Good security = Good operation = Good Business

MGT415 | A PRACTICAL INTRODUCTION TO CYBER SECURITY RISK MANAGEMENT

SIEM = Security Info & Event management

* Privacy Rights Clearinghouse (Data breaches)

2 - Ick (Indicator of Risk)
42 - MSFT log Parser
45 - CDM (Homeland Security)
48 - Open Source/Free risk tool
78 - CSET
85 - SIEM (OSSIM)
88 - Commercial tools

415.1

A Practical Introduction to Assessing Cyber Security Risk

* csrc.nist.gov (NIST)
* enisa (european eq. NIST)

John Purcell
SANS Internet Storm Center

1
17
36
41

2
8
10 — 800-30/37/39
11
12
13/14 * (18) NIST monitoring metrics
21 - OGRCM3/ORMM, ISO
TARA, CAPEC, OCTAVE, FAIR, (STRIDE & DREAD)
GAIT(IIA); FMEA/FMECA, MASR;
0

SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

HOANG VINH NGUYEN, 175 Water St, NYC 2016-07-14 15

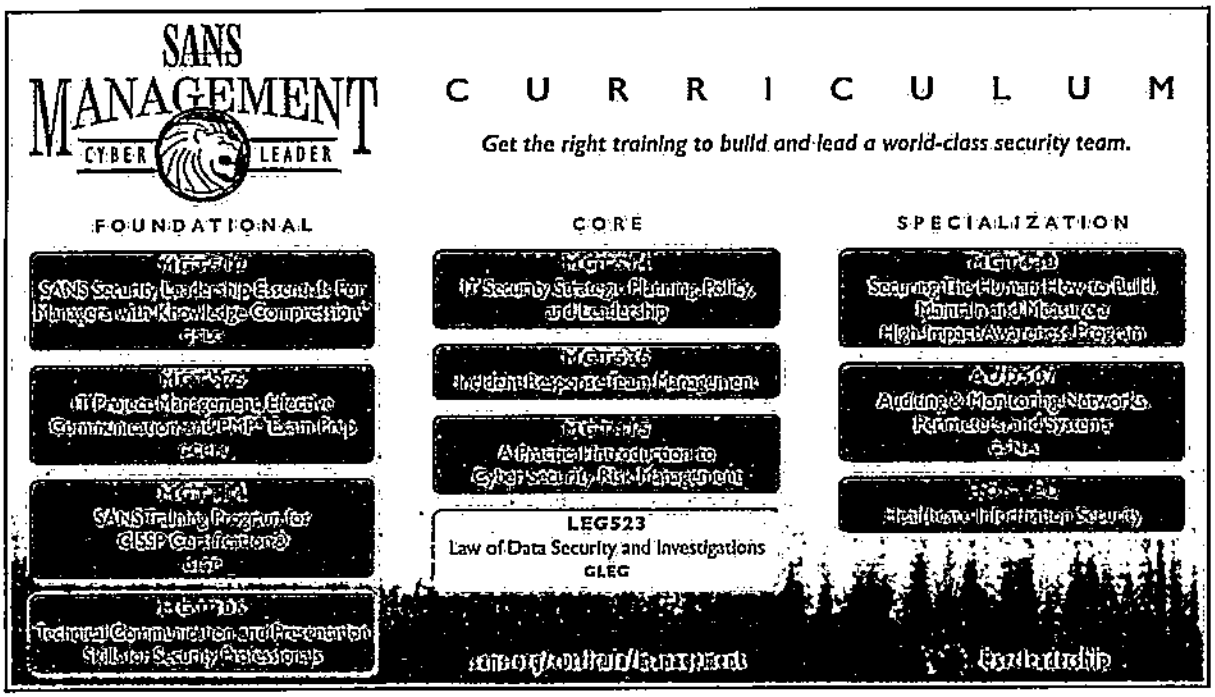
SANS

A Practical Introduction to Cyber Security Risk Management

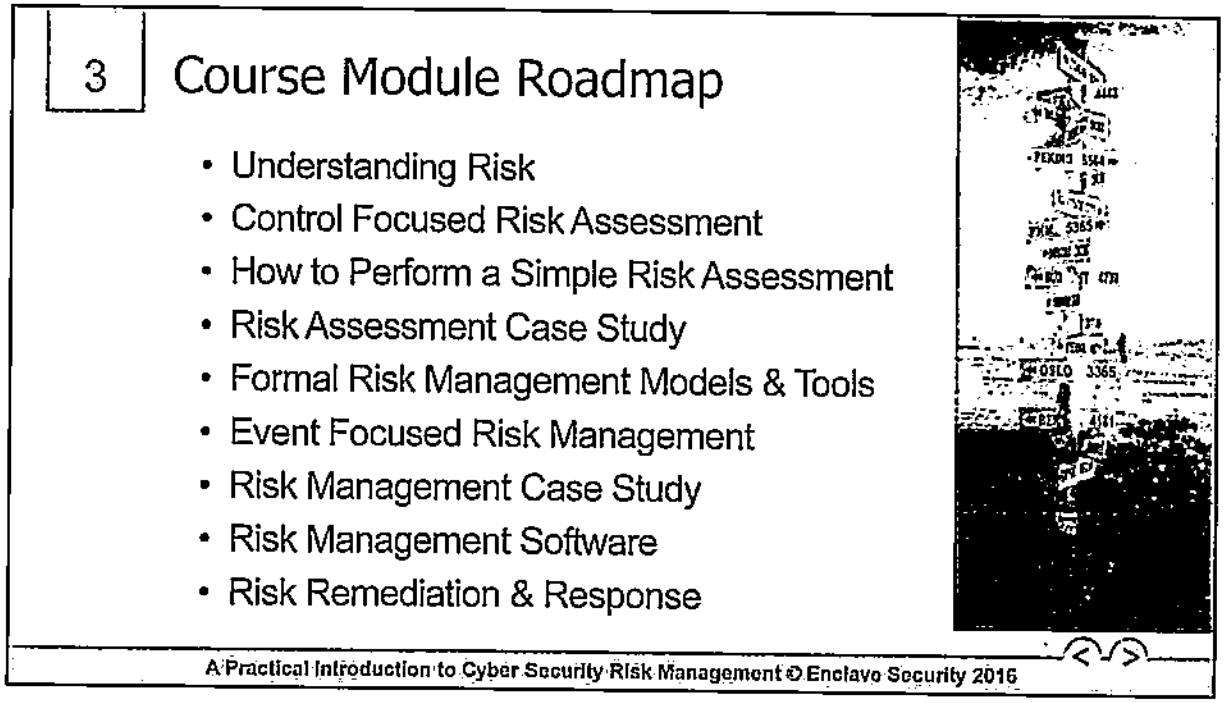
The SANS Institute

Written by James Tarala (james.Tarala@enclavesecurity.com)
& Kelli Tarala (kelli.Tarala@enclavesecurity.com)

This page intentionally left blank.



