LAUREA
UNIVERSITY OF APPLIED SCIENCES
Prime Mover

Fundamentals of Vulnerability Assessment

Schneider, Stefan

2014 Security Management

Laurea University of Applied Sciences
Leppävaara

Fundamentals of Vulnerability Assessment

Schneider Stefan
Security Management
Bachelor's Thesis
February 2014

Laurea University of Applied Sciences
Laurea Leppävaara
Bachelor´s Degree Programme in Security Management

Abstract

Stefan Schneider

Fundamentals of Vulnerability Assessment

Year 2014 Pages 66

Our modern society is built up by complex infrastructure systems that need to be able to deal with not only their own supporting system, but also to be part of a more complex sophisticated system where several independent systems are required to work together.

During the last decade security managers and security specialists all over the world have started to understand that the complex and sophisticated systems we take for granted on a daily basis need to be better protected.

Government and other official authorities have started on a higher and deeper level to assist more with the protection of common infrastructure due to the fact that a temporary or in the worst case a full stop of the infrastructure will not only affect the economic life, but it will also create a fear among the citizens that they are unprotected and not secure.

The purpose of this thesis is to gather relevant areas for a fundamental vulnerability assessment that could be the foundation for current and future security managers and specialists when they start a vulnerability assessment of their facility. The main sources used for the theoretical background comes from ASIS and Sandia.

In the appendix of this thesis the reader can find the suggested vulnerability assessment templates. The templates should function as guidelines and not as a de facto standard. Depending on the investigated facility the reader can choose to adjust the templates to fit their requirements.

The main conclusion of this thesis is that a proper and logical fundamental vulnerability assessment is needed for the management of a specific facility to make the proper security changes.

Keywords: vulnerability assessment, facility characterization, threat assessment, asset identification, vulnerability assessment report, risk identification, project management and auditing.

Laurea University of Applied Sciences
Laurea Leppävaara
Bachelor´s Degree Programme in Security Management

Tiivistelmä

Stefan Schneider

Haavoittuvuus arvioinnin perusteet

Vuosi 2014 Sivumäärä 66

Nyky-yhteiskunta on rakennettu monimutkaisten järjestelmien varaan. Näiden järjestelmien täytyy toimia sekä itsenäisesti ja ylläpitäen itsenäisiä tukijärjestelmiä, että osana hienorakenteista kokonaisvaltaista järjestelmää.

Viimeisten vuosikymmenien aikana turvallisuus päälliköt ja asiantuntijat ovat alkaneet ymmärtää, että näitä hienovaraisia ja monitahoisia järjestelmiä, joita pidämme yhteiskunnassa itsestään selvinä, täytyy suojella ja suojata.

Valtiovalta ja muut viranomaiset ovat ymmärtäneet, kuinka tärkeää on näiden tavallisten yhteiskunnan järjestelmien turvaaminen. Näiden järjestelmien väliaikainen tai pahimmassa tapauksessa täydellinen toimintakyvyttömyys, ei vaikuta yhteiskuntaan vain taloudellisesti, vaan synnyttää lisäksi turvattomuuden ja epävakaisuuden tunteen kansalaisten keskuudessa.

Tämän opinnäytetyön tarkoituksena on kartoittaa haavoittuvuus arvioinnin keskeisimmät alueet. Opinnäytetyö voi siis toimia nykyisten ja tulevien turvallisuuspäällikköjen ja asiantuntijoiden perustana uuden hankkeen tai kohteen haavoittuvuuden arvioinnissa. Keskeisimpinä lähteinä työssä on käytetty ASIS ja Sandia järjestöjen haavoittuvuus arvioinnin teorioita.

Sisällysluettelosta lukija voi löytää ehdotetut mallit haavoittuvuus arvioinnin tekoon. Mallien tulee toimia teoreettisena ohjenuorana arvioinnin tekemiselle. Jokaisen kohteen kohdalla lukija arvioi ja mukauttaa mallit sopiviksi kyseisen kohteen yksilöllisten tarpeiden mukaan.

Opinnäytetyön keskeisimpänä johtopäätöksenä voidaan todeta, että haavoittuvuus arvioinnin tekeminen on olennaista ja tärkeää, jotta turvattavia kohteita voidaan hallita ja turvata laadukkaasti.

Avainsanat: Haavoittuvuus arviointo, kohde arviointi, uhka analyysi, voimavarojen tiedostaminen, haavoittuvuus arvioinnin raportti, riskianalyysi, projekti johtaminen ja tutkiminen.

Table of Contents

1 Introduction 7
1.1 Background 7
1.2 Purpose and structure of this thesis 7
1.3 Theoretical background 8
1.4 Methodology and limitations of the thesis 9
2 Facility characterization 11
2.1 Determining the level of assessment 12
2.2 Physical condition 16
2.3 Facility operations 18
2.4 Facility policies and procedures 19
2.5 Legal aspect 20
2.6 Safety consideration 20
2.7 Corporate goals and objectives 20
3 Asset Identification 21
3.1 Category one – People 21
3.2 Category two – Property 22
3.3 Category three – Information 22
3.4 Category four – Critical Assets 22
3.5 Intangible assets 22
3.6 Scale of measuring the relevance of the assets 23
3.7 Asset identification in aspects of an adversary 24
4 Threat Assessment 24
4.1 Gathering information on existing and potential threats 25
4.2 Intelligence sources 26
4.3 Crime analysis 26
4.4 Published literature 27
4.5 Government directives and legislation 27
4.6 Capabilities of the adversary 27
4.7 Example of threat capability spectrum 30
4.8 Calculate the threat spectrum and evaluate the risks 30
5 Auditing 32
6 Red Teaming 34
7 Vulnerability Assessment Report 37
8 Project Management 38
8.1 Development 39
8.2 Planning process 39
8.3 Execution phase 39

8.4 Conclusion phase 40
9 Conclusion 40
References 43
Internet references 43
Illustrations 45
Figures 46
Tables 47
Appendices 48

1 Introduction

1.1 Background

Security managers around the world have since September 11, 2001 understood that traditional security that has been applied to the majority of buildings today is far from optimal. Traditional security consists of the essential package of installing a CCTV-system, having a guard at the front door and making sure that the stereotypical thief does not steal technical hardware and/or vandalize the facility in the form of graffiti or littering.

For over a decade, a growing amount of security managers understands that the needs and demands from facility stakeholders and human and non-human threats are a vital part of the security foundation if we want to establish a decent security level.

Security managers and specialists understand that the management of a facility cannot approve expensive or for that matter any kind of security solutions unless there is a proven and documented reason why it is a necessity, and that it will lead to return on investments.

If a security manager or specialist would like to or ordered to do a vulnerability assessment, he can chose from several different methods. Some methods are very complicated and involve detailed financial calculations that will take a vast amount of working hours and might not be adequate to their facility or adjusted to the intention of their security.

This thesis goes a little bit deeper and gives the reader and hopefully the security manager a more solid foundation to stand on when he or she would like to start a vulnerability assessment project. Depending on the facility and the criticality of it there might and most likely will be differences and, as stated before, this thesis serves only as a guideline and not as a de facto standard.

1.2 Purpose and structure of this thesis

The primary purpose and target of this thesis is to produce a vulnerability assessment concept for future and current security managers.

The primary research question of this thesis is: What essential information should be included in a primary vulnerability assessment according to theoretical information used in this thesis?

This thesis is divided into nine different chapters. Through chapters one to seven, the theoretical part of the thesis allows the reader to understand the empirical data that needs to be

collected for a primary vulnerability assessment and in chapter eight and appendices the reader receives practical information on how this empirical data can be gathered and reported.

1.3 Theoretical background

ASIS International was founded in 1955, and it is a security organization devoted to developing educational programs and materials for security professionals all over the world. The latest information is that ASIS International has over 38,000 members all over the world.

The most central aspects from ASIS that are part of this thesis foundation are the needed information to be able to take the PSP certification. The PSP certification is the ASIS certification to become a certified Physical Security Professional. To be able to achieve the PSP certification a person needs to study eight publications.

The main book used from ASIS PSP reference material was "Design and Evaluation of Physical protection systems, 2nd Ed. The main reasons why this book was the foundation for this thesis is due to the comprehensive approach to the subject by the author of the book. Every chapter is well written and a clear green thread follows through the whole book. The book is based mainly on Sandia reports, legal requirements from American departments such as the department of labor, regulations published by the Federal Bureau of Investigation (FBI), the environmental protection agency, and the United States department of commerce, Federal Emergency Management Agency, U.S department of defense, U.S department of justice, and department of homeland security. In the appendix, a short summary of the books used from ASIS can be found.

The secondary main source for this thesis comes from Sandia National Laboratories. Sandia National Laboratories have for over 60 years helped with scientific and technological advancements regarding security issues for the U.S. Sandia National Laboratories is owned by Martin Corporation and has several contracts with the U.S Department of Energy Nuclear Security Administration. Sandia also cooperates with and supports several federal, state, and local government agencies, companies and organizations.

Besides published books/publications from the ASIS PSP reference set and Sandia National Laboratories, other publications had an important function in this thesis. The amount of data that can be collected for a vulnerability assessment is extensive, and research for this thesis was limited to the ASIS PSP reference set and Sandia National Laboratories due to reason that their material is commonly used. A short description of the material can be found in the appendix.

1.4 Methodology and limitations of the thesis

The primary idea of constructive research is to find a new or alternative method to a problem/situation. The end goal of this thesis is to give the reader an alternative method of how a vulnerability assessment can be conducted. According to the constructive research approach "the research should solve several related knowledge problems, concerning feasibility, improvement and novelty" (Lukka 2003, 83-101). The outcome of this thesis is to produce an option regarding vulnerability assessment for the future or current security managers.

Phases of a constructive research plan are according to Hair. Money, Page & Samouel (2007, 179-222) divided into six different phases.

1. Find a practically relevant problem
2. Obtain an understanding of the topic and the problem
3. Innovate, i.e. construct a solution idea
4. Demonstrate that the solution works
5. Show theoretical connections and research contributions
6. Examine the scope of applicability

During this process group discussions, brainstorming with fellow students in the vulnerability assessment course at Laurea University of Applied Science, listening to experts from different organizations and simple observation was used as a supplementary research to help this thesis to be completed. The use of proper theme interviews was considered but not used due to the vast differences in knowledge and positions with the interview persons.

This thesis will work as the foundation for two different development projects. The first project is the vulnerability assessment course at Laurea University of Applied Sciences, and the second development project is a vulnerability assessment report done for a local international company. The findings and the process of the vulnerability assessment done for the company is confidential and will not be included in this thesis.

This thesis has limitations. The first and most significant limitation of this thesis is that it is constructed as a set of guidelines and not as a final product that can be used on all kind of facilities all over the world. That means that the reader must understand that each facility and placement are individual and should be considered like that during the vulnerability assessment process.

The second limitation of this thesis is that the vulnerability assessment topic is a very dynamic area and/or field of expertise, so one set of guidelines formed in this thesis might be obso-

lete in the near future due to technical advancements, the way the adversaries are operating, legal limitations and so on.

The third imitation of this thesis is that this thesis is primarily influenced on American standards, American literature and reports created by American governmental bodies and agencies. Most of the published material gathered from various agencies within the American governmental bodies only reference themselves or other departments. The primary source of the literature or published material is not found, and therefore this should be considered when the reader goes through this material. The literature collected for this thesis is primarily gathered from books written by American security authors, and therefore the standards or requirements needed in Finland or any other European country might differ.

