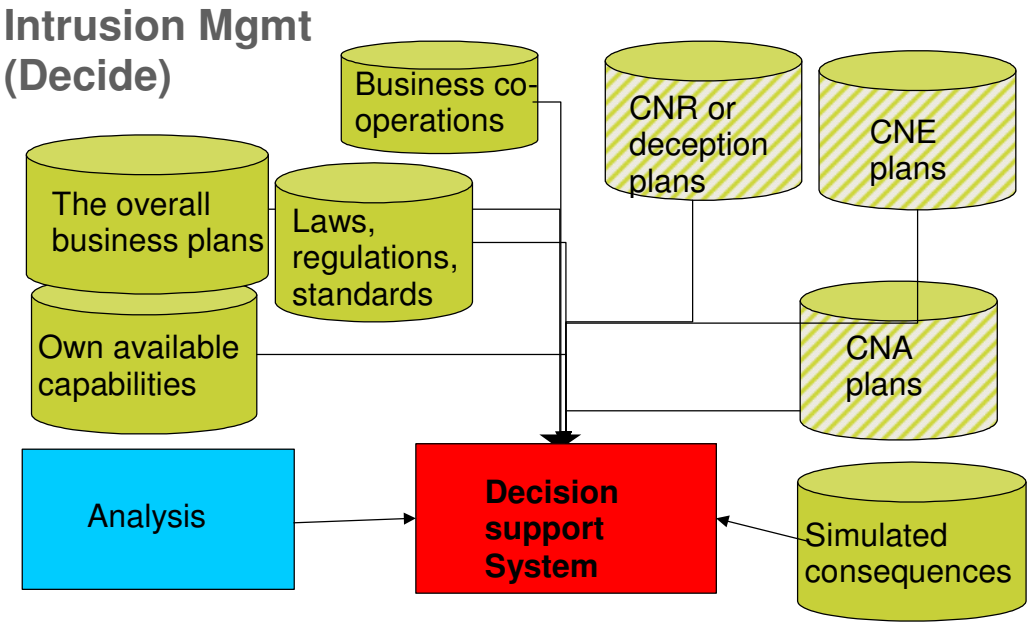
After the initial Observe and Orient blocks, the information is passed as input to the Decision block, composed of the decision support system that will lead to decision that is passed as output to the last block of the OODA loop, the Action block. After the last block has been executed of the initial cycle, a new cycle of the Intrusion Management system is done in order to make sure that the actions hade the expected effects on the adversary or the system. This last cycle is called the *simulation cycle*.

The decision support system needs to define Intrusion Managements comprehensive characteristics and therefore define roles and reasonability's between different instances depending on the security level. This means that there must be restrictions on the Intrusion Managements rights to use different capacities.

During operations, the decision support system needs to be constantly aware of its

own operational and available capacities. This doesn't necessarily mean network based capacities (CNR, CNE, and CAN) but also traditional defense capabilities such as lawyers, business operations (such as hostile takeovers, marketing warfare strategies etc), police, medical service and fire departments. These operations are governed by laws, regulations, business plans, standards, de facto standards and co-operations between businesses (partners, suppliers etc) amongst other tings.

Dependencies regarding the decision support systems are visualized by the following figure:



Picture 7.5: showing dependencies for the DSS and the input from the Analysis OODA-loop block.

The whole decision process must be analyzed in order to correspond to the business workings. In order to gain a tactical advantage through speed the level of decision automation must also be analyzed. This is in order to find the levels of, amongst other:

- Automation
  - Robustness
  - Determination
  - Decision hierarchies
  - Time complexity
  - Reliability of actions
  - Assurance levels
  - Confidentiality
- Autonomity
- Human intervention
- Different security levels depending on threat
- Business organization
- Steering or management models
- Reporting and action models
- Audit and revision and metrics

- Laws and regulation analysis
- Escalation routines of decisions
- Business intelligence

The surrounding process blocks of the OODA-loop need to be taken into account, such as the Action and Orient blocks. Interfaces needs to be defined in order to make sure that no information is lost between the transitions between the different blocks. This is done by making sure that that the information is in the correct format and is relevant to the DSS so that the information can be adequately analyzed. The same goes for the output of the Decide block.

Design considerations that have to be taken into account are:

- Pedagogic visual displays
- Dynamics of the underlying infrastructure
- How the decision is made:
    - Automated vs. manual decisions
    - Centralized vs. decentralized decision process
    - Different levels of decisions, tactical vs. administrative
    - Competences needed in order to be resolute in the decision making
    - Power of execution and the need to have executive authority
- Consequences of decisions based on both time and space
- The design criteria of the second loop, the simulation cycle
- Technical design aspects from the underlying infrastructure

An interesting aspect of the decision support system is the rule work that the DSS needs to consider. Considering both international and nation laws and regulations (Laws and regulations over an international arena can sometimes contradictory!) a governance and compliance process needs to be incorporated into the DSS. Information classification in itself is governing. Individual information pieces might have meta data attached considering the information's security classification. The joint information (all the information pieces put together) might justify a need for a higher information security classification than the individual information pieces put together.

As stated above the DSS needs information in order to recommend decisions. These decisions are then translated into action plans (orders) to the Action block. In order to execute these action plans the Intrusion Management system might have to share all, or parts of the information that the decision is based upon to all or some its input sources from the OODA-loop. This means communicating with its business partners, other privies or even governmental social assets such as police, health services, fire departments or national security incident organizations (such as Sweden's CITIC, or EU's CSIRT). Regulations regarding this communication must be developed.