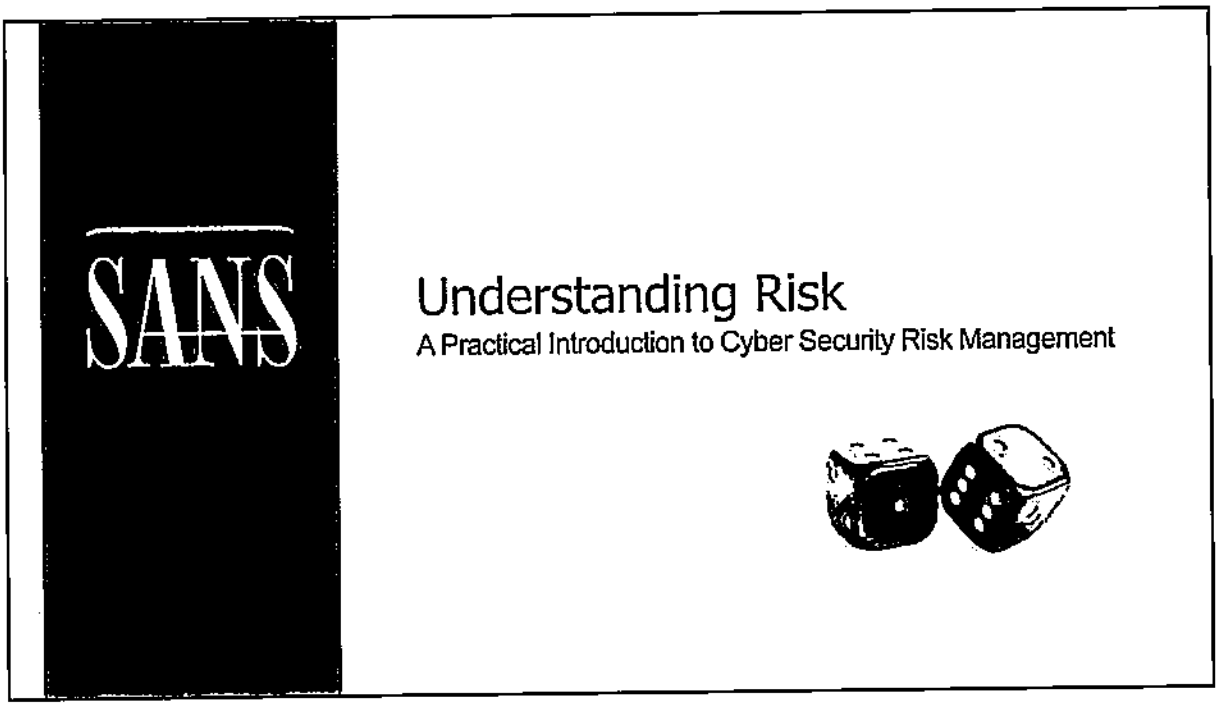
This course, SANS MGT415: A Practical Introduction to Cyber Security Risk Management, is a part of the SANS Institute's management and leadership curriculum as a part of it's core curriculum. In this course students will learn the practical skills necessary to perform regular risk assessments for their organizations. The ability to perform a risk assessment is crucial for organizations hoping to defend their systems. There are simply too many threats, too many potential vulnerabilities that could exist, and simply not enough resources to create an impregnable security infrastructure. Therefore every organization, whether they do so in an organized manner or not, will make priority decision on how best to defend their valuable data assets. Risk assessment should be the foundational tool used to facilitate thoughtful and purposeful defense strategies.



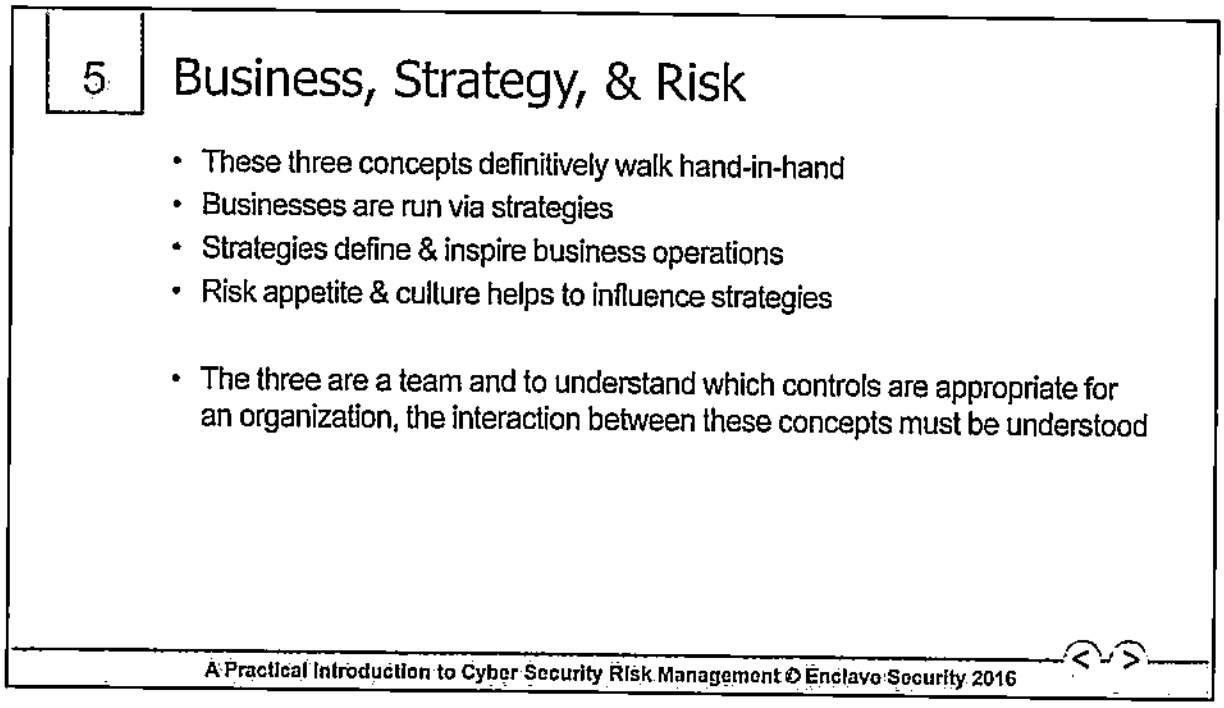
In this course we will explore the concept of risk and its practical impact on an organization. Ultimately the goal of this course is to prepare students to effectively utilize risk assessment as a tool for enterprise defense. Too many times organizations think of risk assessment and risk management as academic tools with little to no practical application. These concepts are often viewed as a formal task to pursue when an organization has free time rather than as a core business activity that drives other enterprise security efforts. In today's course students will have the opportunity to learn about the proper place of risk assessment and risk management in an enterprise. They will also be given practical skills for how to perform a risk assessment on a step by step basis, from data collection to the point of presenting their findings to business leaders. Students with a desire to perform more in depth analysis will also be given tools and formal models to consider to empower them to create a long term / formal risk management program.

Specifically today we will cover the following subjects:

- Understanding Risk
- Control Focused Risk Assessment
- How to Perform a Simple Risk Assessment
- Risk Assessment Case Study
- Formal Risk Management Models & Tools
- Event Focused Risk Management
- Risk Management Case Study
- Risk Management Software
- Risk Remediation & Response



This page intentionally left blank.