1.5 ISO 31000:2009

This segment describes in short the ISO 31000:2009 and it´s relevance in this vulnerability assessment thesis. Another name for the ISO standard 31000:2009 is Risk Management.

According to the ISO.org own website the ISO standard 31000:2009 is a Risk Management standard – Principles and guidelines, provides principles, framework and a process for managing risk.

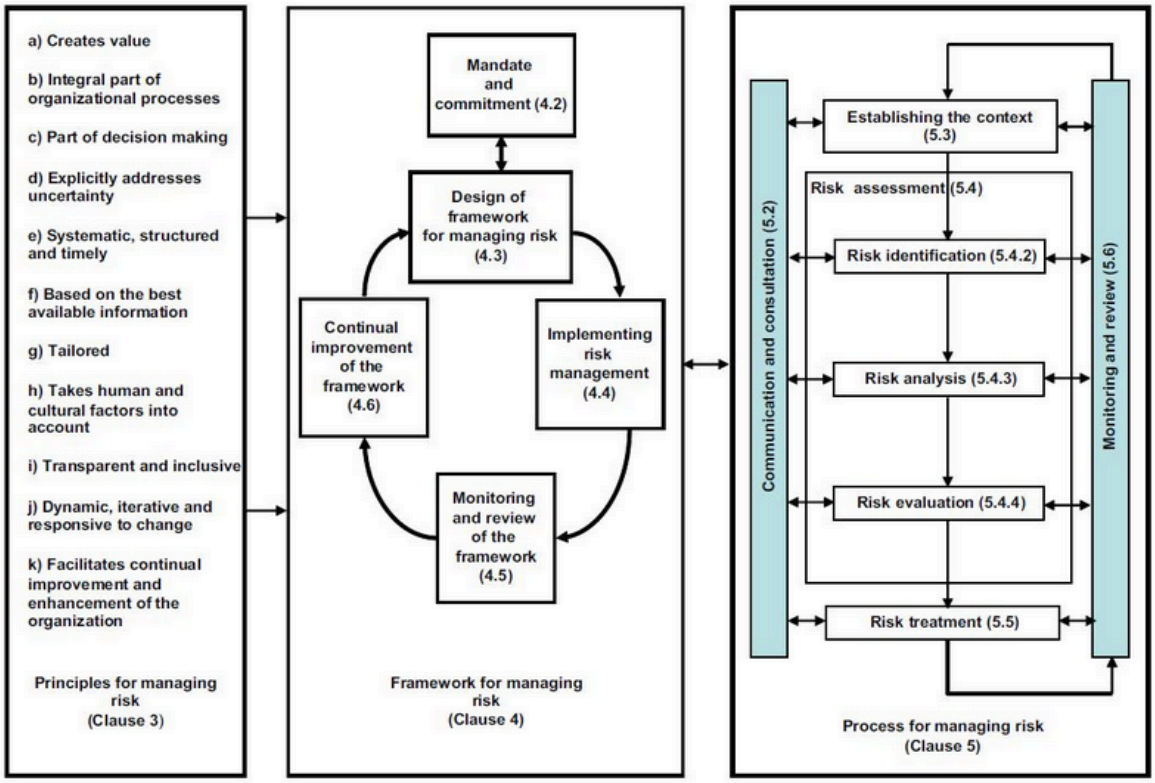

Figure 1 ISO 31000:2009 Risk Management

The purpose of ISO 31000:2009 is to standardize, provide principles and guidelines for anyone dealing with risk management. If no existent vulnerability assessment process exists the ISO standard is qualified tool to start the process.

The Risk Management standard is divided in three sections. The first section is principles for managing risk, the second section is framework for managing risk and the last section is about the process for managing risk. The general outline and process can be found by searching for it on the Internet, but the full version can only be bought or borrowed from libraries that have them. The original text that the ISO 31000:2009 is based on is from the AS/NZS 4360:1995. The ISO standard 31000:2009 can´t according to iso.org be "used for certification purposes, but does provide guidance for internal or external audit programs".

2 Facility characterization

This segment describes the importance of a proper facility characterization in the vulnerability assessment. This segment is divided in several chapters and in the end of the thesis in the appendix a suggestion of a facility characterization document can be found. The central part of the facility characterization is taken from the book, The design and evaluation of physical protection systems, second edition (Garcia 2008).

As the first step in a Vulnerability Assessment process, "before any decisions can be made concerning the level of protection needed, an understanding of what is being protected and the surrounding environment are essential" (Garcia 2008,15). An essential feature of the facility characterization and the initial step of a vulnerability assessment are to understand the priorities of protection and characterization of the facility and its surroundings. (Garcia 2008,15-23)

According to Garcia (2008), the first and the most important aspect when doing a facility characterization is to have an open mind and to use all relevant sources. An up to date audit can only be done if working staff, security officers, management and even neighboring companies are addressed and involved in the vulnerability assessment. Obviously their involvement will differ according to their relevance and need of involvement in the assessment. This chapter is divided into several sub categories, and it starts with the crucial aspect of determining the level of assessment. When each sub category has been evaluated a proper characterization is done.

2.1 Determining the level of assessment

Before the assessment starts, the person or group responsible must determine how deep the characterization and the whole vulnerability assessment process should go. According to the Risk Assessment FEMA 455 there are different factors such as "type of building, location, type of construction, number of occupants, economic life, the owners particular concerns and available economic resources" (FEMA 455 2009, 6).

The most relevant factor that all vulnerability assessment shares is the benefit versus the cost factor. No one wants to invest a substantial amount of money into a system that in the end protects something with little value.

In FEMA 452 and FEMA 455, the level is divided into three different groups or tiers. Tier one is the lowest grade security building, and a Tier three building is a high-grade building.

In FEMA 455, a rapid screening table has been made to show a general overview of the work-load that is necessary for each Tier group.

Tier	Description	No. of Screeners	Duration	Building Types
1	Screening Evaluation	1-2	Up to 2 days	Majority of standard commercial office buildings and other non-critical facilities and infrastructure
2	Full On-Site Evaluation	3-5	3-5 days	Most high-risk buildings, iconic commercial buildings, government facilities, schools, hospitals and other designated high value infrastructure assets
3	Detailed Evaluation	8-12	Several days to weeks	High value or critical infrastructure assets.

Figure 2 FEMA 455 Rapid screening table

The most significant aspect of this table is to recognize that the Department of Homeland Security, which produced this guideline, has their own auditors who fill their requirements regarding education, experience and have additional programs with ready-made material that can be used from the start.

The second aspect of this table and a good point of direction is that tier one vulnerability as-sessment should be done for most standard commercial buildings. The tier two is done for more high-risk buildings such as government facilities, schools, hospitals and so on. The last tier, the tier three is done for high value or critical infrastructure assets. An important part of

the vulnerability assessment of the security installations of the facility is to understand what kind of building will be analyzed. In general, there are four general components that need to be considered before a deeper analysis is started.

In general terms according to FEMA 445, there are three different modes that a building can operate under. The first mode is the so-called open mode that means that the facility has no security at the entry level so anyone can access without being checked.

The second mode is a closed mode that means that any person who wants to enter the building needs to pass through some kind of security check (assessment of the security check will be explained later on). That means that the person who wants to enter will have his credentials checked, and they need to be on an authorized “list” if they want to continue inside.

The third mode is the hybrid, which means that it is a combination of the first two. It does not have to be a security check at the entry level, but some areas of the facility are closed and the only way of accessing them is through a security check or some other form of credentials check.

Regarding the operating hours there are three general operating hours a building can follow (buildings like military buildings or other high risk buildings are not considered here).

When assessing the opening hours the auditor needs to establish the opening hours of the facility. There are three common varieties regarding opening hours. Business hours refer to the common opening hours of that facility, and follow the requirements of the majority of the tenants. The second variety is intermediate hours that mean that the facility is open a couple of hours before and after the regular business hours and in some cases on weekends. In general, the security department should already be up and running during these pre/post hours. A third common option is the “other hours” that means the facility is open during late evenings, nights, early mornings, and weekends. Depending on the facility, the security might be needed all hours of the day.

Regarding the facility areas there are four different types of areas that need to be considered when doing the vulnerability assessment. The initial analysis is to understand if there are any public areas that can be accessed by anyone. The second area is the rented or assigned area, where a tenant has the possibility to rent a specific area for a specified time. The maintenance area is another area that needs to be evaluated and analyzed. The last area is the restricted area where all visitors need to have the right credentials to enter.

A Tier one facility according to FEMA 452 is a standard commercial office building. The initial step is to review the technical schematics and the site analysis so the investigator can get a general overview of the building itself and its environment.

The secondary part of the tier one analysis is to go through the critical core functions and do a general vulnerability assessment. The mitigation plans of the building are also written down, and everything is logged in the DHS database. Everything is presented to the management of the building, and a small portfolio is constructed with recommendations for the management. The portfolio only targets the general facility, and the security systems and procedures of it.

According to FEMA 452 the most significant factors that the report will be pointing out is how the management can prepare themselves for emergency operations, disaster recovery and other similar plans and procedures.

A tier two facility according to FEMA 452 is a high-risk building, an iconic building, governmental building, school, hospital, asset for the infrastructure and other similar buildings. The tier two analyses are more extensive and cover more areas of the facility. It also involves more security professionals.

In addition to the tier one analysis, the tier two team also analyze the structure and building envelope of the facility, the mechanical and power systems, the landscape where the facility is located and its IT system. The report portfolio will contain the same scope as tier one but with additional information regarding costs for mitigation options for blasts, CBR and physical security upgrades.

A tier three facility according to FEMA is a "high value and critical infrastructure" (FEMA 452 2005, 3-3). It is an in depth analysis with the mindset that explosives and weapons of mass destruction will be used against it. The tier three evaluation is the highest level according to FEMA, and therefore includes a number of additional sections of importance, such as the effects of a blast occurrence.

The Ministry of defense "uses KATAKRI (2011) as their primary tool when checking the fulfillment of security requirements" (Ministry of Defense 2013). "The main goal of the National Security Auditing Criteria is to harmonize official measures: when an authority conducts an audit in a company or in another organization to verify their security level. The second important goal is to support companies and other organizations as well as authorities with their service providers and subcontractors, to work on their own internal security" (Ministry of Defense 2013).

In practice, they use three levels: base level, increased level and high level. In standardized terms these would be restricted, confidential and secret. The KATAKRI (2011) looks at the following four areas: Administrative security, personnel security, physical security and information assurance.

The KATAKRI (2011) is built up in the form that the auditor has a book with four main areas (mentioned above), and in every area the auditor needs to evaluate the particular statements according to KATAKRI (2011) against the level of the organization being audited.

According to Renfroe & Smith (2011) the categorization of a facility can be divided into four different categories:

Category	Description
Very high	This is a high profile facility that provides a very attractive target for potential adversaries, and the level of deterrence and/or defense provided by the existing countermeasures is inadequate
High	This is a high profile regional facility or a moderate profile national facility that provides an attractive target and/or the level of deterrence and/or defense provided by the existing countermeasures is inadequate
Moderate	This is a moderate profile facility (not well known outside the local area or region) that provides a potential target and/or the level of deterrence and/or defense provided by the existing countermeasures is marginally adequate
Low	This is not a high profile facility and provides a possible target and/or the level of deterrence and/or defense provided by the existing countermeasures is adequate

Table 1 Categorization of a facility according to Renfroe & Smith (2011)

2.2 Physical condition

When the Vulnerability Assessment team has chosen the level of analysis they want to conduct the first item on the list is to investigate the physical condition of the facility. The physical condition of the facility can be divided into six different areas according to FEMA 455 outline and "The design and evaluation of physical protection systems".