In order to automate and therefore speed up the decision support in order to gain tactical advantages, a high degree of simulation is needed. Scenarios have to be developed and simulated in order to create a foundation of probable situation that might occur. Consequences of the decisions have to be simulated in order to evaluate dependencies of different departments and their individual protection plans for action. What are the consequences of shutting down a part of the network for the business that are depending on the network? Prioritizations of business fields have to be made through

(BIA) Business Impact Analysis [BCI05]. Prioritization has to be made based upon functionality and overall use for the business.

7.4 Action

This section discusses the Action block of the OODA loop. The Action block has the Decide blocks output as its input values. The Action blocks task is to execute the decision that has been made in the Decide block (by the Decision Support system). The Action block is therefore a divers block when it comes to competence demands and regional reach (even international reach) in order to execute effectively the decided upon action plan. It reports its actions back into the Observe block of the OODA loop. Actions can be either actual, concrete actions or simulations of a chain of events. This simulation must not under any circumstances disturb the daily business.

There are a multitude of different plausible actions to take depending on many different circumstances such as the type of business, environment, etc. There is also a multitude of management software to assist in the execution, such as network management equipment, security management equipment, etc. These management software uses policies, log information, software functionality, authentication and authorization information in order to function. It is important that this equipment is not limited to networks but also manages software and services. Training of personnel must be a large part of the effort within the Action block.

Examples of actions are:

- Shut down services, parts of- or the entire network.
    - Proactive change network or services available in the network
    - Reactive change network or services available in the network
    - Create autonomous networks
- Change threat levels (that is minimize either the probability or the consequence of a threat)
- Change security level
- Change the authority levels to the network or the services (authentication and authority levels have to be dynamic in order to change authority levels)
- Offensive response to threats (CAN, CNE, CNR, police, and law suits, etc)
- Change business partners
- Change marketing or business strategies
- Ignore events/incidents in the network
- Patch and update systems and infrastructure equipment
- Add or remove services in the network
- Minimize the services functionality
- Reconfigure both networks, software and services
- Start honeypot networks [HONEY]
- Track events/incidents in the network, log events/incidents
- Forensic traces
- Neutralize the threat by network attacks (CNA)

8 Results and achievements

The achievements of the Intrusion Management system are dynamic and dependant on a number of different factors such as time, space, network load, objectives, available services, and threat levels just to name a few factors. The mayor achievements of the Risk Management process are listed below, in no particular order.

8.1 Ability to dynamically shape the security protection depending on the threat

In a traditional protection strategy, protection is based on a layered model where attackers have to brake through many different layers of protection in order to reach the information (security in-depth). The downside of a layered protection strategy is that the protection is static, and when the protection is broken the information is vulnerable (a good comparison is a door protecting a house, when the door breaks the house is open and available to burglars). The layered approach to security is not dynamic in its protection strategy which means that costs of protection are constant over time.

In the Intrusion Management system the information will be handled dynamically and therefore need a more dynamic security protection.

The largest advantage of adopting a Risk Management based protection strategy is that the **security protection is balanced towards the perceived threat**. This balance is based upon the ability to weigh different factors against each other, such as the ability to secure information with the best possible protection in any given situation, or the need to implement a security solution whose dominant demand is cost. Risk Management can therefore create cost effective and dynamic protection.

A dynamic security protection model, based upon Risk Management, has the ability to create different protection levels for the same piece of information over both time and space. What this means is that the protection levels are different depending on perceived threats, where the underlying threat analysis changes all the time. A particular piece of information might be considered a vital protection asset in a restricted, contained international operation where the same piece of information at home might be considered none-vital and of low protection value. The actual protection should reflect these needs. This leads to different benefits such as quality and cost effectiveness.

Risk (i.e. DEFCON) levels stipulate the amount of, and the type of protection needed. In calm times (ordered state) the protection emphasis is given to legal aspects of security such as traceability, confidentiality and forensics, this need changes when the risk (i.e. DEFCON) levels change and the organization enters a disaster-like state in order to protect it self (This is of course simplified, as organizations usually have some sort of escalation chains and specific “security states” have to be breached in order to move through the states crises and disaster. The disaster state, through a network perspective, could be compared to a war-like state without the CNA-abilities). In crises and disaster like states the security needs are different and emphasis is given to safety, reliability and the need to fulfil once business objectives.