The first thing to understand is that business, strategy, and risk do work hand-in-hand. In fact if we try to see how these aspects play together, what we see is that businesses are run with strategies. Strategies then define and inspire how a business operates and what activities that business engages in. In addition, risk (and risk appetites) and culture of the business helps to influence which strategies will be adopted, and therefore by proxy, which operations will be performed.

The bottom line is that these concepts are a team, they work together, and ultimately will form the foundation of which controls an organization chooses to implement.

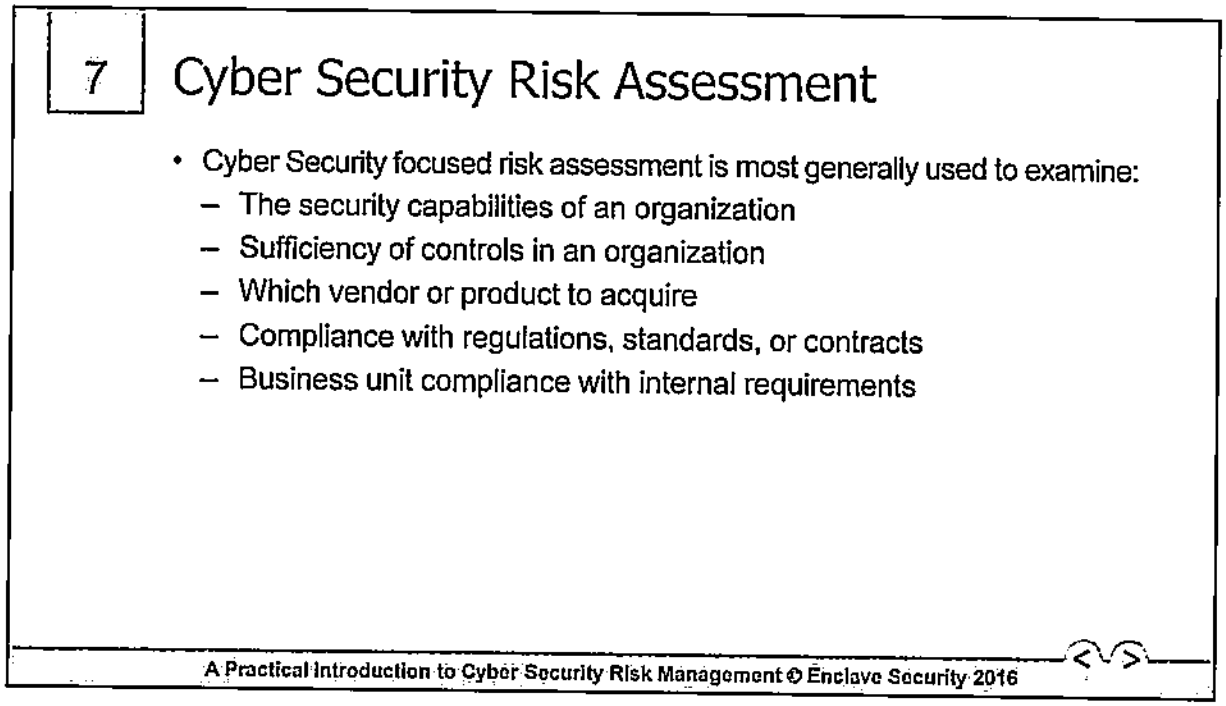
Why Manage Risk?

- Organizations have limited financial resources
- Organizations have limited personnel resources
- Therefore organizations must prioritize their security defenses

- Risk management allows organizations to:
  - Prioritize / focus their limited financial & personnel resources
  - Prioritize / focus defensive controls with the best return
  - Determine which controls are not feasible in the short / long term
  - Measure themselves for ongoing management & compliance

The reality of the situation for most organizations is that they have limited resources, both financially and in personnel. As a result while many times organizations know what the right thing is to do in order to defend the organization, many times resource constraints limit their ability to follow through. As a result they must prioritize their security defenses. The goal of most organizations is not simply to defend their data assets, they have other reasons for existing. This defense is necessary in pursuit of the larger goal.

Risk management therefore allows organization to prioritize and focus the resources they have available. In addition this leads the organization to be able to better prioritize the defensive controls they implement which will bring them the best possible return. Unfortunately the flip side of this discussion is that organizations may also need to prioritize which defenses they will not be able to implement in the short or long term. Risk management can help in this effort as organizations try to make these hard decisions between what is good and what is best. As organizations mature this process can be used for strategic advantage as they measure themselves for ongoing betterment and compliance with the requirements they have agreed to follow.

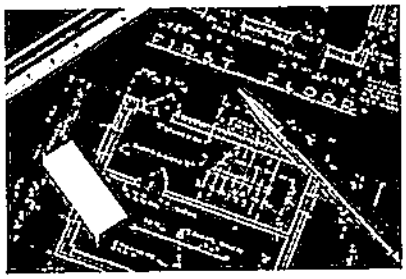


Practically cyber security risk assessment is used in a more narrow sense than enterprise risk management. Practically it focuses the organization on those things which can practically and best defend the organization from violations of the organization's data confidentiality, integrity, or availability. Specifically this type of risk assessment is most commonly used to examine:

- The security capabilities of an organization
- Sufficiency of controls in an organization
- Which vendor or product to acquire
- Compliance with regulations, standards, or contracts
- Business unit compliance with internal requirements

Throughout this course we will seek to go into more depth on these issues and provide practical insights on how organizations can be successful in these activities.

A General Framework



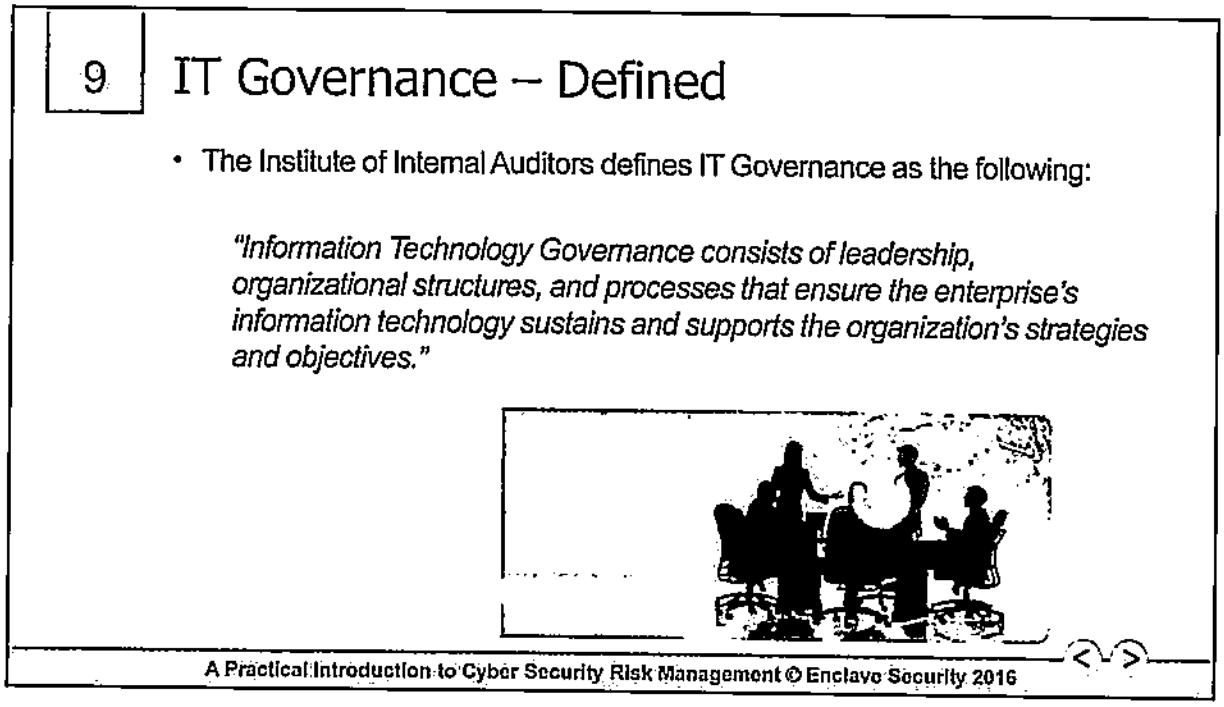
- Business goals lead to…
- Strategy, which leads to…
- Policies, which are defined by…
- Procedures, which are clarified by…
- Standards & Guidelines, which necessitates…
- Risk Management, which causes the evaluation of business goals
- And so the process repeats