The first category is about the country and the placement of the facility. The initial step in the physical condition is to make sure that the vulnerability assessment team understands that every region is different. The political climate, local inhabitants and neighboring companies/residents can and will play an important role of the assessment.

Second category in the vulnerability assessment is to look at the topography and the surroundings. The topography aspect is very interesting the further away the facility is located from neutral land or familiar areas. By placing, constructing or even rearranging the assets inside the facility, the surrounding area can either act as an asset to the facility or as a weak spot.

The surrounding aspect is more focused on the aspect of what kind of other important facilities or areas exists in the nearby surroundings. According to FEMA 455, the surrounding area is divided into three different areas: Zone 1 is 30m and less from the building, Zone 2 is 30-90m from the building, and Zone 3 is 90-300m from the building. The different zones play an important role depending on how far the vulnerability assessment team wants to conduct their analysis and the need for it. In some regions and for some facilities this kind of depth is unnecessary, but for others it can play an important factor if the company wants to place their facility there.

The last general zone that plays an important role, and that needs to be evaluated, is if other high value targets or communication hubs exist in the region. If a nuclear plant or an airport exists in the area it can affect the vulnerability assessment for the facility. Again the type of the facility and the depth of the analysis play an important role.

When the investigation of the surroundings of the facility is done, the next step is to analyze the facility itself. The initial step is making sure that the vulnerability assessment team has updated blueprints in their possession and, if possible, an extra set of copies that the vulnerability assessment team can make notes on. In general, the blueprints should contain information regarding the electrical system, plumbing system, ventilation system, phone and Internet cables, etc.

Schematics of the facility are also necessary because on them are the different areas such as placement of CCTV-cameras, panic buttons, alarm sensors, fire extinguishers, doors, emergency doors, windows etc. A separate schematic should be done for the hazardous areas, vital environmental areas, vital assets, etc.

The fourth category for the Vulnerability assessment team to analyze is the security installations in the facility. The vulnerability assessment team needs to look at the current security system installed if any exist. The general physical protection system is divided into four parts.

The first part is the detection, which means that the system needs to discover the intrusion, communicate the alarm to a controller and give the controller enough information so he can assess it. This part is often referred to as the outer layer of security.

The second part is a delay, which means that the system needs to be able to delay the adversary by having barriers and different layers of security so the adversary will be delayed.

The third part is the response, which means that a security force, internal or external, responds to the detected intrusion. This part is often referred to as the middle layer of security. This section belongs to the delay section, but it is not on the envelope of the building, but inside. It is referred to as the inner layer of security and depending on the type of building there might be several inner security layers.

The fourth part, which is a topic that the most modern books start to cover, is the neutralization part. The neutralization part does not mean that the security force will eliminate the adversary but rather that the security officer responding to the adversary has enough tools, knowledge and legal rights to respond and deal with the situation. It is important that the neutralization part is according to the legal requirements and demands, otherwise the consequences of the actions undertaken by the security guards and/or the security system can be worse then calculated.

The fifth category that the vulnerability assessment team needs to analyze is the exterior intrusion system. The main focus of the exterior intrusion system is to detect and, if possible, delay any intrusion attempts. The vulnerability assessment team needs to look at how the current exterior intrusion system works. There are different methods of analyzing the exterior intrusion systems and one simple method is mentioned below.

According to Garcia, “the probability of detection depends primarily on target to be detected, sensor hardware design, installation conditions, sensitivity adjustment, weather condition, condition of the equipment and acceptable nuisance alarm rate” (2008, 70).

Testing of the different systems should be done during different phases of the day and it should be done minimum ten times to ensure that the data collected is enough to give a clear picture of if the system works or not.

The vulnerability assessment team analyzes the exterior physical security system based on the factors mentioned above. The exterior physical security system should be working according to the different zones, country and placements of the facility, legal regulations, goals and objectives of the company housed in the facility, the assets it protects and according to the budget that the security department has.

The sixth category that the vulnerability assessment team needs to analyze is the interior intrusion system. The interior intrusion system works under different conditions. The vulnerability assessment team constructs their analysis on the same criteria as for the exterior intrusion system, but the central focus is on how the interior intrusion or detection system works for the security department in regards of detection and assessment.

If the intrusion system is constructed so that an alarm will go off when anyone is moving inside the building during daily operations, the nuisance alarms will be too high and most likely often ignored by the alarm operator. The vulnerability assessment team analyzes how the security officers assess each alarm, their response and communication to other security officers and the entry control itself.

2.3 Facility operations

The exterior is now completed, and the vulnerability assessment team moves forward and start working with the interior. The interior can be divided into the daily operation of the facility, non-daily operation of the facility, emergency operations, security operations and procedures.

The daily operation of the facility is usually going on between 09:00 and 18:00. During this time, most of the staff, visitors, guests, etc. are in the facility. That means that the vulnerability assessment team needs to look at, for example, how the staff arrives to the facility, behaves in the facility and how they leave the facility.

The non-daily operation is the time before the facility is open or when the facility is closed from the general employees, visitors, guests, etc. Most facilities today use a night cleaning crew to deal with the cleaning, and the vulnerability assessment team needs to analyze how they behave, work and operate during these hours.

Depending on the facility they might have their own security, hired security, or external security that arrives in case of an emergency. How the security is incorporated in the facility and trained with the local staff can and will play an important role in case something happens. The most significant factor here is that the vulnerability assessment team looks at how the staff works during an exercise compared to a plan, if any exists.

The most significant part of the auditing is to analyze how the security manages the building in the sense of opening, running and closing it. It is also important for the vulnerability assessment team to analyze if the security reports are delivered to the facility stakeholders or stopped in the middle.

The vulnerability team that conducts the analysis will depend on the structure of the facility security has reports of logged incidents. These reports will be the foundation for the vulnerability assessment team when they investigate how the security, staff, employees and others conducted themselves/behaved during an incident. The reports should be at the disposal of the vulnerability assessment team so they can analyze them and interview the necessary persons to gain an overview of how the emergency situations works in a real situation.

Depending on the facility and its function there might be "what if" plans/recommendations. These plans need to be checked to verify they are up to date and practiced with the relevant staff. In general terms, this plan is called a business continuity plan, but this vulnerability assessment analysis is only done for the security part of the facility and not for the business side or other aspects.

2.4 Facility policies and procedures

A facility can have written and unwritten policies and procedures. The management of the facility or sometimes the particular manager for their individual department in general, sets the policies of a facility. All procedures need to be approved by the highest management and in some cases even approved by the legal department.

The procedures are based on the policies that the management has approved. The procedures can be constructed very strictly or as guidelines. The structure of the procedures depends on the facility and legal requirements

The policies and procedures of the facility should be available for all relevant personnel if they are directly connected to that specific area. There is no need for having a security officer reading about the legal procedures of trading with a foreign country if they do not take

any part in the process or interact at any point with the trade. Relevant information to relevant people is the key phrase.

Even though the goals are always the same the difference between the educated and operational set of procedures can be extensive. The operational could be a more efficient method of achieving the same goal, but the risks that come with it could be greater. Therefore the vulnerability assessment team should be guided around the facility by experienced and trusted staff, but they should also have the possibility to observe how for example security officers work on a day-to-day basis.

2.5 Legal aspect

Upon entering the legal aspect of the facility it does not matter what the function of the facility is. The important aspect here is to find out if there are any legal aspects that need to be followed.

The legal aspect of a facility could be a very crucial part of how the security is structured and why some procedures are the way they are. A professional should approve the legal aspects of the facility. If something happens and it comes out that the management and stakeholders did not follow the regulations, the company might not only go bankrupt but also be liable for the consequences of their actions.

2.6 Safety consideration

Security needs and safety needs might not always go hand in hand. From the security manager point of view, security comes first, and the assets need to be protected at all times. From the human resource manager side, the most valuable assets are the employees and they should be protected at all times. Even though we are all humans we sometimes forget that even humans can and will continuously do mistakes.

The security manager should cooperate with the human resource manager to construct different safeguards that work both ways. It can be something as easy as locking the computer before leaving it.

2.7 Corporate goals and objectives

Every organization that is housed in a facility has their goals and objectives. They do not have to aim at earning money, but they do exist. For the security department, it is necessary to understand the goals and objectives of the organization.

By understanding the goals and objectives of the organization the security department can integrate their procedures with the people, procedures and equipment of the facility. That will lead to a mutual understanding of the security needs and the company will see the benefits of having a well working security department.

The vulnerability assessment team needs to look at the goals and objectives of the organization in the facility and see how that is incorporated into the procedures of the security staff of the facility.

3 Asset Identification

This segment describes the importance of proper asset identification in the vulnerability assessment. This segment is divided in several chapters and in the end of the thesis in the appendix a suggestion of asset identification document can be found. There are multiple options when a asset identification is done and in this segment the asset identification process is put together from several different methods. The methods are gathered from ASIS, FEMA 452 & 455 and Strategic Security Management, A risk assessment guide for decision makers (Vellani 2007).

In general terms, an asset is a resource of value, requiring protection. The asset itself has a value, belongs to the business function and could be difficult to replace within a required timeline. The most significant part regarding the asset identification for the VA team and the facility management is to value the assets and put everything in perspective and prioritize. Some assets might at first glance seem valuable but in the end are not.

The VA team analyzes five different areas when it comes to assets. The three main categories that the vulnerability assessment looks at are how critical the asset is to the business operations, the replacement value and value of the asset itself. The value of the asset is sometimes not measured in money, but in lives. Proper insurance can cover most of the costs, but loosing life is something that is not repairable.

3.1 Category one – People

According to Vellani (2007), the first category is the people that are inside or adjacent to the facility. When the vulnerability assessment team analyzes the people category, it contains the staff during working hours and outside working hours, visitors, visiting contractors or similar, any kind of guests, tourists and so on.

3.2 Category two – Property

According to Vellani (2007), the second category the vulnerability assessment team analyzes is the property the facility owns or consists of. The design of the facility can attract bad intentions from adversaries in the form of graffiti or destruction of the exterior/interior facility. Graffiti, vandalism, destruction of property, etc. are likely not a critical part of the business, but the visual damage can be destructive enough.

3.3 Category three – Information

According to Vellani (2007), the third category that the vulnerability assessment team analyzes is the information that the company handles. As mentioned earlier, both the FEMA 452/455 and KATAKRI (2011) divide the information into three subcategories, depending on their relevance for the company. The categories can be open information, confidential information and restricted information. In KATAKRI (2011), the division is into base level, increased level and high level. Each category has different guidelines.

3.4 Category four – Critical Assets

According to Vellani (2007), the fourth category that the vulnerability assessment team analyzes is the critical assets. The critical assets are different in every facility. In some organizations the people are the most critical assets, but in others, like a gas plant, the safeguards of the plants are critical assets and they need to be regularly monitored, otherwise the consequences can be extremely high.

3.5 Intangible assets

According to Vellani (2007) there are three principal intangible components regarding assets that the vulnerability assessment team needs to take into consideration during the assessment.

Depending on the position of the head of security he or she needs to assess every routine, procedure and policy that his or her security guards follows. Different levels of security and different methods of approaching different types of problems will affect the reputation of the security of the company. The bad reputation of the security of the company will affect not only the security guards, but also the trust of internal and external colleagues.