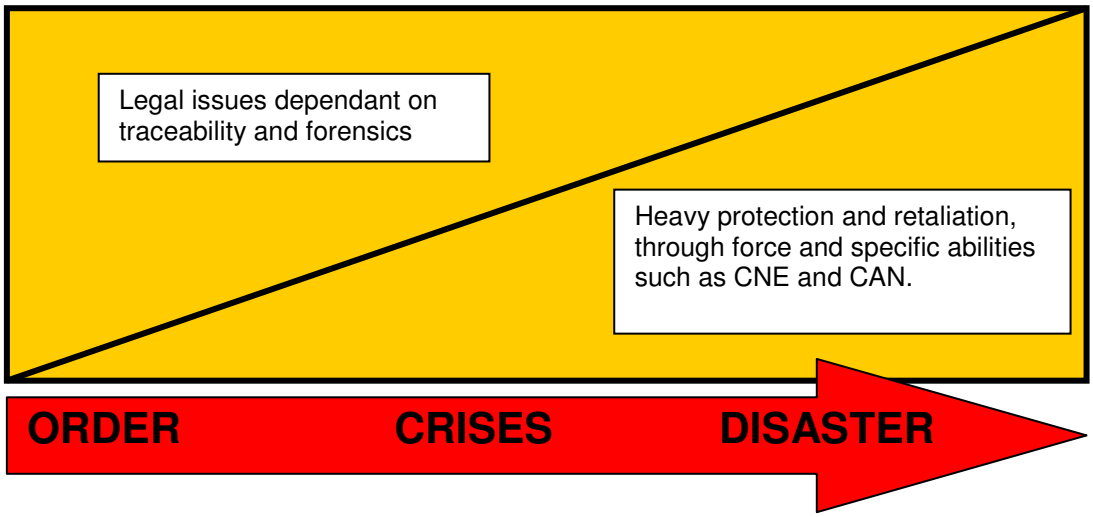


Figure 8.1: Picture describing the different needs depending on the current state of affairs. In calm times the legal issues are prioritised, in disaster times the protection and retaliation abilities are prioritised.

8.2 Management of trust during system lifecycle

A Risk Management system has an important influence on the establishment of trust in any environments during the entire environments life cycle. The fist phase where trust issues have to be addressed are in the initial deployment phase. When the environment is initially installed and turned on, that is when its components are initialized and registered as services the Risk Management service has to assess its trust-value. A trust-value is the components degree of trust worthiness to the rest of the environment. Without the **initial trust** control a fake service might be inserted into the environment whose sole purpose is to create disorder or to gather information.

When a system is being used, at system runtime, a user has to ensure that the system or service truly is who it says it is, and will perform the task the way that the user wants it to perform. The Risk Management system has to ensure **trust during runtime**. As an example, two companies that have not met and conducted any business before, acknowledge each others presence and reliability through technology today (this is usually done by SLL based Server Certificates that guarantees the servers authenticity and therefore hopefully the business behind the server). They need at runtime be able to automatically establish trust between each other in order to work together towards a common goal (do business). Intrusion Management has to be able to ensure trust assurance to the systems and users at runtime. All failures to establish the trust has to be handled by the Risk Management system in order to establish the security protection needs for the environment at that particular time and space.

An adjacent complexity that the Risk Management system has to address is the **detection of broken trust** links in the environment. In the ordinary everyday workings of business systems, services can and are in fact expect to lose their connectivity for either a brief instant of time or for longer times. When the service looses its connectivity the Intrusion Management system need to be able to detect broken trust links. A similar system needs by Risk Management, **re-establish the trust** from the broken links following an autonomous network state. A risk assessment regarding trust has to be performed before the service can be accepted back into the network environment again.

When a service is being **dismantled** from the environment infrastructure, it needs to make sure that the dismantling leaves the network in a trusted state and that the service in turn can be trusted in the destruction phase, i.e. won't leak any information and can not be reintroduced into the network infrastructure during dismantling.

The system trust is depending on management of the system during its lifecycle. Management systems have an important task to be the common system to observe and manage critical functionality to establish and sustain trust. The management system in its observing role is the most capable measuring tool of how well trust is achieved. Most of the management capability is built for purposes that have security implications. This means that the management system has information about security and system status and will thereby contribute to decision support and the availability to do a relevant risk management evaluation. The management system will to some extent depend on trusted systems for its functionality, but must still be able to help re-establish and preserve trust in the system itself. To enable this process, then technology and organization together must be able to establish initial status of trust from which repeated trust can be built upon.

8.3 Time factor

In the civilian, academic and modern military arena, speed is of the essence in order to succeed with any goal or mission. A popular envisioning of the strategy used in order to visualise the necessary speed in a business environment or in a battle scene, is the OODA-loop (Observe, Orientate, Decision, and Action). As described in chapter 2.1.2.

An advantage with Risk Management is that it gives strategists tools for simulating different scenarios and the security result of those scenarios. This will increase the decision speed within the Intrusion Management system which in turn will increase the decision speed within the network environment.