A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

If we try to say this another way, we might say:

Business goals lead to…
Strategy, which leads to…
Policies, which are defined by…
Procedures, which are clarified by…
Standards and Guidelines, which necessitates…
Risk Management, which causes the evaluation of business goals
And so the process repeats

This process is a cycle, which starts with business goals and ultimately ends with the implementation of controls in the enterprise. These controls are the foundation of information assurance and define how we implement such a program.



To begin with today, let's start with a definition of what really is governance. Again, governance is one of those terms, similar to Governance Risk Control (GRC), which is defined in different ways by different organizations. Therefore, for the sake of this discussion, we think the best approach is to go to a well-respected industry source and use their definition. After our research we prefer the definition provided by the Institute of Internal Auditors (IIA) definition as documented in GTAG® 15: Information Security Governance. This document is IIA's Global Technology Audit Guide and is one practice guide in their International Professional Practices Framework (IPPF).

In this example, the IIA defines governance as:

"Information Technology Governance consists of leadership, organizational structures, and processes that ensure the enterprise's information technology sustains and supports the organization's strategies and objectives." [1]

So again we see the combination of process and business goals and the linking of appropriate controls that will return to support the overall business objectives.

[1] Glossary - The Institute of Internal Auditors. (n.d.). The Institute of Internal Auditors (IIA) - Welcome - The Institute of Internal Auditors. Retrieved February 1, 2011, from http://www.theiia.org/guidance/standards-and-guidance/ippf/standards/glossary/

Elements of IT Governance (from ISACA)

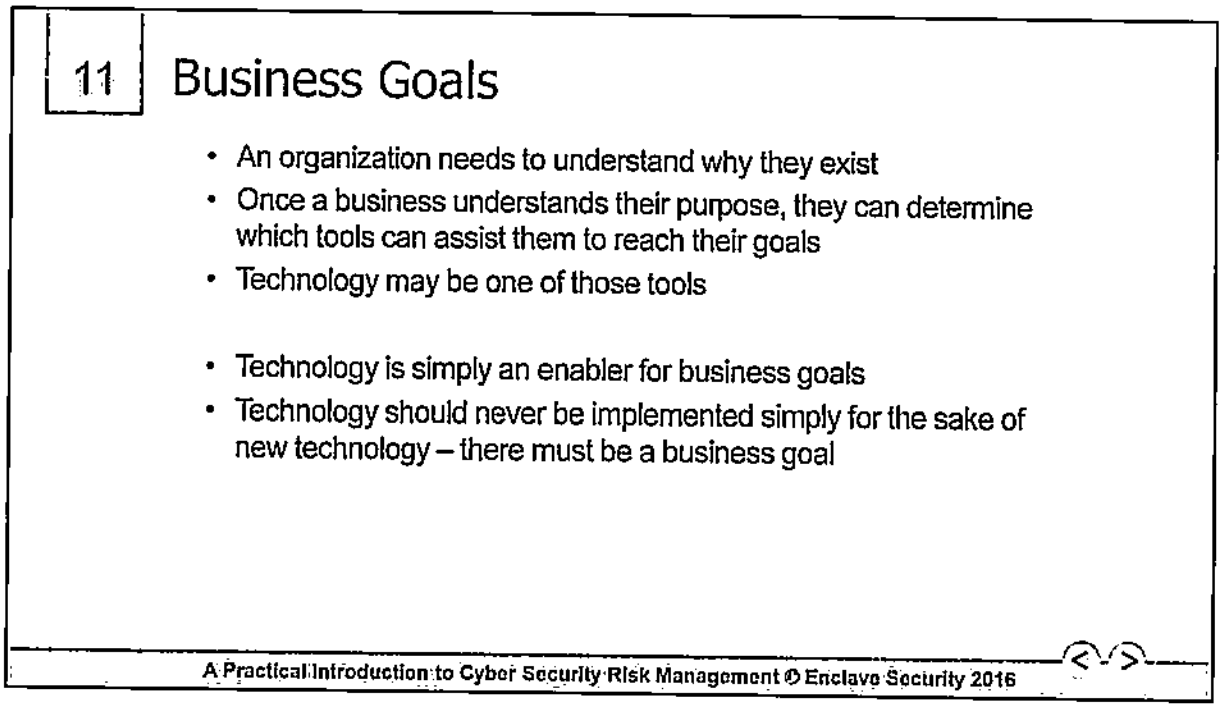
- ISACA (ITGI) defines the elements of IT governance as:
  - Aligning IT strategy with the business strategy
  - Cascading strategy and goals down into the enterprise
  - Providing organizational structures that facilitate the implementation of strategy and goals
  - Insisting that an IT control framework be adopted and implemented
  - Measuring IT's performance

Another group that seeks to provide us feedback on the characteristics of governance is the IT Governance Institute (or ITGI). The ITGI is basically a sub-group, governed overall by ISACA. As with the OCEG[1], the ITGI prefers to give us the characteristics of governance rather that trying to give us a simple definition as we saw from the IIA.