The second area of intangible assets that needs to be evaluated belongs more to the business side and less to the security side. It does not mean that they will not affect each other, but the creditworthiness of the company does not on a regular basis belong to the security side.

Regarding the viewpoint of relationships to other companies, the security department can play an important role. The security manager and his/her security officers can create a friendly atmosphere in the area by being friendly, giving a helping hand and supporting in the ways they can without compromising the security of the facility or themselves. The relationships to other companies are always important.

By creating a goodhearted relationship with the immediate nearby companies, the security officers might receive information about a potential threat before they even spot them by themselves.

3.6 Scale of measuring the relevance of the assets

In his book, Vellani (2007, 20) mentions a four level relative scale for measuring the relevance of the assets.

Category	Description
Low	A manageable impact to business operations and no likelihood of mission failure
Medium	Moderate operational impact that may only affect a portion of the business processes and for a short period of time
High	Serious unwanted impact that may impair normal operations in their entirety or complete loss of a portion of operations for an extended time period
Critical	Asset that, if lost, damaged, or destroyed, can result in mission failure

Table 2 Relative scale for measuring the relevance according to Vellani (2007)

Another method for valuing the assets is by using a cost formula, as suggested by ASIS:

K= (Cp + Ct + Cr +Ci) -I

K = Total cost of loss

Cp = Cost of permanent substitute

Ct = Cost of temporary substitute

Cr = Total related costs (removal of the old asset, installing new, etc.)

Ci = Lost income cost

-I = Available indemnity or insurance

3.7 Asset identification in aspects of an adversary

The VA team needs to include the method of thinking of different terrorist groups in the Asset identification. The symbolic value of a building, organization or assets inside the facility may play such an important role in the Asset identification that everything else is ruled out.

The vulnerability assessment team needs to analyze the organization, and rank according to the suggested scale above each asset that exists in the company. In the next chapter “Threat Assessment” the threat against the organization will be analyzed, and a clearer picture regarding the connection between the threat and the asset is given.

4 Threat Assessment

This segment describes the importance of proper threat assessment in the vulnerability assessment. This segment is divided in several chapters and in the end of the thesis in the appendix a suggestion of threat assessment document can be found. Several options exist and in the appendix a suggested document can be used as a reference template. The main ideas are taken from FEMA 452 & 455, ASIS and the books written by the authors Vellani, Bringer et al and Garcia.

The threat assessment team needs to overlook the full range of adversaries that could affect the given facility. Authors such as Vellani (2007) and Garcia (2008) generalize the adversaries in three main groups.

The threats can be insiders, outsiders and outsiders working together with insiders. After these three broad groups, we have natural disasters and accidents. Basically, the threats are divided into human and non-human related threats.

The threat analysis is divided into the following areas: gathering information on potential threats, analyzing the different adversaries, their capabilities, finding the general interest of the adversary and the assets of the facility (likelihood) and creating an overview.

4.1 Gathering information on existing and potential threats

The initial step in the threat analysis is to gather as much information as possible from different sources. The vulnerability assessment team needs to divide the sources according to the capabilities of its members, but also according to the individual connection that every person might have

As an example, the Vulnerability assessment team can distinguish the human threats in the following categories: Terrorists (international, domestic), Criminals, Extremists, Vandals, Foreign intelligence personnel, Psychotics, Industrial Espionage, and Insiders.

The amount of terrorist groups that exist in the world is huge, but luckily the different groups can be in general divided into regions, aims and goals, relevance and more.
A terrorist group is driven by political, ideological and issue-oriented reasons. The vulnerability assessment team does not need to investigate how different cells in different groups function, but they need to understand that the terrorist groups (in general) work in small teams, are well trained, highly skilled, sophisticated and not afraid of using heavy weapons and creating casualties and devastation.

The vulnerability assessment team needs to look at the given facility because the varieties of terrorist groups are vast. Terrorist groups can come in many forms such as ecological groups, white supremacists groups, environmental groups, animal activists groups etc. In YLE News (2012), Antti Pelttari of the Finnish National Security Intelligence Service said, “the amount of people linked to terrorist groups in Finland has multiplied in the last decade”.

When the Vulnerability assessment team investigates the criminal category they can use official sources (see below). Criminals in general are driven by profit or economic gain, and visible assets are the ones in the danger zone.

Extremism in the European region is growing, and until the last couple of years they have mainly been involved in fighting, protesting, demonstrating, and writing articles/hate blogs, but after the attack in Norway by Anders Breivik, the general idea about the danger extremists pose has radically changed. Information regarding extremists can be found by using intelligence sources, different scholarly papers and books.

In general terms, vandals do not pose any sophisticated or large threat to a company. The intentions of the vandals are usually to vandalize, spray graffiti and create a mess in the area of their location.

The vulnerability assessment team started with the facility characterization, and during this stage the need for investigating the threat from foreign intelligence personnel will clearly evolve. A typical facility that encounters foreign intelligence personnel is technological companies.

In the book Security Risk Assessment and Management (Biringer, Matalucci & O´Connor 2007, 55) define an insider as “anyone with knowledge of operation or security systems and who has unescorted access to facilities or security interests” (2007, 55). An insider can be passive (provide information), active non-violent (shutting off alarm system, CCTV etc.) or active violent (fighting, shooting, destroying etc.).

4.2 Intelligence sources

The most reliable sources that exist are the reports made by the local authorities. The reports are official documents and can be ordered from the police or other law agencies.

The second intelligence source is companies around the facility. By investigating the nearby surroundings, the vulnerability assessment team can, if possible, create a new network consisting of security managers from neighboring companies where information can be shared.

The thirds intelligence source is different organizations and companies. There are numerous companies that can provide the information needed. There are also organizations such as ASIS that provide the possibility for security managers to meet and share information and solutions.

4.3 Crime analysis

There are different non-profit organizations, schools, universities, departments, etc. that conduct crime analysis on a local and national scale. By working together or at least by going through their information, the vulnerability assessment team can create a general picture of the current and historic crime situation.

If the facility is a more attractive place for adversaries the vulnerability assessment team can study international studies or reports from international organizations to see how similar buildings in other countries in the nearby area and further have been affected. Common

crimes are usually not evaluated in the threat spectrum so therefore it should have its own analysis based on statistics done by the authorities.

4.4 Published literature

Libraries, professors, students, newspapers, private persons and more can be a useful source of information. Studies or reports by local and national newspapers and universities can be very helpful if other official documents do not exist or there is a lack of them.

The vulnerability assessment team can also look at the local library if any up to date books exist about the threats concerning their facility.

4.5 Government directives and legislation

Depending on the facility, the vulnerability assessment team analysis might have to take into account some legal directives and legislation that need to be obeyed. This is already mentioned in the facility categorization as an important factor in understanding how the building operates and why some procedures need to be done in a specific order or with a specific method.

4.6 Capabilities of the adversary

When the vulnerability assessment team has gathered all the information mentioned above, they are obligated to understand the capabilities of each adversary category that exists. It is significant that the Vulnerability assessment team analyze each adversary thoroughly because the findings of the analysis will lay the foundation of the amendments to the current physical protection system.

According to Biringer et al. (2007), the capabilities of the adversaries can be divided into ten different categories.

Category	Short description
Motivation	The motivation level of the adversaries differs and therefore the scoring of this category should be accordingly.
Tactics/Method	Different threats use different tactics/method to achieve their goal and objectives.
Intelligence Gathering	Depending on the goals and objectives of the threat the level of information gathered for the event differs.
Level of interest	Different facilities give different level of interest from the adversary.
Equipment of the adversary	Depending on the adversary the access to a different type of equipment can vary from basic tools to sophisticated military grade equipment.
Transportation	Depending on the categories mentioned above the transportation needs is something that needs to be thought of.
Weapons/Explosives	Depending on the threat and their goals and objectives the use of weapons and explosives is something that should fall in a different category due to the implications it can create
Level of knowledge	Depending on the desired outcome the level of knowledge from the adversary differ.
Financial support	Depending on the categories mentioned above the financial support for the adversary could play and important role
Collusion with an insider	Depending on the goal and objective of the adversary the help of an insider could mean the difference between success or failure.

Table 3 Categories of capabilities (Biringer et al. 2007, 56-57)

In general terms, the motives are based on the goals and objectives of the adversary. The motives can be based on financial gain, ideology, personal reasons, hostility, revenge, psychosis (mental illness) etc. Some adversaries might conduct an illegal act against a facility to create a statement due to its connection to their cause, and of course terrorists might conduct acts to create terror, mass casualties, economic disaster etc.

Each threat against the facility can use different tactics to achieve their goals. A heroin addict that breaks in to steal a forgotten wallet is completely different from a rival company that wants to steal the company secrets. The methods need to support the motivation that is based on the goals and objectives of the adversary.

When the intelligence gathering means are discussed, they depend on the sophistication of the tactics and motivation regarding the different levels of information needs of the adversary. As mentioned above, the addict that passes by the facility will use a more direct and quick tactic to attain his goal while the information thief from the rivaling company needs to analyze and invest more time in the attack. The same way of thinking is applied to each threat depending on their tactics, motivation, and goals and objectives.

The target of interest is also something the vulnerability assessment team will need to analyze due to the fact that different assets attract different threats. By defining the different threats and their interests, the vulnerability assessment team can understand and make a better analysis of the facility and how the adversary will think. Depending on the interest of the adversary, their goals and objectives, their motivation, the target, and their intelligence information, the adversaries will either work alone, in small groups or even in cells. Each threat acts differently, and it should be taken into consideration by the vulnerability assessment team.

The next step for the vulnerability assessment team is to look at the most common equipment the different threats are using. By going through the steps above the vulnerability assessment team can quickly, based on past incidents, similar incidents and common sense, start to understand what kind of equipment the threat will use against the facility. By analyzing the equipment needed the vulnerability assessment team can start to see if any soft spots exist.

Different threats use a different type of transportation to the targeted facility. The person who wants to break in and steal something small might walk but the adversaries that would like to do a smash and grab need to use a minimum two cars to conduct their attack.

Another important factor concerning the adversaries and their equipment is if they are using any kind of weapons. Crime analysis and trends in the particular area, region, country, laws and regulations, past incidents, and similar incidents need to be analyzed so the vulnerability assessment team can have a better understanding of any forms of weapons that might be used and how they are used. Each adversary will act differently and his or her skills and knowledge vary. The person who wants to break in through a window needs fewer skills compared to a person who would like to steal company secrets or conduct a terror attack.

Some crimes need financial support while others demand more resources, and more resources means greater possibility to get caught. Depending on the threat and the factors mentioned above there is always a possibility that the adversary will conduct his act together with an insider. The central problem with an insider is that he or she has access to the assets in most cases without being checked.

4.7 Example of threat capability spectrum

When a threat capability spectrum is constructed the auditor should consider the following areas: information about the adversary, history of the adversary and attractiveness of the target in the eyes of the adversary. Each category is filled with subcategories and a general threat capability spectrum of each subcategory can be found at the end of the appendix.

In general terms the information category contains subcategories regarding the needed information about the adversary under investigation. The history of the adversary is information needed to understand the past activities of a specific adversary in the aspect of a specific facility. The last category is the attractiveness of the facility for the adversary. By understanding how interested an adversary is of the protected building, the auditor will understand to what kind of extent will the adversary go to achieve his goals.