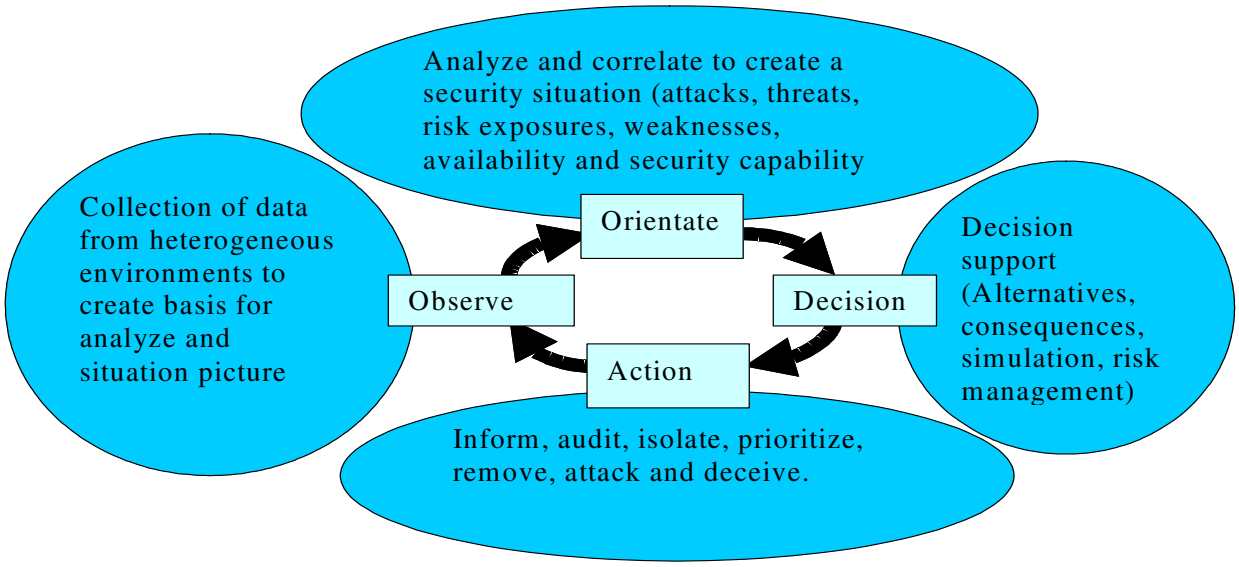


Figure 8.2: Picture showing the four major steps of the OODA-loop and example of actions taken within each of these steps.

Risk Management is a vital component of the OODA-loop in order to identify and prioritize the different threats towards a modern network environment. It is important that the Risk Management process handles both risk that exists within the system itself (risks that one tends to be knowledgeable about and that are handled in a classical manner, by among other things thick walls, locks and armed guards), and dynamic risks that threaten the system from the outside that is dependant on both time and space and inevitable will need more attention and effort in order to handle.

Simulated scenarios with plausible results and risks should be carried out continuously in order to ease the decision making process what probably will be carried out under great stress and under a very short timescale.

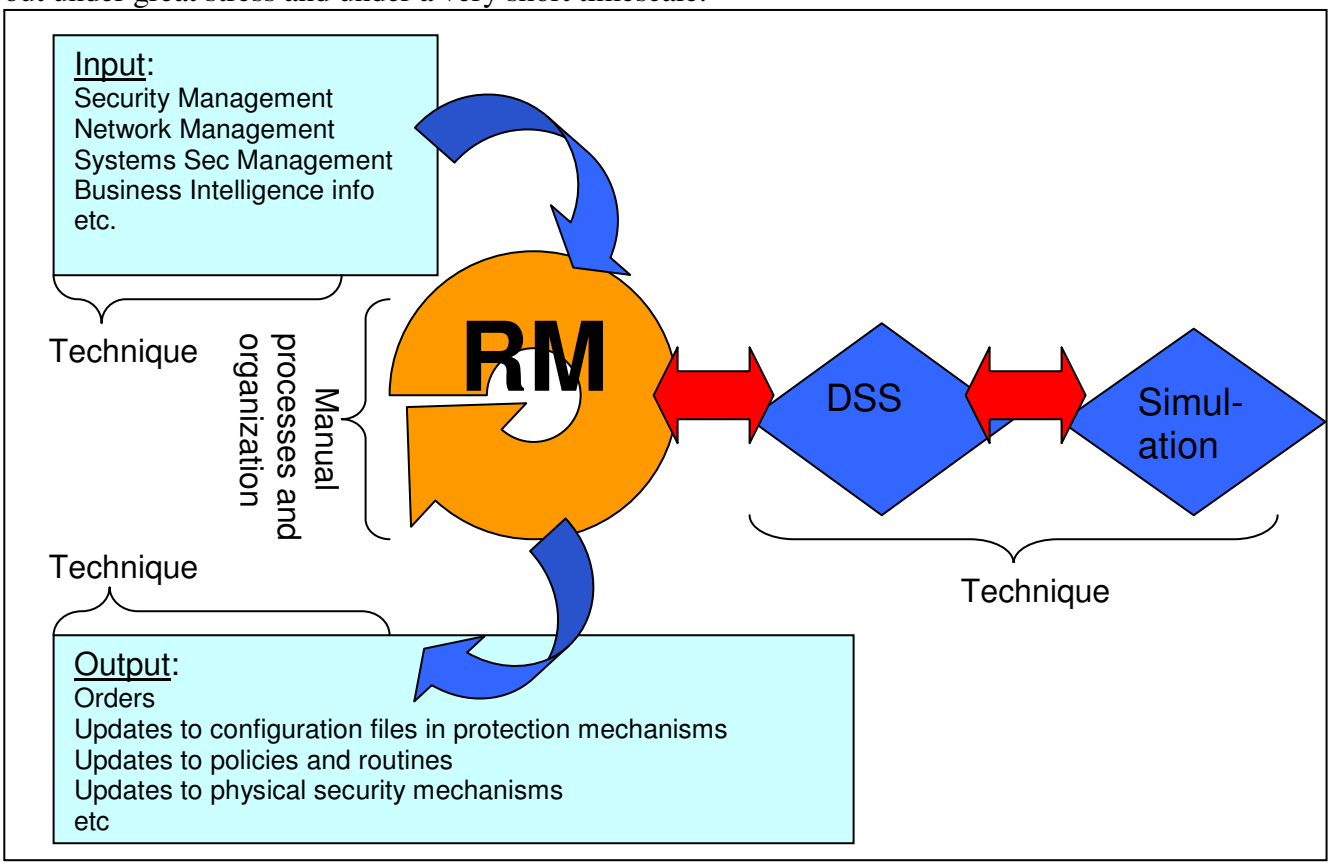


Figure 8.3: Picture showing the in- and output of the Risk Management (RM) cycle, with the support systems that the RM cycle depends on; the Decision Support System (DSS) and the simulation process. Manual and technical processes are shown.