Specifically ISACA / ITGI defines the characteristics of IT governance as the following: [2]

- Aligning IT strategy with the business strategy
- Cascading strategy and goals down into the enterprise
- Providing organizational structures that facilitate the implementation of strategy and goals
- Insisting that an IT control framework be adopted and implemented
- Measuring IT's performance

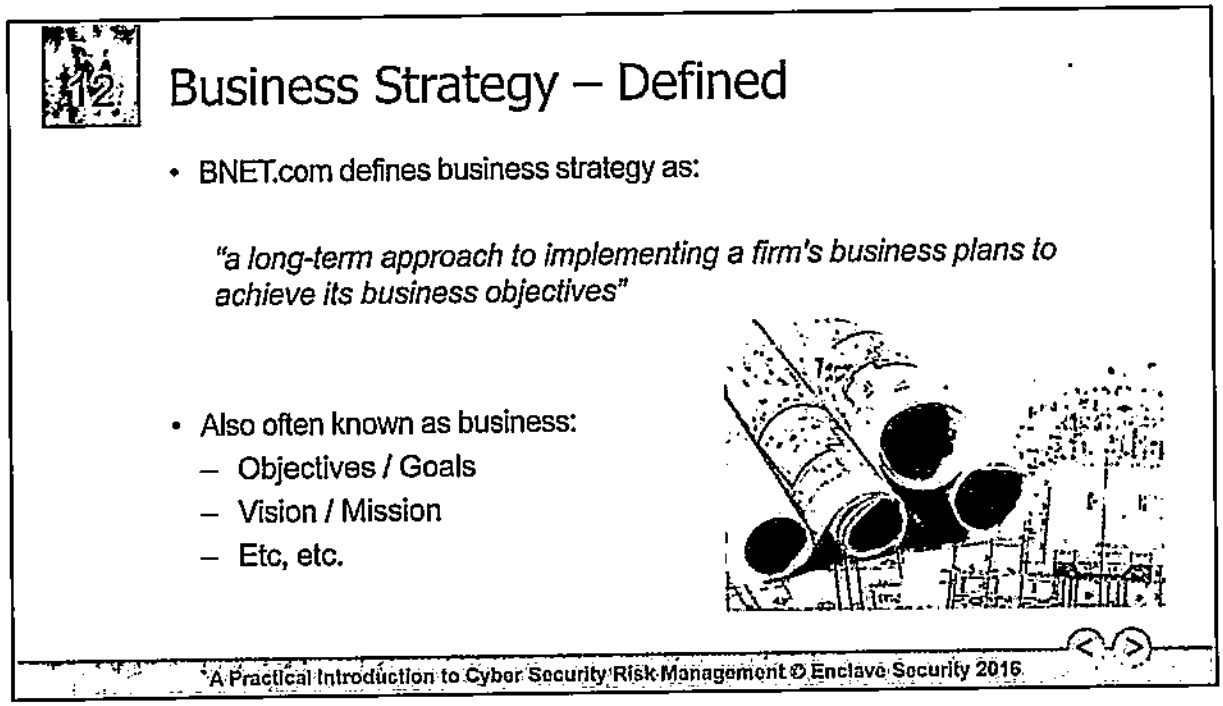
[1] http://www.oceg.org/about/
[2] About IT Governance Framework. (n.d.). ITGI. Retrieved February 1, 2011, from http://www.itgi.org/template_ITGIa166.html?Section=About_IT_Governance1&Template=/ContentManagement/HTMLDisplay.cfm&ContentID=19657



The place to start in this process is with business goals. Too many times, we have failures at various levels within an organization simply because we do not completely understand why the business exists. Even worse, many times organizations do not clearly have an internal agreement on this issue. Maybe certain parts of the organization understand why they are there, but overall there may be confusion. A business has to know why they exist and what their goals are. These business goals need to be clearly communicated to workforce members if the organization is to be successful.

Once an organization has made that decision as to why they exist, then they can decide what tools they need in order to achieve those goals. Without an understanding of purpose though, there is no reason to simply implement tools. Some of the tools that will be likely considered during this process include technology tools, whatever form they take.

Remember, technology is simply an enabler for business goals. Technology involves tools to achieve a particular goal. If you do not understand your goals, how can an organization understand what tools it needs to better perform its job? Technology, therefore, has to have a reason to be implemented. If there is not a clear link between a business goal and a technology there is definitely something wrong.



So the first thing we should consider is a good definition to the term "business strategy." What does this term mean?

Like many business terms, there is not always agreement on what a term like this actually refers to. There are likely going to be quite a few experts with different views and different reasons for us to adopt their way of thinking. But to keep things simple, for the sake of our discussion, let's consider a definition given by BNET.com.

"a long-term approach to implementing a firm's business plans to achieve its business objectives" [1]

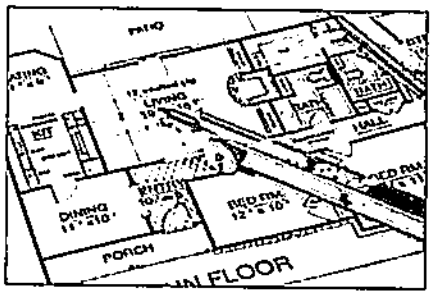
In the business world this idea has multiple names or synonyms we could use. Again, not to start a holy war over the issue here, but often times you may also see this concept referred to as business objectives, goals, vision, mission, and likely many other terms.

Let's look at a famous technology company as an example of business strategy. Apple has long controlled their operating system, the interactions between the operating system and software as well as the hardware that those components run on. Apple's strategy was to build a consistent and stable experience for its users no matter if they were using a cellular phone, a tablet, or a desktop computer. The strategy was to create a walled garden of consumer experience and this strategy supported its business objectives of selling more hardware units, more applications for purchase, as well as other electronic consumables like music, electronic books, movies, and games.

[1]Business Strategy - Featured Articles, News and Other Resources | BNET. (n.d.). BNET - The CBS Interactive Business Network. Retrieved February 1, 2011, from http://www.bnet.com/topics/Business+Strategy. – Link no longer live.

13 Defining / Documenting Strategy

- Somehow businesses have to document what their strategy is
- These are documented for clarity, consistency, and to help educate workforce members
- Different business gurus recommend different methods of documentation, some options include:
  - Mission statements
  - Vision statements
  - 3 / 5 / 10 year plans
  - Strategic roadmaps
  - Etc.