4.8 Calculate the threat spectrum and evaluate the risks

The threat spectrum above is an example constructed by using threat spectrum tables from FEMA 452, FEMA 455, and the works of Vellani (2007), Garcia (2008), and Biringer et al. (2007). The purpose is to give a hint of what kind of threat levels different threats possess against a given facility. The lists above do not work unless the Vulnerability assessment team creates a list of potential threats that the given facility can encounter.

According to TRA-1 (Communications security establishment Canada C-2 2011) a threat spectrum can consist of the three main categories: deliberate, accidents and natural hazards. The three categories consist of in total 260 threats that need to be categorized and analyzed.

Some facilities have more sophisticated threats and others have less sophisticated where a shorter analysis can be done to conclude the threat analysis. To be able to do a proper threat spectrum, a crime analysis needs to be done. The police usually do the crime analysis, and statistics are published for the general audience (International statistics on Crime and Justice 2010).

The given value can be transformed into numbers, and it can be further developed if the Vulnerability assessment team thinks it is needed. For this thesis, the different values H, M, L are given the values 3x.2x.1x. That means that the highest value regarding the information about the adversary can be 14*3 = 42p. The highest value regarding the attractiveness of the adversary can be 3*3=9p. So by drawing a simple X/Y (information/attractiveness) chart the values and threats will be more tangible and comparable.

The federal security risk management uses the following model to determine the risk level for each threat

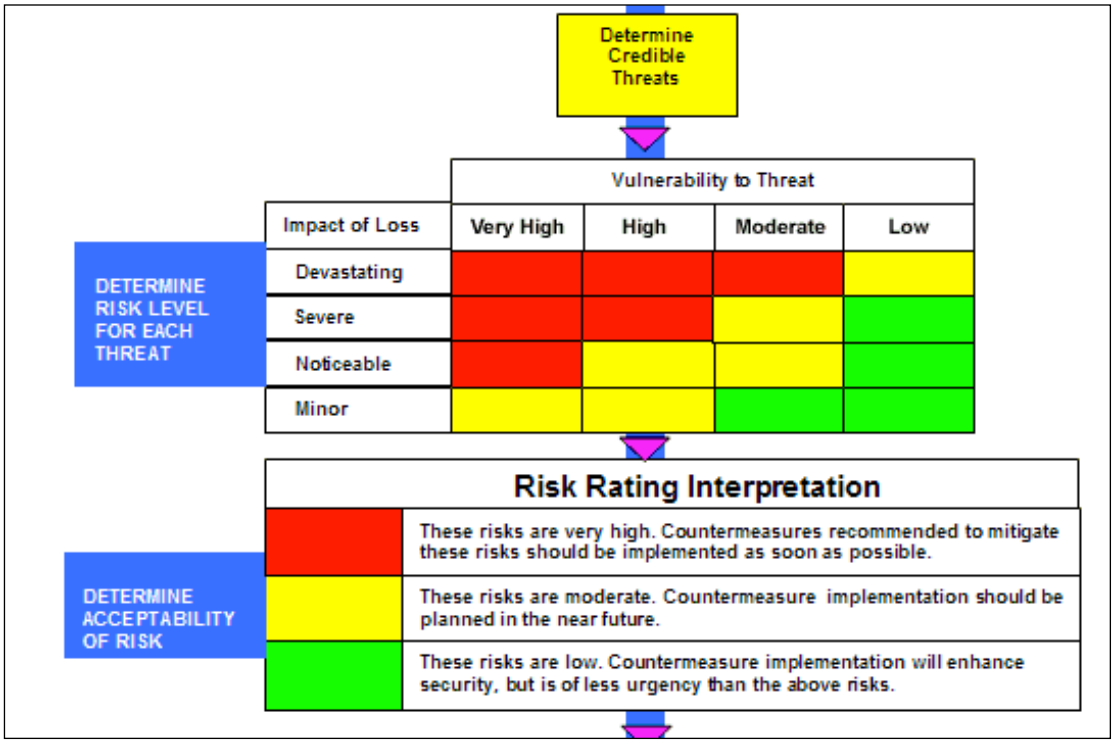

Figure 3 Threat/vulnerability assessments and risk analysis risk rating

According to Renfroe & Smith (2011) the different impacts of loss levels are defined as:

Devastating: The facility is damaged/contaminated beyond habitable use. Most items are lost, destroyed, or damaged beyond repair/restoration. The number of visitors to other facilities in the organization may be reduced by up to 75% for a limited period of time.

Severe: The facility is partially damaged/contaminated. Examples include partial structure breach resulting in weather/water, smoke, impact, or fire damage to some areas. Some items/assets in the facility are damaged beyond repair, but the facility remains mostly intact. The entire facility may be closed for a period of up to two weeks, and a portion of the facility may be closed for an extended period of time (more than one month). Some assets may need to be moved to remote locations to protect them from environmental damage. The number of

visitors to the facility and others in the organization may be reduced by up to 50% of a limited period of time.

Noticeable: The facility is temporarily closed or unable to operate, but can continue without an interruption of more than one day. A limited number of assets may be damaged, but the majority of the facility is not affected. The number of visitors to the facility and others in the organization may be reduced by up to 25% for a limited period of time.

Minor: The facility experiences no significant impact on operations (downtime is less than four hours) and there is no loss of major assets (Renfroe & Smith 2011)

5 Auditing

This segment describes the importance of proper auditing in the vulnerability assessment and in the end of the thesis in the appendix a suggestion of auditing document can be found. The auditing process itself varies extensively depending on the targeted facility but the central part of the auditing chapter is taken from the author Broders who wrote Risk Analysis and the security survey. 4nd Ed.

The security audit that the Vulnerability assessment team conducts will evaluate how the security system performs against a set of criteria set previously. The central criteria should be based on the threat assessment done earlier and on the crime analysis.

The auditing needs to follow a logical order and in a vulnerability assessment for security installations it should be done from the outside in. It follows the principle of detect, delay and, in some cases, neutralize.

“Purpose of the Survey: To identify critical factors affecting the security of the premises or operation. To analyze vulnerabilities and recommend cost effective solutions” (Broder 2012, 55).

The auditing is based on the principles of detect and delay (the delay part is at this moment an estimation). The assessment and every section of it that undergoes auditing will be divided into these principles and evaluated. The most significant aspects to remember during the auditing are the timeframe at hand, purpose, and the type of facility, threats against the facility, level of knowledge from the auditor and if it is a quantitative or qualitative assessment.

The assessment and auditing in this thesis are based on the qualitative assessment because the time to evaluate a specific building is usually limited. Other positive benefits from a qual-

itative assessment are the ability to use manpower with lower knowledge of security and achieving the goals with satisfactory results. To be able to comprehend the audit use L, M, and H (Low, Medium and High) in aspects of how secure the specific object is.

In general terms, the audit can be divided into different groups, and each group requires specific evaluation information beforehand. The evaluation information needs to be based on the legal requirements, the need for protection, internal and external requirements, if they exist (for example ISO standards). The following subgroups need to be evaluated: perimeter area, exterior doors, exterior windows, other exterior entry points, security checks (gate, door, exterior, interior, exterior lighting, keys, safes (backups) etc.

The first part of the audit is to evaluate the perimeter, its existence, and its ability to detect an intruder. Not all facilities have a perimeter defense such as a fence, walls, natural elements such as rivers, mountains, or a clear line of sight (military posts and prisons) etc. Therefore for most facilities the perimeter is the shell of the building (walls, emergency exists, windows, etc.) Some examples will be used to show how the audit should be conducted and what kind of information is needed to understand the level of security and how to perform a basic audit.

Type	**L**	**M**	**H**	**N/A**	**Comment**
Perimeter Fence					
L = Lack of fence					
M = Fence exists, but only partial of the area is sealed off					
H = Fence exists, and provide security against for example an intruder					
Type of fence?					
Type of locking mechanism?					
Clear area on both sides of the fence?					
Estimated time to penetrate?					
Vulnerable according to threat assessment?					
Perimeter lightning					
L = Lack of lighting					
M = Partial lighting of the perimeter area					

H = Perimeter lighting exists and covers all the surrounding areas					
Is the lightning working with other means of security?					
Is the lightning constant or by movement?					
Estimated time of effectiveness?					
Vulnerable according to threat assessment?					

Table 4 Basic audit template

6 Red Teaming

This segment describes the importance of proper red teaming in the vulnerability assessment. The central parts of the red teaming segment is gathered from the Red Teaming guide (UK Ministry of Defense 2013) and The information design Assurance Red Team (Sandia 2009).

According to the UK Ministry of Defense (2013, 1-1),"Red Teams and Red teaming processes have long been used as tools by the management of both government and commercial enterprises. Their purpose is to reduce an enterprise risk and increase its opportunities…Red Teams are established by an enterprise to challenge aspects of that very enterprise´s plans, programs, assumptions, etc."

Red teams within IT Security often consist of so called "white hats" that have not only the legal authorization to conduct the checks, but they report their findings back so the targeted company can use the information and improve their security.

According to Sandia (2009b), red teaming is defined as "authorized, adversary-based assessment for defensive purposes.". The management of the target facility authorizes the assessment and the idea is to conduct different exercises so the security can be evaluated.

According to UK Ministry of defense (2013) the objective of the red team can be categorized into three different categories. The first category is the Diagnostic phase, the second category is the Creative phase and the last phase is the Challenge phase.

For the vulnerability assessment team, the most relevant phase would be the Challenge phase where the red team can analyze the security installations by acting as the adversary within a particular framework. Before acting as the adversary it is necessary to create a general pro-

gram regarding the red team. According to Sandia (2009b) the red team program should be divided into four phases.

Phase one is to understand the need of a red team in a vulnerability assessment analysis. To use a red team without understanding the purpose of the red team is only creating more work for the assessment. The red team needs to understand what we want to achieve and work accordingly.

The second phase is to determine what the red team needs to do. Is it a penetration attempt, acting as different adversaries and verifying the security, checking the information quality, analyzing the equipment and needs, or other goals? Some needs might require that the red team have access to all the material, and in other cases the red team needs to work separately as a stand-alone unit.

The third phase is to determine the people that should be part of the red team. Depending on the needs and the goals, of members of the red team can and should differ. In some cases, the members need to have more experience in the security field and in other cases it can be more on an academic level.

The fourth phase is how the outcome of the red team will be used in the vulnerability assessment. The findings of the red team can be, depending on the level of the red team, down to the fundamental structure or only focusing on the central points. Depending on the need and the goal (phase one and two) of the red team, the report and outcome of the red team should be structured up before the operation is started.

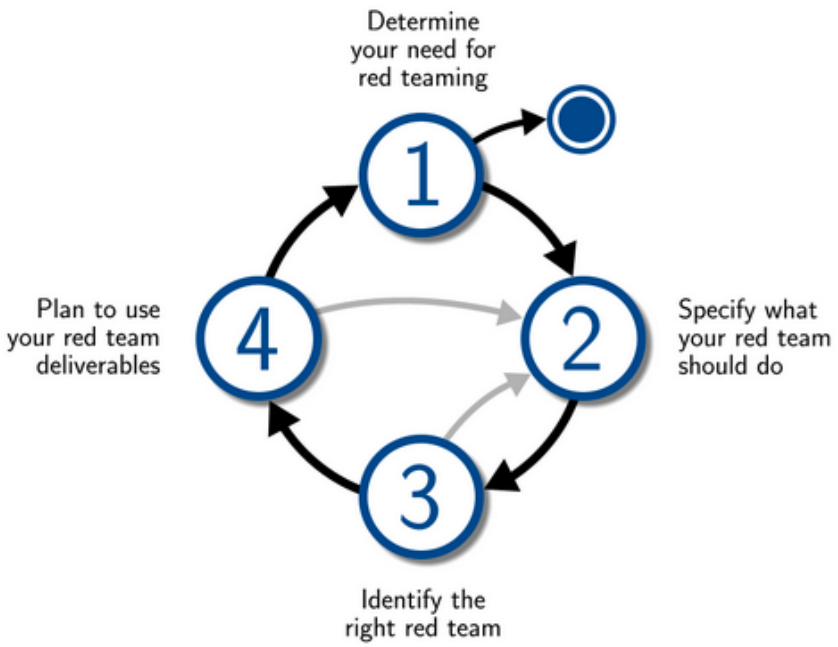

Figure 4 Sandia Red Team Process (2009a)

When a vulnerability assessment team takes the decision to use a red team, the following guidelines (example) should be used so the risk of safety and security issues is limited.