The picture above describes the input problems very simplified. The Risk Management decision function will have difficulty in making a decision because of the information overflow. All different input units will demand a quick decision without prioritization, and in some cases without regards to the overall goal (business or military objective). Another parameter, to add to the complexity, is all the partners and interconnected parties to the network. The decision making process has support from the Decision Support System (DSS) with its simulations, but the DSS will only guide the decision function up to a certain level and the decision will be, and should always be human because of it complexity. The final decisions can not, and should not be left to the individual experts or to expert systems but should rather be made by a human with the

overall comprehensive (or bird's eye) view of the whole network and business or military goals.

Another complexity regarding the input of information into the Risk Management system is the security classification. Sensitive or secret information should be classified, for and example such as confidential, restricted, secret, and top secret, are all extrapolations from legislation (such as "the Official Secrets Act" in Sweden) where secret means different things to different organizations. As an example, military secrets differ from medical or business secretes in its protection needs (integrity over confidentiality). Even when confidentiality is prioritized such as in the case of military secrets and business secrets different prioritizations are made as a regard to the protection needed for different organizations leading to the need of different policies for different organizations.

The protection based on security threats are usually portrayed in information security policies which are different to different businesses, and definitely between business and other organizations such as the military or medical installations. This means that risk management can not treat information equal. Information coming from civilian agencies, partners or competitors might be correct (integrity and confidentiality vice) but the risk management system cannot be sure unless the security protections (technically, administrative, or policy wise) are the same. This is of course under the assumption that both the physical protection mechanisms and policies, rules and guidelines are the same which leads to a joint environment with equal trust towards the information. This is extraordinary and is usually solved with the use of accreditation.

8.4 Ability to prioritize

Risk Management gives a network environment the ability to prioritize between different abilities depending on the particular mission that has priority at any given time. The major prioritization that has to be made is between costs, resource allocation, safety, business or military objectives and security risks.

Risk Management gives the network environment the ability to coordinate and adapt the resources needed, force based upon the objectives, and the risks involved. The fundamental concept of the OODA loop is that our own decision cycle should be smaller, and therefore faster than the adversary's cycle resulting in giving us the information superiority.

8.4.1 Simulation as an input to the decision making process

A simulation should through different scenario exercises create different outcomes through the use of the same initial scenario. The quantitative values of the simulation should be the ability to carry out business objectives, estimate cost, effort and security risk. A simulation would further enhance the prioritizing process in order to be able to offer answers regarding the outcome of a particular decision very fast indeed. This would speed up the OODA-loop in order to be able to acquire the information superiority. Threats that should be handled within the Risk Management process should not only be IT-security threats but also information security (personnel, organization, etc) threats, business and political threats or any other threat that has a bearing on the network.

8.4.2 Strike capability based on objective and risk

The ability to prioritize must be an essential ability of the Risk Management system. Prioritization has to be made at all levels within the network environment, for example at different levels such as network trafficking (IP/routing/ transmission), protocol level, service level and even up to a cogitative level. That is the human interaction level. Prioritization is done in order to secure that the right or correct force is used. One can streamline the military ability based on the threat in order to make sure that only the correct amount of protection or retaliatory force is used. This is not only a humanitarian issue but also a logistic, political and a financial issue and in the end the result limits all risks.

8.4.3 Ability to delimit between business and network based objectives

Based on state of alert levels (i.e. DEFCON levels) different needs have to be addressed in the network environment. In calm times (through a security perspective) for example general network traffic such as maintenance and support traffic has to be prioritized in order to make sure that the network and services are resilient and kept in a ready state in case of a crisis or even disaster. In case of crisis or disaster, network traffic and services containing business information has to be prioritized and all other traffic and none essential services to the business objectives should be down prioritized. Risk Management therefore, has to have the ability to prioritize between network traffic and services.

9 References

[ISO17799] Information technology, Security techniques, Code of practice for information security management, http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612&ICS1=35&ICS2=40&ICS3=, 2006-06-11

[CLAUS] Carl von Clausewitz, (1780-1831), http://www.clausewitz.com/CWZHOME/Quotations.html, 2006-06-11

[FBI03] CSI/FBI Computer Crime and Security Survey 2003, http://www.gocsi.com/, 2005-11-07

[KBM04] Samhällets informationssäkerhet - Lägesbedömning 2004, Krisberedskapsmyndigheten, http://www.krisberedskapsmyndigheten.se/, 2005-11-07

[ISACA05] ISACA (2005) CISM (Certified Information Security Manager) Review Manual 2005, page.70. ISBN: 1-933284-04-8

[SCHN04] Bruce Schneier (2004) Secrets and Lies: Digital Security in a networked world, Wiley Computer Publishing, ISBN: 0-471-25311-1

[CISSP] Ronald L. Krutz, Russell Dean Vines, and Edward M. Stroz (2001) The CISSP Prep Guide: The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, Wiley Computer Publishing, ISBN: 0471413569

[GUSTH00] Gustaf Hamilton (1996): Risk Management 2000, Studentlitteratur, ISBN 91-44-00082-0

[BOYD86] Col. John R. Boyd (1986) "Patterns of Conflict" slideshow.