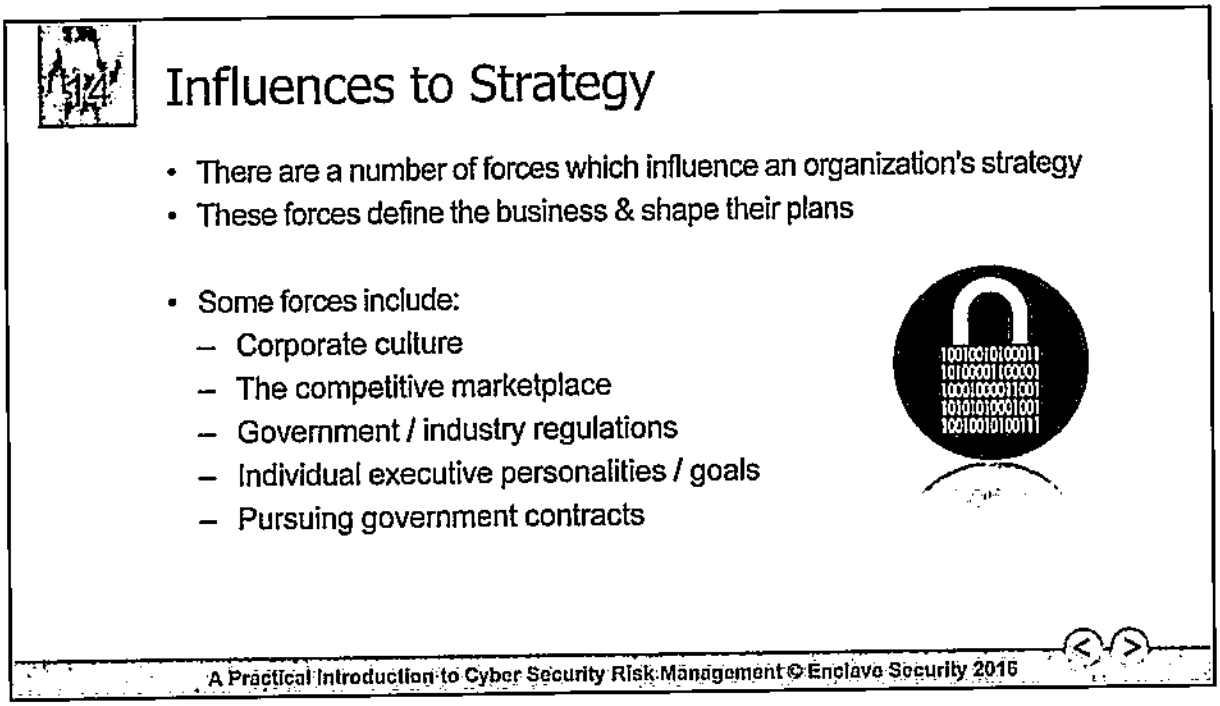


A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

If we understand what strategy is, then the next thing to look for, is whether or not the business actually has a documented business strategy. If we say that this strategy is something that must be defined, that the organization as a whole needs to be in agreement with it, and it is something that all workforce members should be aware of, then one would hope that it is documented at least somewhere in the organization.

Again, business gurus will likely give you different names to the documents where this information should be recorded. We don't want to start a fight with them (have you ever seen a business guru?); however, we think you should be aware of some of the terms that are used to define this sort of strategy. The types of documentation you should be looking for are:

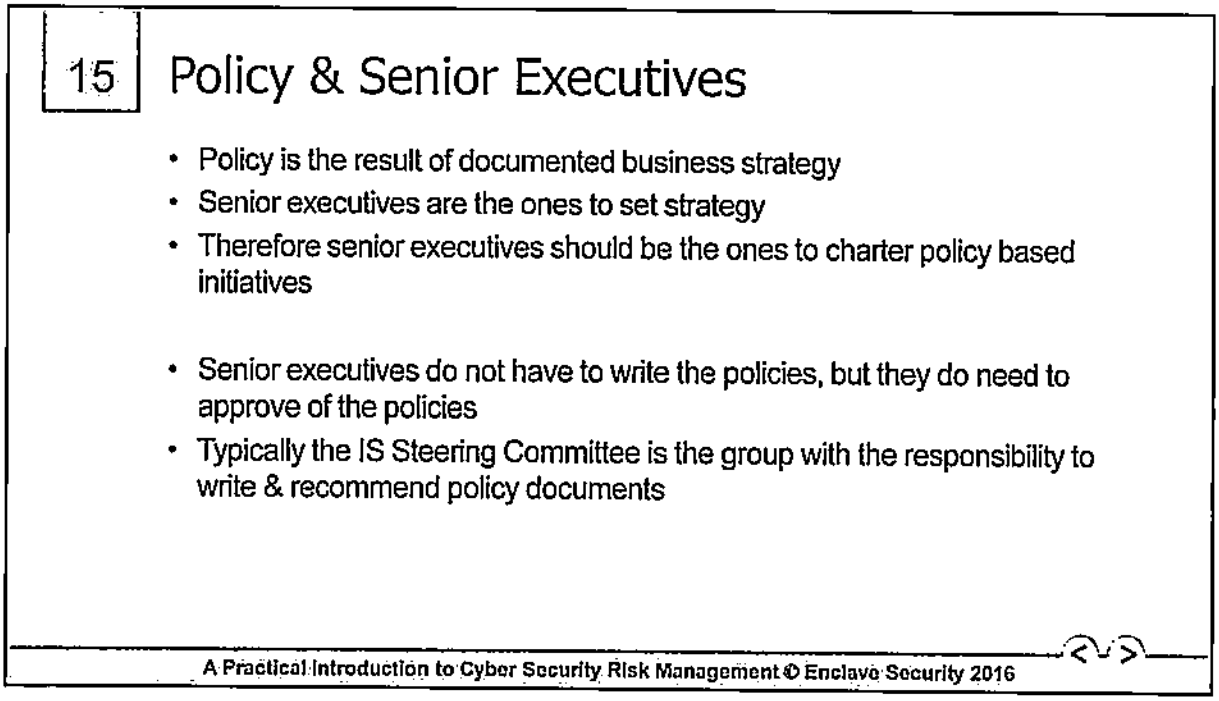
- Mission statements
- Vision statements
- 3 / 5 / 10 year plans
- Strategic roadmaps



Every organization's culture and risk appetite's are going to define what the organization's strategy actually is. This will also determine which controls are eventually chosen and put into policy statements. The important thing at this point is to understand that every organization will be different. You are not trying to push your beliefs or your opinions at senior executives. Instead, you are trying to evaluate whether appropriate documentation exists to define the organization's strategy.

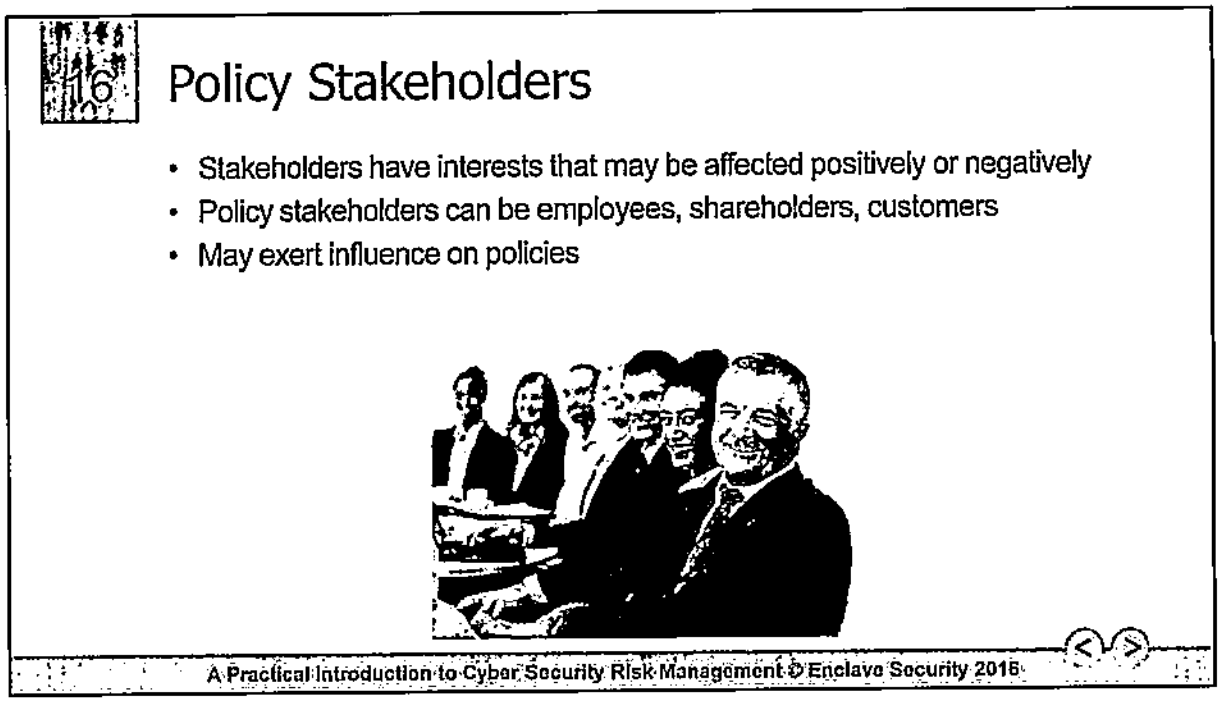
Strategy will be influenced by multiple factors. Likely, most of the organizations you evaluate will differ, and rarely will culture be the same. Some of the factors that likely will go into this process are:

- Corporate culture
- The competitive marketplace
- Government / industry regulations
- Individual executive personalities / goals



Just as business strategy is the direct result of senior executives, policies should be an extension of senior executives. Remember, business strategy is set by senior executives. It is one of their primary roles within the business. Also, remember that policies are a direct result of documented business strategies. Therefore, even if senior executives are not the ones to sit and actually document policies, it should still be their drive that ultimately dictates those policies. In other words (using project management terms from earlier), senior executives should be the ones to charter a policy development and maintenance program in light of their documented strategies.

Do not expect that an executive will be the one to actually sit at a keyboard in order to document these policies, because that is not likely something that is going to happen. However, one might expect that this is a perfect task to be assigned (chartered) to the IS Steering Committee. In most organizations, this is the group that takes responsibility for actually writing policies, deciding on the wording, coming to a consensus (or something close to it), and then recommending those policies to senior executives. It is definitely a teamwork exercise, but at the end of the day, executives need to be the ones that sign off on these policies and propagate them to the entire workforce.



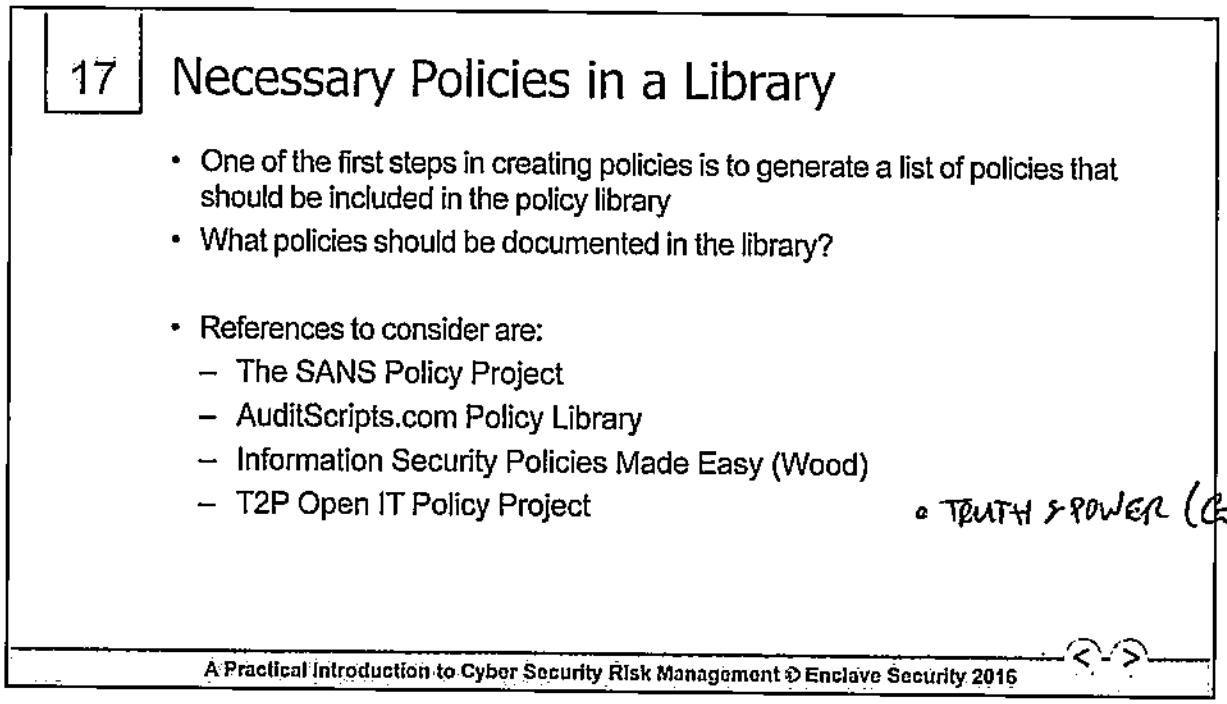
Stakeholders are more than the people that have investments in your company. Of course these people have something to win or lose, but so do the many teams of people for a company. Policy stakeholders are people that will be positively or negatively impacted by the polices, or team members that actively involved in policy creation as well as people that influence on policy creation.

Stakeholders play an important role in policy creation. Remember, policy is the result of documented business strategy, and stakeholders make crucial decisions to support business strategy.

For example, let's look at our Apple computers example again. Let's say that Apple has a policy that addresses confidentiality of intellectual property, especially new products and services that are in the development stage. That confidentiality is very important because if a competitor gains that intellectual property and duplicates it, that will directly affect the sales of that Apple's product. If we were to list the potential stakeholders for the confidentiality policy, that list could include the employees, the shareholders, the product team, the market team, and even Apple's manufacturers and distributors.

When the IS Steering Committee is drafting policies, it is important for these team members to consider who the main stakeholders in the new policy will be. These stakeholders can be advocates for the policy throughout the organization. Stakeholders may share all or some of these interests or "stakes":

- Knowledge of a particular topic
- Ownership of property or contract
- Rights granted such as legal rights
- Influence on the policy
- Impact by the policy



When it comes to policy documents, one of the first things to address is whether or not the policies that are included in the policy library are comprehensive enough to cover all of the control areas that are appropriate and necessary. Undocumented policies are not policies and should be considered non-existent. If a topic is not covered anywhere in the policy library, then it should be included.

So the question becomes, what topics should be included in the policy library?