Area	To think about
Authorities	▪ Make sure the proper authorities (& security companies) are aware of the audit so no emergency situation will occur ▪ If needed, place a police car in the area so in case of emergency during the audit ▪ Make sure that the alarm system is put in testing mode (should still give signals)
The company	▪ Make sure that a contact person at the company is aware of the audit and what systems/department/area is audited ▪ A letter signed by someone in the audited company should be drafted and worn by the red team person in case he needs to identify himself
Use of force	▪ No force or act of force is allowed to be used against security staff, or other workers ▪ In case off force is used, the audit should immediately stop and identification (letter) should be shown

Items	▪ Every suspicious item that is brought into the facility should be clearly informed to the supervisor so it will not be forgotten after the test ▪ Every suspicious item that is brought into the facility should be clearly marked as a dummy so no one will call the emergency units or start emergency procedures
Rules for the red team members	▪ Safety is priority number one, and in case a red team member foresees a potential threat to their safety or the people involved in the exercise, the red team member should immediately stop the audit. ▪ A red team member is not allowed to change the audit without consulting the leader of the audit.

Table 5 Basic topics to be considered before a red teaming exercise

7 Vulnerability Assessment Report

This segment describes the importance of the vulnerability assessment report done from the vulnerability assessment. A general template for a vulnerability assessment report can be found in the appendix.

The vulnerability assessment report that will be presented to the management for further analysis and decisions on how to proceed can follow this structure. There are several templates on the Internet that could be used when writing the security assessment report. A good example is a template written by Watson (Watson 2005).

There are several different methods of writing a vulnerability assessment report, and according to the findings of this thesis, the best method is to keep it short, based on facts, and direct to the point. The report itself will be directed to the management of the company and the person in charge of the security (unless the author is in charge of security), and in most cases relevant staff such as fellow security workers. In the Appendix a basic template based on the template made by Watson (Watson 2005) can be found.

8 Project Management

This segment describes the importance of proper project management skills in the vulnerability assessment. The project management process itself varies extensively depending on the targeted facility. The project management method used in this thesis is gathered from the book "Strategic Security Management" by Karim H. Vellani (2007). The reason for choosing this method is the to the simplicity and effectiveness.

A vulnerability assessment is a time consuming project that depending on the extent and resources can take anything from a couple of hours, to days or weeks. To help the designated individual conducting the vulnerability assessment the process should be done as a project. If project management is googled the number of hits exceeds 300 million. To be able to find the most appropriate methodology can be very time consuming and therefore in this thesis the project management methodology comes from "Strategic Security Management" by Karim H. Vellani (2007, 251-263).

The reason for choosing his methodology over other tools or software is due to the simplicity and the adaptability of the methodology, and due to the fact that the person doing the vulnerability assessment does not need any equipment that would cost money. If the person conducting the vulnerability assessment is used to a specific project management tool or methodology can and most likely should continue with that approach. In this chapter the project management methodology comes from the book Strategic security management that was mentioned above.

To reach successful completion in a project there are three central components that need to be fulfilled. The first one is the scope, second is time, and the third is the costs. These main subjects can and most likely will be further defined depending on the size of the project. Each project is, as stated above, unique and therefore it should be treated as such.

The primarily reasons for using this method are because of the simplicity, clear assignments, ease of beginning and not requiring any special software or tools. The appropriate project management method, if one is required, is up to the reader and their knowledge regarding different project management tools. There are project management tools that do not cost anything such as GanttProject, Open Workbench, jxProject, in addition to software and sites that can provide the necessary tools/software for the person undertaking this project. Project Management Institute is one of many examples of a site where a person with no knowledge regarding project management can sign up, undertake webinars regarding project management and get help to create a template for the vulnerability assessment project.

8.1 Development

The main tasks that need to be done within the development section are defining what the project is about (scope statement), constructing concrete goals and objectives, coming up with a strategy, trying to locate the risks, constructing a project charter and identifying the stakeholders in the project. Sometimes the project needs to follow regulations/laws, internal requirements, etc. and therefore the definition of the project might grow.

In the Vulnerability Assessment project, the development stage is a crucial stage because it sets the tone of how extensive the project will be. If the development part is written in a general and vague form, the project can be never-ending. If possible, the auditor should go through any old vulnerability assessment analysis done within the company or other relevant/similar facilities to understand the best strategy to undergo this project with the resources given and the knowledge and manpower available.

8.2 Planning process

“Depending on the nature of the project, planning, may be an extensive, time-consuming process or it may be a simple, streamlined process” (Vellani 2007, 252). The most important part in the planning process is to write down the summary tasks and individual tasks requirements. Summary tasks are the general tasks that the project consists off, and the individual tasks are the tasks within every summary task that must be done before that section can be closed. Sometimes several summary tasks can be initiated at the same time and others need to wait until another summary task is completed.

In the planning phase, the Project Manager has an important role to make sure the necessary resources and equipment are at hand for their team members. They also need to be supportive of the Project Management members.

8.3 Execution phase

The execution phase of the project is the most time consuming part of the whole project. In this phase each individual that belongs to the project starts to collect the relevant raw data, and update other members of their process. Depending on the nature or construction of the project, the individuals might have physical or non-physical meetings to present their status, findings, problems or advancements.

Each Summary task (deliverables) has individual tasks. For example, the facility documentation summary tasks consists of documenting the physical conditions, the facility daily and

none daily operations, policies and procedures, regulatory requirements, goals and objectives of the company etc. One of the most important factors in the project management is the control structure where the project manager can make sure that each individual is doing the assigned tasks and on time, otherwise the project might be delayed.

8.4 Conclusion phase

The conclusion phase is the phase where everything is put together, and a report is generated. Depending on the size of the project and the audience the report is intended to, the extent of the report varies. The conclusion phase ensures that the scope and the objectives of the security project have been met, quality of the work performed, and that all required documentation has been completed.

The significant sections regarding project management and vulnerability assessment is that in the conclusion phase each segment investigated is analyzed and the project management group needs to analyze if the budget was on target, otherwise future changes might be required, if the work was done in the time given otherwise future scheduled work might need an adjustment, the end result of each segment and if it is in a satisfactory level.

9 Conclusion

This thesis contains guidelines regarding project management, facility categorization, asset identification, threat identification, auditing, red teaming and the manager report.

The project management chapter describes the general process of how a vulnerability assessment can be done. I tried to identify the critical parts of the project and make sure the reader understands the basics. There are numerous project management tools and the person conducting the Vulnerability assessment needs to take several critical aspects such as time frame, level of knowledge, resources, experience, level of assessment and more into consideration before the project is started.

The facility categorization chapter describes the general process of the common knowledge regarding the facility that is necessary to know before anything else is done. Many vulnerability assessment teams tend to forget to analyze aspects such as the surroundings, terrain, neighboring companies, population density and more.

The third part is about the asset identification. Several security organizations and vulnerability assessments tend to start with the threat analysis and then the asset identification. In the majority of the cases the vulnerability assessment team conducts the assessment on a fully

operational facility and therefore at this point the different assets have fixed places, and it is necessary to analyze where they are before going into the threat analysis. To be able to understand how the adversary thinks and acts you need to understand what they are after.

The fourth part is about the threat assessment, which means that the vulnerability assessment team starts to analyze the adversaries they think could act against their facility. There are numerous threats that could be taken into consideration, but by first categorizing the facility and identifying the assets, the vulnerability assessment team can leave out or prioritize the most up to date threats against the given facility.

The vulnerability assessment team needs to understand that a threat analysis is one of the most dynamic chapters in the vulnerability assessment if we think about how rapidly it can change.

The fifth part is the auditing that the vulnerability assessment team conducts on the facility and staff itself. The audit can be divided into the project itself, and some parts can be done in the beginning during the categorization and by allowing the facility staff to fill in the information, while other parts of the auditing needs to be done by the vulnerability assessment team themselves. The most important part here is to understand the threats against the facility and to conduct the central part of the audit with that in mind.

The sixth part of the vulnerability assessment is the red teaming. Red teaming means in general that the vulnerability assessment team conducts different tests to see how, for instance, the general staff and/or security staff reacts to different problems or situations. Some organizations use this tool very often to keep their staff up to date and alert.

Part seven, last part, is the vulnerability assessment report itself. Depending on the vulnerability assessment team and their work, the gathered amount of information can be huge and serve as a vital component for further security development, but the vulnerability assessment report is a report for the management. The management does not need to know every detail about the assessment, but they do need to know the relevant aspects.

My findings are that this thesis is a very basic tool for future security managers, but it is a good starting point to continue further development in aspects of vulnerability assessment. Majority of security companies today want to sell their products at the highest price and care very little about the actual threats and/or the deeper assessment that needs to be done so the proper equipment, and in some cases cheaper and more efficient equipment, can be bought and installed.

The amount of knowledge that has been written regarding vulnerability assessment is huge and therefore the first limitation of this bachelor's thesis is the lack of complete coverage of all the written material. The first and most important aspect is that the companies that conduct vulnerability assessments are reluctant to share their methods because it actually means that a potential adversary can understand how the security is constructed.

The second limitation of this thesis is the vast and diverse information regarding how a vulnerability assessment should be done. There is no correct and simple method and the most important factor the vulnerability assessment team should rely on is their knowledge and experience.

The dynamic world we live in is the third limitation to this Vulnerability assessment. Our adversaries develop new methods to achieve their end goals and therefore a standard or method set today might be obsolete very quickly.

Due to the fact that vulnerability assessment is something that I personally am very interested in, I will continue to work on my own templates and update them with the latest information I can receive. Hopefully one day I will have enough knowledge to put everything in a computer based program so a more accurate calculation and assessment can be conducted.

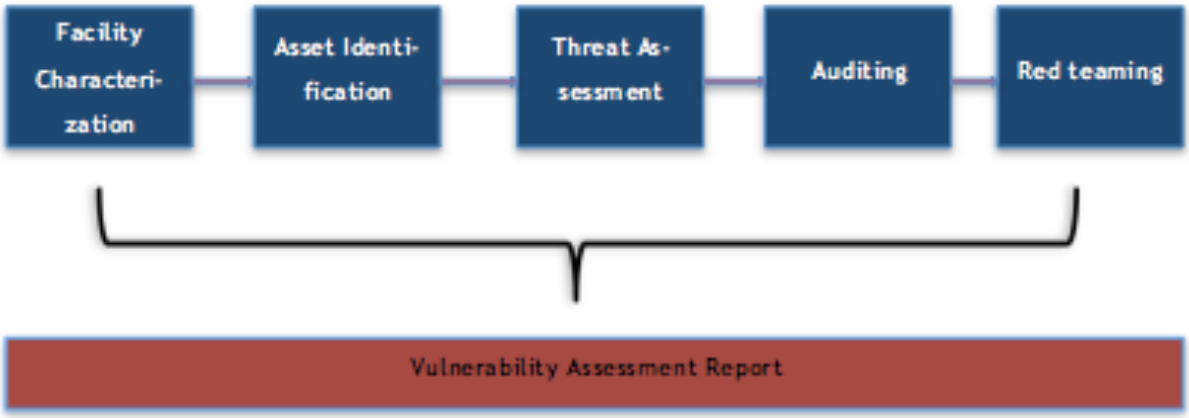

Illustration 1 Vulnerability Assessment process summary

References

Biringer, B. Rudolph V, Matalucci, S & O´Connor. 2007. Security risk assessment and management. Hoboken:John Wiley & Sons inc.