[MTP00] Michael T. Plehn (2000), Control Warfare: Inside the OODA lopp, School of advanced airpower studies, Air University, Maxwell Air Force Base, Alabama

[DOD36001] DoD Instruction S-3600.2 (1998), "Information Operations Security Classification Guidance (U),"

[JCF96] Joint Chiefs of Staff, (July 1996) “Joint Vision 2010”, Government Printing Office, page. 69

[FMVIO] Briggen Håkan Bergström, Övlt Håkan Gustafsson, Övlt Åsa Warg, Mj Ulf Forssberg, Mj Jörgen Röstberg, Foing Mia Löw, (2003)”Försvarsmaktens grundsyn Informationsoperationer, IO” HKV beteckning: 01 600:78657

[DOA03] (2003) Information Operations: Doctrine, Tactics, Techniques, and Procedures. Headquarters, Department of the army, FM 3-13 (FM 100-6)

[SCHNCR] Bruce Schneier, CryptoGram, Natural Advantages of Defense: What Military History Can Teach Network Security, Part 1, http://www.schneier.com/crypto-gram-0104.html#1, 2004-05-15

[DEMM] Wikipedia contributors (2006). PDCA. Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/w/index.php?title=PDCA&oldid=41266164, 2006-02-26

[CWR03] Chester W. Richards (2003), A Swift, Elusive Sword: What if Sun Tzu and John Boyd Did a National Defense Review?, Center for Defense Information, ISBN: 1932019014

[DEMOC] Wikipedia contributors (2006). Damocles. Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/w/index.php?title=Damocles&oldid=40652753, 2006-02-26

[AS\NZS] AS\NZS 4360:2004, Australian/New Zealand Standard RISK MANAGEMENT, ISBN 0 7337 5904 1.

[HAR68] Garrett Hardin (1968) "The Tragedy of the Commons", http://dieoff.org/page95.htm, 162(1968):page:1243-1248, 2006-06-11.

[PSSSW] Porras, P et al: The Common Intrusion Detection Framework Architecture, http://www.isi.edu/~brian/cidf/drafts/architecture.txt, 2006-06-11

[BRACE] Bace, R.G (2000): Intrusion Detection, Macmillan Technical Publishing, ISBN 1-57870-186-6.

[IDWG] Intrusion Detection Working Group (IDWG), http://www.ietf.org/html.charters/OLD/idwg-charter.html , 2006-06-11

[Tel00] Tel, G (2000): Introduction to distributed algorithms, Cambridge press

[Lynch97] Lynch, N (1997): Distributed Algorithms, Morgan Kaufmann

[Mullen93] Mullender, S (1993): Distributed Systems, Addison-Wesley

[PTPNET] Wikipedia contributors, 'Peer-to-peer', Wikipedia, The Free Encyclopedia, , http://en.wikipedia.org/w/index.php?title=Peer-to-peer&oldid=57152325, 2006-06-06

[LEVGJB] Laurent Eschenauer, Virgil D. Gligor, and John Baras (2003) "On trust establishments in mobile ad-hoc networks", Electrical and Computer Engineering Department, University of Maryland, 2003

[DG03] Gorton, D (2003): Extending Intrusion Detection with Alert Correlation and Intrusion Tolerance, Technical Licentiate Thesis, Report no 27L. Department of Computer Engineering, Chalmers University of Technology, Göteborg, Sweden.

[JVA04] Jonsson, Erland; Valdes, Alfonso; Almgren, Magnus (2004): 7th International Symposium, RAID 2004, Proceedings, Springer-Verlag Lecture Notes in Computer Science, September 2004. ISBN: 3-540-23123-4

[K03] Karresand, M (2003); Separating Trojan Horses from Viruses and Worms - A Proposed Taxonomy of Software Weapons, page. 127-134, Proceedings of IEEE Systems, Man and Cybernetics Society Information Assurance Workshop, 18-20 June 2003, West Point, USA

[BCI05] The Business Continuity Institute, Business Continuity Management – Good Practice Guidelines, 2005, page 22 onwards. www.thebci.org

[HONEY] The Honeynet Project, http://www.honeynet.org/, 2006-06-10.

9.1 Inspirational sources

Ramverk Säkerhetsmålsättning 2010 LedsystT, 2002-04-??, KC Ledstöd 10750:44592/01, LT 01-DP4-007

Handbok för Försvarsmaktens Säkerhetstjänst, Sekretessbedömning, 1999-06-30, M7745-734081

Handbok för Försvarsmaktens Säkerhetstjänst, Informationsteknik, 2001-05-02, M7745-734061

Direktiv för Försvarsmaktens informationssystem/informationteknikverksamhet, DIT 03 v1.0D, bilaga 1 till HKV skr 2003-03-18 09 626:64756

NATO Document C-M(2002)49 ”Security within the North Atlantic Treaty Organisation (NATO)”

LTO1O 030025 Regelverk för Security Management funktionen ver 0.2

CRAMM, from UK Government’s Security Service, http://www.cramm.com/

Magerit, “Consejo Superior de Informática” (Information Technology Council) in Spain

Octave - The Operationally Critical Threat, Asset, and Vulnerability Evaluation- a Risk, Management methodology, by Carnegie Mellon University, http://www.cert.org/octave/

A Risk Management Standard, by AIRMIC, ALARM, IRM, http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf

IEEE Std 1540-2001, “IEEE Standard for Software Life Cycle Processes – Risk Management”, IEEE, ISBN 0-7381-2834-1, 17 March 2001

Appendix A - Standards and methodology

This section should be regarded as a non comprehensive guide, and motivation for Risk Management through the standards and regulatory perspective. In a globalized world, Sweden can not act independent and isolatory but rather as an important part of a larger joint operation. In order to execute joint military operations, policy's, standards and guides have to be agreed upon and implemented in a similar, if not identical manner. There are many different standards and methods to consider, and this section does not in any way try to encompass all the different available standards or methods. Rather, a cross-section of the most popular, relevant or regulatory standards, methodologies and regulations are presented.

A.1 Risk Management and the EU Council Decisions and Regulations

Sweden is a part of the European Union since 1995 and therefore subject to EU's rules and regulations. Detailed Risk Management information in the scope of the EU is currently under development and an initiative has started within ENISA called "ENISA ad hoc Working Group on Technical and Policy Aspects on Risk assessment and Risk Management".

A high-level European Union documentation is the Council Decision 2001/264/EC adopting the Council's security regulations. The annex is called "Security Regulations of the Council of the European Union" and is currently regarded, superseded by the Common Security and Defence Policy, as the information security policy for the European Union and its member states. In part 1 of the document, the introduction point six (6) states: "*…It is fundamental that the degree of protection should correspond with the security criticality of the individual piece of information and material to be protected...*". Section XI entitled Protection of information handled in information technology and communication systems, states that information and communication systems require security protection that is based on a risk assessment.

Another high level EU document is the Regulation of the European Parliament and of the Council. Regulation (EC) No 460/2004 established the European Network and Information Security Agency (ENISA) and contains references to Risk Management. The sixteenth (16) bullet of the Regulation states that "*Efficient security policies should be based on well-developed risk assessment methods, both in the public and private sector. Risk assessment methods and procedures are used at different levels with no common practice on their efficient application. The promotion and development of best practices for risk assessment and for interoperable risk management solutions within public and private sector organisations will increase the security level of networks and information systems in Europe*". All systems classified CONFIDENTIAL UE and above should have a System-Specific Security Requirement Status (SSRS) produced. This SSRS is based on, among other inputs, a risk assessment.

A formal definition is also given within the Regulation in Section 1 Scope, objectives, and tasks under Article 4 Definitions, bullet (j) stating *"'risk management' means the process, distinct from risk assessment, of weighing policy alternatives in consultation with interested parties, considering risk assessment and other legitimate factors, and, if need be, selecting appropriate prevention and control options;"*

A.2 Risk Management and NATO integration

In an effort to look at integration issues (coalition issues) and inter dependencies between armed forces on a national level, NATO has the most complete and demanding set of rules and guidelines. This chapter is added as a motivational incite into what NATO demands from its members. It is also important to look at future integration issues between FMLS 2010 and NATO in case of future joint military ventures.

The NATO definition of Risk Management is:

"A systematic approach to determining which security countermeasures are required to protect information and supporting services and resources, based upon an assessment of the threats and vulnerabilities. Risk management involves planning, organising, directing and controlling resources to ensure that the risk remains within acceptable bounds."

According to NATO document C-M(2002)49 - Security within NATO, under "Basic principles and minimum standards of security" section "Basic Principles"

(c) security risk management shall be mandatory within NATO civil and military bodies. Its application within NATO nations shall be optional;

Further on in the policy, it is stipulated under Enclosure "F", bullet 2 that:

"…the "Primary Directive on INFOSEC" is supported by directives addressing INFOSEC management (including security risk management, security approval, security-related documentation, and security review / inspection) …" this is further elaborated on under bullet 4:

"The integrity and availability of NATO classified information, and of supporting system services and resources, shall be protected by a minimum set of measures aimed at ensuring general protection against commonly encountered problems (whether accidental or intentional) known to affect all systems and supporting system services and resources. Additional measures shall be taken, appropriate to the circumstances, where a risk assessment has established that NATO classified information and/or supporting system services and resources are subject to increased risks from specific threats and vulnerabilities."

Under bullet 15 the policy states:

"Systems handling NATO classified information, in NATO civil and military bodies, shall be subject to risk assessment and risk management in accordance with the requirements of directives supporting this policy."

A.3 Risk Management and ISO/IEC 17799

The International information security standard ISO/IEC 17799 is perhaps the most widely used standard for information security in the civilian sector. ISO/IEC 17799 heavily relies on Risk Management in order to evaluate different risks to an organisation. Risk Management is used within most of ISO/IEC 17799's ten security areas. ISO/IEC 17799's definition of Risk Management is formulated as "**risk management:** process of identifying, controlling and minimizing or eliminating that may affect information systems, for an acceptable cost".

Under the Introduction chapter, a subchapter entitled Critical Success Factors lists different factors that are critical in order to implement information security into an

organization. The bullet entitled (d) states that a critical success factor is "*a good understanding of the security requirements, risk assessment and risk management;"* Risk Management is not described in great detail in the standard; instead a new standard is being developed as an international standard for Risk Management. This standard is currently in a draft format but is expected to be released shortly (expected within three years). There has been a formal release of ISO/IEC Guide 73 Risk Management – Vocabulary – Guidelines for use in standard.

A.3.1 Comments on the International Risk Management standard draft

According to the Risk Management draft; Risk Management involves managing to achieve an appropriate balance between realizing opportunities for gains while minimizing losses. It is an integral part of good management practice and an essential element of good corporate governance. It further states that Risk management involves establishing an appropriate infrastructure and culture and applying a logical and systematic method of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risks associated with any activity, function or process in a way that will enable organizations to minimize losses and maximize gains.
According to the draft, risk management in order to be effective, should become part of an organization's culture. It should be embedded into the organization's philosophy, practices and business processes rather than be viewed or practiced as a separate activity. When this is achieved, everyone in the organization becomes involved in the management of risk. The key benefits of Risk Management are:

- better identification of opportunities and threats;
- gaining value from uncertainty and variability;
- pro-active rather than re-active management;
- more effective allocation and use of resources;
- improved incident management and reduction in loss and the cost of risk, including
- commercial insurance premiums;
- improved compliance with relevant legislation; and
- better corporate governance.