Broder, J F. 2012. Risk Analysis and the security survey. 4nd Ed. Oxford: Elsevier Inc.

Garcia, M L. 2008. The design and evaluation of physical protection systems, second edition. Burlington:Butterworth-Heinemann.

Hair, J. Money, A. Page, M & Samouel, P.2007. Research methods for business. John Wiley & Sons: Chichester

Lukka, K. 2003. The constructive research approach. Case study research in logistics. Publication of the Turku school of economics and Business administration, Series B 1.

Vellani, K. 2007. Strategic Security Management, A risk assessment guide for decision makers. Oxford: Elsevier Inc.

Internet references

Communications Security Establishment Canada. 2011. Threat listening C-2. <http://www.cse-cst.gc.ca/its-sti/publications/tra-emr/> (Accessed 10.07.2013).

George G. Baker III. A vulnerability assessment methodology for critical infrastructure facilities. James Madison Univeristy. Harrisonburg. VA 22807. <http://www.jmu.edu/iiia/wm_library/Vulnerability_Facility_Assessment_05-07.pdf> (Accessed 24.07.2013).

ISO 31000:2009. 2009. RIsk Management. <http://www.iso.org/iso/iso31000> (Accessed 10.03.2014).

Stefan Harrendorf, Markku Heiskanen, Steven Malby. International statistics on Crime and Justice. 2010. EUNI Publication Series No. 64. Helsinki 2010. http://www.unodc.org/documents/data-and-analysis/Crime-statistics/International_Statistics_on_Crime_and_Justice.pdf> (Accessed 14.07.2013).

FEMA 452. 2005. A how-to guide to mitigate potential terrorist attacks against buildings (Hardcopy). Federal Emergency Management Agency. Show print publication. <http://www.fema.gov/media-library/assets/documents/4608?id=1938> (Accessed 21.07.2013).

FEMA 455. 2009. Handbook for rapid visual screening of buildings to evaluate terrorism risks (Hardcopy). Federal Emergency Management Agency. Show print publication. <http://www.fema.gov/media-library/assets/documents/2298?id=1567> (Accessed 24.07.2013).

Katakri. 2011. National Security Auditing Criteria. Version II. Finnish National Security Authority. Ministry of Defense. http://www.defmin.fi/files/1871/KATAKRI_eng_version.pdf (Accessed 04.07.2013).

Pelttari, A. 2012. Interview with managing director of SUPO. 27 Nov 2012. Interviewed by YLE. Helsinki. <http://yle.fi/uutiset/supo_chief_terrorism_growing_in_finland/6392166> (Accessed 10.07 2013).

Renfroe, Nancy. Smith, Joseph L. 2011. Threat/vulnerability assessments and risk analysis. National Institute of Building Sciences.

<http://www.wbdg.org/resources/riskanalysis.php> (Accessed 20.07.2013).

Sandia. 2009a The information design Assurance Red Team. Sandia national laboratories.2009 Sandia Corporation
<http://www.idart.sandia.gov/index.html> (Accessed 20.07.2013).

Sandia. 2009b. The information Design Assurance Red Team (IDART). Sandia national laboratories.2009 Sandia Corporation.
<http://www.idart.sandia.gov/methodology/RT4PM.html> (Accessed 26.07.2013).

UK Ministry of Defense. 2013. Red Teaming Guide. Second edition. Development, Concepts and Doctrine Centre. Shrivenham.
<https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/142533/20130301_red_teaming_ed2.pdf> (Accessed 30.04.2013).

Watson, Keith A. 2005. ITAS Year two Security Assessment report. Keith A. Watson. 2005.
<http://www.docstoc.com/docs/88366249/Security-Assessment-Report-Template-(DOC)> (Accessed 25.07.2013).

Illustrations

Illustration 1 Vulnerability Assessment process summary..... 42

Figures

Figure 1 ISO 31000:2009 Risk Management 10
Figure 2 FEMA 455 Rapid screening table..... 12
Figure 3 Threat/vulnerability assessments and risk analysis risk rating 31
Figure 4 Sandia Red Team Process (2009a) 36

Tables

Table 1 Categorization of a facility according to Renfroe & Smith (2011) 15
Table 2 Relative scale for measuring the relevance according to Vellani (2007) 23
Table 3 Categories of capabilities (Biringer et al. 2007, 56-57) 28
Table 4 Basic audit template 34
Table 5 Basic topics to be considered before a red teaming exercise 37

Appendices

Appendix 1 ASIS PSP reference books used for this thesis 49
Appendix 2 Sandia National Laboratories books/publication used for this thesis..... 49
Appendix 3 Additional books/publication used for this thesis 50
Appendix 4 Security analysis cover page 51
Appendix 5 Facility Characterization 52
Appendix 6 Measures keys and locks 58
Appendix 7 Access control 59
Appendix 8 Alarm system 61
Appendix 9 Floor information 62
Appendix 10 Security Policy 63
Appendix 11 Information needed for Threat spectrum..... 64
Appendix 12 History of the adversary..... 65
Appendix 13 Attractivenes against the facility in the eyes of the adversary 66
Appendix 14 Vulnerability assessment report template..... 68

The following books from ASIS PSP reference material were used:

Title	Short description
Design and Evaluation of Physical protection systems, 2nd Ed.	This book is in my opinion the most comprehensive book available regarding specific areas that a Vulnerability Assessment needs to have. It covers everything from facility characterization to Threat analysis.
Risk analysis and the security survey, 4th ed.	This book is in my opinion a good start for any security manager that would like to have basic knowledge regarding risk analysis and security surveys
PSP Reference, 2nd Ed	This book was mostly used for the theoretical information needed for the asset protection.
General Security Risk Assessment	This publication was used as a reference on how the vulnerability assessment outline needs to be constructed.

Appendix 1 ASIS PSP reference books used for this thesis

The following books/publications were used from Sandia National Laboratories:

Title	Short description
Sandia Report – Categorizing threat	The Sandia report assisted me with a fundamental framework regarding assessing a threat, and how to categorize it.
Sandia Report – The IDART methodology	This methodology gathered from Sandia report was partly used for the Red Teaming section.
Sandia Report – Security Assessment Report	The methodology used in this publication was the central point of the Vulnerability assessment chapter in the end of this thesis.
Sandia Report - A Risk Assessment Methodology (RAM) for Physical security	The methodology and risk calculation was part of the risk assessment, asset identification and general methodology used in this thesis.

Appendix 2 Sandia National Laboratories books/publication used for this thesis

The following books/publications were used from other sources:

Title	Short description
Anti-Terrorism: Criteria, Tools & Technology	A general understanding regarding documented threats, tools, and criteria was extracted from this publication.
A Vulnerability Assessment Methodology for Critical Infrastructure Facilities	This publication was used as a reference point for the vulnerability assessment content and methodology.
University of Foreign Military and Cultural Studies – Red Team Handbook	This handbook was part of the red teaming summary in this thesis.
Ministry of Defense – Red Teaming guide	This manual was part of the red teaming summary in this thesis
A tradecraft Primer: Structured Analytic Techniques for improving intelligence analysis	These guidelines helped me with the assessment of the material for this vulnerability assessment thesis, and it was also used for the red teaming chapter.
Strategic Security Management – A Risk Assessment guide for decision makers	This book was mainly used for the threat assessment, crime analysis, Asset identification, and risk assessment chapters.
FEMA 452 – Risk Assessment	FEMA 452 helped me structure this thesis regarding identifying critical assets, fundamental methodology for a vulnerability assessment, and how to access risks
FEMA 455 – Handbook for visual screening of buildings to evaluate terrorism risks	FEMA 455 helped me understand and structure up a fundamental methodology for screening a facility.

Appendix 3 Additional books/publication used for this thesis

Security Analysis

Name of the company: _____

Country / City: _____

Address of the company: _____

Person conducting the analysis: _____

Position of the analyst: _____

Contact details of the analyst: _____

Additional notes from the analyst regarding the confidentiality or the company

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Appendix 4 Security analysis cover page

Security Analysis

Facility characterization

(1/3)

Type of building (e.g. hospital):

_____

Owner of the building: _____

Companies in the facility: _____

Regarding authorities:

- Driving instructions to the closest police station:
- Driving instructions to the closest hospital:
- Emergency contacts to the closets police/hospital:
- Estimated response time for the police:
- Estimated response time for the ambulance:
- Estimated response time for the fire brigade

Connected buildings: _____

Building mode:

Employees during the working hours: _____

Predetermined security level: _____

Has a surrounding / topography picture been extracted:

- *Is the facility clearly marked in the picture?*
- *Have security zones been clearly marked in the picture?*
- *Have surrounding areas/facility been clearly marked?*

Have the following blueprints been extracted:

- *Blueprints of the floors:*
- *Blueprints of the electricity:*
- *Blueprints of the plumbing:*
- *Blueprints of existing security installations:*
- *Blueprints of ventilation routes:*
- *Blueprints of emergency routes:*

Appendix 5 Facility Characterization

Security Analysis

Facility characterization

(2/3)

Information regarding perimeter installations/Vulnerabilities

Information regarding Perimeter Fence

Type	L	M	H	N/A	Comment
Perimeter Fence					
L = Lack of fence					
M = Fence exists but only part of the area is sealed off					
H = Fence exists and provides security against e.g. intruders					
Type of fence?					
Type of locking mechanism?					
Clear area on both sides of the fence?					
Estimated time to penetrate?					
Vulnerable according to threat assessment?					
Security installations?					

Information regarding perimeter lighting

Type	L	M	H	N/A	Comment
Perimeter lighting					
L = Lack of lighting					
M = Partial lighting of the perimeter area					
H = Perimeter lighting exists and covers all the surrounding areas					
Is the lighting working with other means of security?					
Is the lighting constant or by movement?					
Estimated time of effectiveness?					
Vulnerable according to threat assessment?					
Security installations?					

Security Analysis

Facility characterization

(3/3)

Information regarding outer doors

Type	L	M	H	N/A	Comment
Outer door					
L = Door made of low security material					
M = Partially secure door					
H = Security door					
Type of door material?					
Frame around the door is secure?					
Estimated time of effectiveness?					
Vulnerable according to threat assessment?					
Security installations?					

Information regarding other openings

Type	L	M	H	N/A	Comment
Other opening					
Type of opening?					
Opening made of?					
Secure frame?					
Estimated time of effectiveness?					
Vulnerable according to threat assessment?					
Security installations?					