Risk management is a key business process within both the private and public sector around the world.

A.3.2 Comments on AS/NZS 4360:2004 Risk Management

The AS/NZS 4360:2004 provides a generic framework for establishing the context, identifying, analysing, evaluating, treating, monitoring, and communicating risk. The standard forward includes: "*Risk management involves managing to achieve an appropriate balance between realizing opportunities for gains while minimizing losses. It is an integral part of good management practice and an essential element of good corporate governance*." It further states that "*To be most effective, risk management should become part of an organization's culture. It should be embedded into the organization's philosophy, practices and business processes rather than be viewed or practiced as a separate activity.*" Risk is often interpreted in terms of hazards or negative impact, but the standard is not only concerned with risk as exposure to the consequence of uncertainty, or potential deviation from what is planed and expected. The process

described is instead concerned with the management of both potential gains and potential losses.

A.3.3 Risk Management and Information Security Forum (ISF)

The Information Security Forum (ISF) is an international association of over 260 leading organisations which fund and co-operate in the development of a practical research programme in information security. According to ISF's own introduction "*the ISF's work probably represents the most comprehensive and integrated set of material anywhere in the world in the area of information risk management*".

The ISF standard is set as guide for the minimal security demands in an organization. In the standard, risk analysis would typically be used to identify the need for ***additional*** controls in particular areas, over and above those specified in the Standard. Information risk analysis is specified as a recurring topic over the whole standard and therefore added to all parts of the standard.

Section SM 3.3 entitled Information risk analysis describes different tracks for Risk Management. Both business and information risks are handled as opposed to the other standards described in this chapter.

A.3.4 Risk Management and Basic Level for IT Security (BiTS)

Swedish Emergency Management Agency (SEMA) has created BiTS as a baseline for information security for Swedish authorities.

To strengthen Swedish authority's ability to handle crises the regulation (2002:472) requires actions from the authority's to handle emergency. The authority has a requirement to analyse its IT systems every year if the existence of vulnerability or risks on its field is found. The result of this work should be evaluated and merged based on risk and vulnerability analyses. This will be reported together with its annual report. BiTS describe Risk assessment as: **"***Document that include a risk and vulnerability analysis for an IT system, or internal network, and states the requirements on confidentiality, integrity and availability. It also include the taken security measurements, and if necessary further needed measurements to fulfil the security requirements. Risk assessment should reflect the security principle and directives contained within the IT security policy, and the performed roll of the IT system and network within the business.*" This approach is in itself not incorrect, but rather puts Risk Management into a low scope. Risk Management should be an all-embracing method or work process controlling not only information assets and risks but also all other known risk, such as environmental-, business-, and process-risks.

A.4 Laws, regulations and methodology

In the civilian arena there exist a multitude of Risk Management methodologies. Examples of methodologies are:

- CRAMM, from UK Government's Security Service
- Magerit, "Consejo Superior de Informática" (Information Technology Council) in Spain
- Octave - The Operationally Critical Threat, Asset, and Vulnerability Evaluation- a Risk Management methodology from www.cert.org/octave, by Carnegie Mellon University.

- A Risk Management Standard, by AIRMIC, ALARM, IRM
- A IEEE draft regarding Risk Management is called P1540-2001 “Risk Management Standard - Process and Implications”.

The above standards and methodologies are all generalizations of Risk Management methodologies originally developed for specific fields or problem areas. These should all be analysed in a development of a specific Risk Management methodology for the Intrusion Management system in order to custom make a methodology that is tailored to the exact needs of the Intrusion Management system.

A.4.1 Sarbanes Oxley Act (SOX)

An American legislation which has impact on large international corporations that wish to conduct business in the USA is the Sarbanes Oxley Act. SOX was developed in the wake of corporations such as Enron, WorldCom and others, mainly in order to control corporations financial reporting duties. SOX has within the civilian arena created quite a bit of interest. SOX not only controls financial reporting, but also in part IT and information security in order to support reporting capabilities. SOX is added to this document because of the large interest the law has attracted in the civilian community and because of the work that has been put into the SOX field and the experience that can be drawn from this work.

Risk Management is a large part of SOX, especially considering documentation around decisions regarding risk analysis and risk mitigation. There are many parts of SOX that all discuss different aspects of the Risk Management process. In the context of this document two sections are highlighted.

Section 107 discusses risk assessments and the need to perform risk assessments of the total operating environment. By evaluating entity wide and application-level risks in a systematic and linked manner, a complete and balanced measure of the control activities necessary to meet the entity’s control objectives can be developed.

Section 202 discusses Risk Considerations. To assist in determining the overall scope of assurance procedures at the transaction level, management and practitioners need to consider assurance risk at the individual-class-of-transactions level. There are various approaches available that assurers may use to restrict assurance risk at the class-of-transaction level to enable an expression of opinion on the assurance statement. For assurance engagements, a risk assessment analysis should be performed within the context of the overall information systems environment and operations processing cycle.

Växjö
University

Matematiska och systemtekniska institutionen
SE-351 95 Växjö

Tel. +46 (0)470 70 80 00, fax +46 (0)470 840 04
http://www.vxu.se/msi/