Security Analysis

Measures – CCTV-system

(1/1)

General Information regarding the CCTV-system

CCTV-system bought from: _____

CCTV-system installation year:

_____

CCTV-system installed by: _____

CCTV-system brand: _____

CCTV-system type of recorder: _____

Information regarding the recorder

- A manual exists (format): ▫ Yes ▫ No
- Information regarding hardware components exists: ▫ Yes ▫ No
- Information regarding password / access ID exists: ▫ Yes ▫ No
- Information regarding configuration exists: ▫ Yes ▫ No
- Operating system software backup exists: ▫ Yes ▫ No

Information regarding the cameras

- Types of cameras are installed (IP/BNC/Wireless/etc.):
  _____
- Resolution:
  _____
- Software program exists: ▫ Yes ▫ No
- Installation manual exists: ▫ Yes ▫ No
- Information regarding password / access ID exists: ▫ Yes ▫ No
- Amount of fixed cameras and where (marked on overview picture): ▫ Yes ▫ No
- Amount of movable cameras and where (picture): ▫ Yes ▫ No
- Outside cameras are weatherproof protected: ▫ Yes ▫ No
- Outside cameras are vandalism protected: ▫ Yes ▫ No
- Outside cameras are protected against animals: ▫ Yes ▫ No
- Inside camera are vandalism protected: ▫ Yes ▫ No
- Cables between cameras and recorder are protected: ▫ Yes ▫ No

Security Analysis

Measures – Keys & Locks
(1/1)

General Information regarding the Key-system

Key-system bought from: _____

Key-system installation year:

_____

Key-system installed by: _____

Key-system brand: _____

CCTV-system type of recorder: _____

Information regarding the Key-system

- Total amount of exterior door keys issued:
  _____
- Total amount of interior door keys issued:
  _____
- Total amount of master keys:
  _____
- Proper filled-in key log:
  _____
- Who will be informed if a key is lost:
  _____
- If an outside key is lost, will the locks/keys be changed:
  _____
- If an outside key is not returned, will the locks/keys be changed:
  _____
- Are spare keys stored in a secure location: ▫ Yes ▫ No
- Do sensitive areas have specific keys: ▫ Yes ▫ No
- Does the local police/rescue department have a key: ▫ Yes ▫ No

Information regarding the Lock-system

Type	L	M	H	N/A	Comment
Lock system Outside doors					
L = Basic lock with no security					
M = Medium security lock					
H = Lock with high security					
Name of the lock system					
Frame & installa-tion regarding the					

lock is secure?		
Estimated time of effectiveness?		
Vulnerable according to threat assessment?		
Security		

Appendix 6 Measures keys and locks

Security Analysis

Access Control

General Information regarding the Access control system

Type	L	M	H	N/A	Comment
Access control system					
L = No security check of anyone					
M = Partial security check (Employees vs. visitors vs etc)					
H = Everyone who access the facility is checked					
Is the access check done at the perimeter?					
Do security guards do the access control?					
Is the Access control done from a protected area?					
Vulnerable according to threat assessment?					
Security installations?					
Are deliveries checked and verified?					
Is the post security checked?					
Are badges given to visitors?					
Can the security installations					

Additional information regarding the Access control system:

_____

_____

_____

Appendix 7 Access control

Security Analysis

Alarm system

General Information regarding the Alarm-system

Alarm-system bought from: _____

Alarm-system installation year:

_____

Alarm-system installed by: _____

Alarm-system brand: _____

Alarm-system sensors: _____

Alarm-system type of transmitter: _____

Type	L	M	H	N/A	Comment
Alarm system					
L = No alarm system / Not working					
M = Alarm system exists but only internally connected					
H = Alarm system exists and is connected to e.g.police, security (own/outside) (panic buttons)					
Is the alarm system systematically checked (annually/yearly)?					
Is the system tamper/vandalism proof?					
Is the alarm system sensitive to the weather?					
How are alarms verified?					
Is the alarm system connected with other systems (CCTV)					

Vulnerable according to threat assessment?	
Where are the alarm sensors installed?	
Is there any area/s that is not covered with a sensor?	

Additional information regarding the Alarm system:

_____

_____

_____

_____

Appendix 8 Alarm system

Security Analysis

Floor information

Floor no: _____

Following information have been extracted and inserted in the designated floor info appendix:

- Floor plan ▫ Yes ▫ No
- Overview pictures of the floor ▫ Yes ▫ No
- Pictures of each room ▫ Yes ▫ No
- Pictures of the windows ▫ Yes ▫ No
- Pictures of vulnerabilities (soft spots): ▫ Yes ▫ No
- Information regarding the walls: ▫ Yes ▫ No

- Thickness:

_____

- Made off:

_____

- Security/Blast/bullet proof resistance information:

_____

Information regarding the windows

- Thickness:

_____

- Film:

_____

- Security/Black/bullet proof grade information:

_____

- Distance between the window and the outside ground level (reachable):

_____

- Asset information

- Floor overview sheet with assets clearly marked:

_____

- Security installation around the asset:

_____

Appendix 9 Floor information

Security Analysis

Security Policy

General Information regarding the security policy (SOP)

SOP was constructed by: _____

SOP was reviewed last time by: _____

SOP is approved by the legal department: _____

SOP is approved by the management: _____

SOP is in written / verbal form given to e.g. security staff: _____

SOP is in written / verbal form given to all employees: _____

SOP is read annually / periodically by security staff: _____

Does the Standard Operating Procedures (SOP) contain information regarding the following topics

Theft of property	Burglary
Assault	Bomb threats
Arson	Civil disturbance
Terrorists	General criminals
Extremists	Foreign intelligence personnel
Psychotics	Insiders

Additional information inserted in the SOP

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Type of Adversary	Objective	For example theft, sabotage, insider, fraud, extortion		
Information	**H**	**M**	**L**	**Score**
Existence, Intention & Access to region	The adversary clearly exists in the region, clear intention of attacking the facility and exists in the region	The adversary exists in the area or surroundings, low or none intention of attacking the facility but do exists in the region	The adversary has very low presence in the area, low intention of attacking and non/limited access to the region.	
Material resources	The adversary has enough material resources to conduct the attack	The adversary has some material resources but limited to fulfill a full penetration	The adversary has no material resources to conduct the attack	
Technical skills	The adversary has technical resources to conduct the attack	The adversary has some technical skills to fulfill the attack	The adversary has no technical skills to conduct the attack	
Planning/organizational skills	The adversary has enough knowledge, time and organizational skills to conduct the attack	The adversary has some knowledge, time and organizational skills to conduct the attack	The adversary has limited knowledge, time or organizational skills to conduct the attack	
Financial resources	The adversary has enough financial resources to conduct the attack	The adversary has some financial resources but limited to fulfill a full penetration	The adversary has limited financial resources to conduct the attack	
Stealth	The adversary can remain hidden under a long period of time	The adversary can for a limited period remain hidden	The adversary cannot remain hidden and will be in the process spotted	
Corporation with a Insider	The adversary needs the help of an insider or is an insider (active help)	The adversary needs some information to fulfill the attack (passive help)	The adversary needs no help from an insider to fulfill the attack	
Amount of attackers	The adversary needs to be minimum of XX	The adversary needs to be minimum of XX	The adversary needs to be minimum of XX	

Appendix 11 Information needed for Threat spectrum

Type of Adversary	Objective	For example theft, sabotage, insider, fraud, extortion		
Information	**H**	**M**	**L**	**Score**
Past interest	The adversary has shown a clear interest in attacking the given facility or similar facilities	The adversary has shown some interest in the facility or similar attacks has been executed on similar facilities	The adversary has not shown any interest of attacking the building, and no documented incidents exists on similar facilities	
Past attacks	The adversary has attacked the facility or attacked similar facilities	The adversary has attempted to attack the facility or attempted to attack similar facilities	The adversary has not attacked the facility or any other similar facility	
Current interest	The adversary has shown clear intention of attacking the facility	The adversary has shown limited interest of attacking the building	The adversary has not shown any interest in attacking the building	
Current surveillance	The adversary has been monitoring the facility and/or similar facilities and/or monitoring the area	The adversary has during limited time monitored the facility and/or similar facilities and/or monitoring the area	The adversary has not been keeping any kind of surveillance of the building	
Documented threats	The adversary had either been there before, threatened and/or against similar facilities	The adversary has to a limited extent threatened the given facility or similar facilities	The adversary has not shown any interest of the facility	
Motivation (Ideological, economic, personal)	The adversary is extremely motivated to conduct the attack	The adversary Is to motivated to conduct the attack	The adversary is not motivated to conduct the attack	

Appendix 12 History of the adversary

Type of Adversary	Objective	For example theft, sabotage, insider, fraud, extortion		
Attractiveness	**H**	**M**	**L**	**Score**
Desired level of consequence	The adversary is aiming for high level of fatality and/or economic loss	The adversary is aiming for limited or none casualty level and/or limited economic loss	The adversary is not aiming for media publicity or making a statement or aiming for a specific target	
Ideology	The adversary's ideology is on an extremist level and no other viewpoints can interfere	The adversary's is very dedicated but can with proper tools, counter measures and/or change of environment/political climate change viewpoint	The adversary's has no special ideology to convince him/her to conduct the attack	
Ease of attack	The given facility is easy to attack and has no proper physical security and/or guard force	The given facility has limited physical security and/or limited guard force	The given facility has strong physical security, security force with appropriate equipment and connection to the local authority	

Appendix 13 Attractivenes against the facility in the eyes of the adversary

Vulnerability Assessment Report

For the management

Executive summary

In the executive summary the author of the report needs to give a shortened introduction of the assignment, information about the authors, mission statement, findings of the vulnerability assessment in terms of weaknesses (amount depends on the findings), short explanation why these weaknesses are prioritized, recommendations and general budget if the recommendations are approved.

Introduction

The introduction needs to contain a more in depth explanation of the mission (background information). In aspects of the mission, the author needs to explain the scope of the vulnerability assessment (extent and limitations), co-authors, staff used, description of the company targeted and summary of the additional information that can be found in the appendices.

Laws, regulations and policies

In this section the author needs to clarify the laws, regulations and policies that the company needs to follow. This information will give a legal justification for why some of the measures need to be done to achieve the approval from the legal department, but also to make the readers understand that certain methods/rules/laws needs to be followed, otherwise there might be legal and financial consequences.

Facility characterization

The facility characterization needs to contain all the relevant information that was in the scope. The more information that can be gathered and inserted in this section will only benefit the author and the desired outcome. Once the material is gathered it can be edited and upgraded with pictures and even videos.

Asset identification

The asset identification needs to contain all the relevant information about the assets in assigned scope. The order of the assets can be divided in the groups mentioned in the asset identification chapter (tangible and intangible).

The important factor here is to rank the assets in priorities according to the intention of the company, importance, economical value and long and short-term value. The assets should also be analyzed through their attractiveness for the adversary.

Threat assessment

The threat assessment section is based on the threat assessment that can be found in the appendices (as an example). This section might be extensive and therefore the author needs to make sure that he/she understands that all threats cannot be taken into consideration. The most relevant threats against the company should be inserted in this section.

Auditing

The auditing section is based on the auditing documents found in the appendices (as an example). The readers need to understand the scope of the audit, process of the audit, sections audited, questions/procedures of the audit and in the end of the report in the appendices the questions and discoveries should be inserted.

Red teaming

If red teaming is used the scope of the red teaming needs to be explained, the mission of the red team, method used, findings, recommendations and reasons for the recommendations.

Summary

The summary should contain a short summary of the topics mentioned above, but also the suggested budget and timeframe of the suggested alternations. The extent of the summary depends on the findings and the scope.

Appendix 14 Vulnerability assessment report template