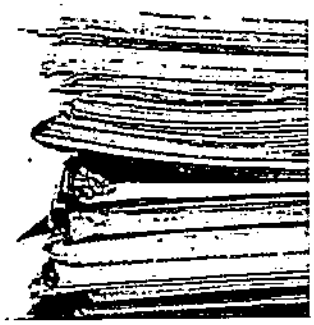
In this case, the best answer to the question is to evaluate reference sources that are available online and use those references to determine if anything is missing. There are a number of free and commercial resources that are available and which could be used to answer these questions. Some of the more popular ones that you might consider are:

- The SANS Policy Project
- AuditScripts.com
- Information Security Policies Made Easy (Wood)
- T2P (Truth to Power) Open IT Policy Project [1]

[1] https://www.t2pa.com/project-open-it-policy-project/oitpp-directory/

Sample Information Security Policies

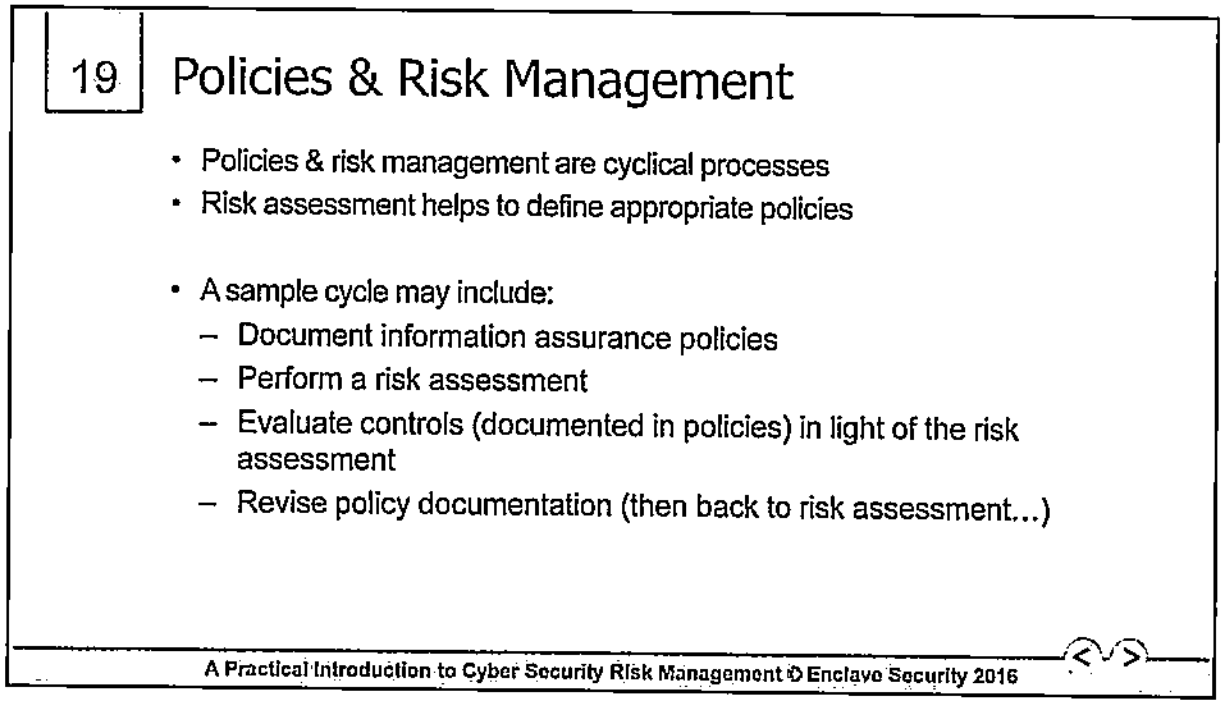
- Some sample security policies to consider are:
  - Acceptable system use policy
  - Acceptable encryption policy
  - Remote network access policy
  - Data access authorization policy
  - User authentication policy
  - Network monitoring policy
  - Incident handling policy
  - Business continuity / disaster recovery policy
  - Physical security policy



Many times we hear people ask, "Which policies should actually be in a policy library then? How much policies need to be documented and which policies should exist?" Ultimately, the answer to this question is something that each company will have to decide for themselves. There is no easy answer to this question. However, there are a number of good resources mentioned already that certainly will be helpful when a company does decide that they want to write this documentation.

There are a number of policies that you will certainly run across on a regular basis. Some examples of policies you are likely to see numerous times throughout their careers are:

- Acceptable system use policy
- Acceptable encryption policy
- Remote network access policy
- Data access authorization policy
- User authentication policy
- Network monitoring policy
- Incident handling policy
- Business continuity / disaster recovery policy
- Physical security policy



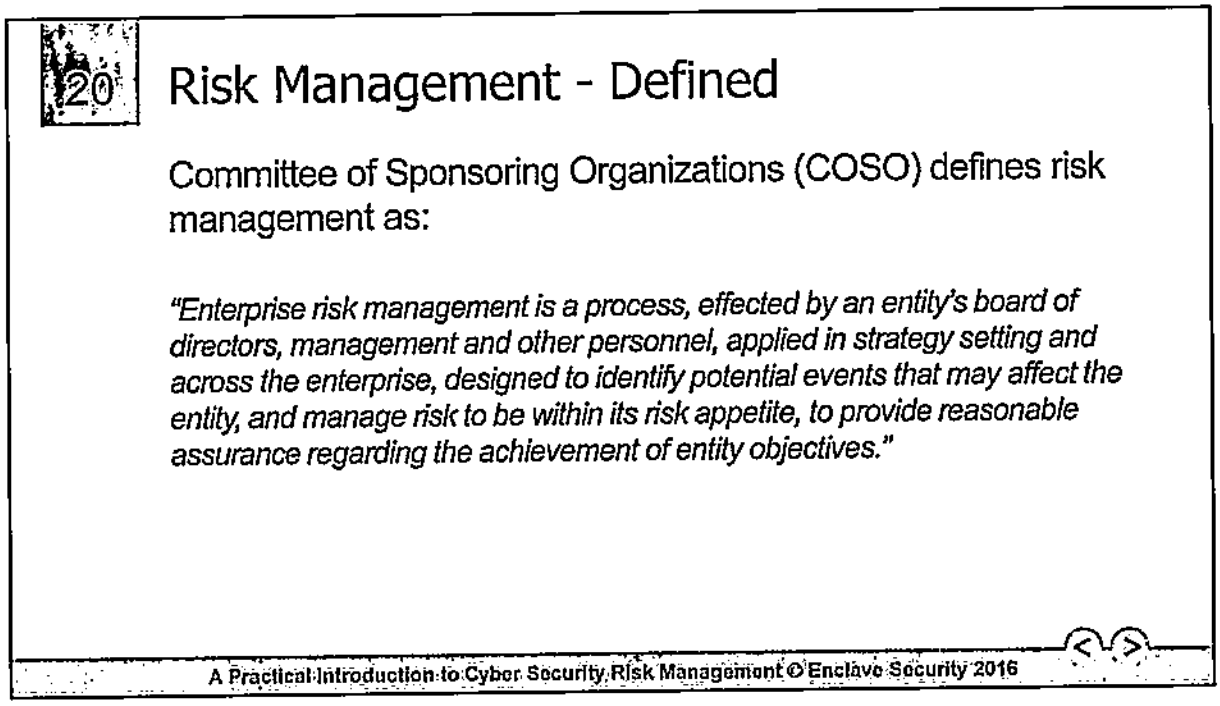
Policy documents and supporting documentation are not static documents. They are living documents, which change with the culture and goals of the organizations. Remember, these documents are based on the goals of the business, which for nimble businesses may change on a regular basis.

Therefore, one would have to imagine that the process of policy definition and risk management are cyclical, continuous processes. Risk assessment helps to define which policies are appropriate, and policies form the foundation of performing a risk assessment.

A sample cycle working through this process therefore might look something like this:

1. Document information assurance policies
2. Perform a risk assessment
3. Evaluate controls (documented in policies) in light of the risk assessment
4. Revise policy documentation (then back to risk assessment…)

But we will address this topic in much more depth soon…



Now that we have spent some time analyzing frameworks for governance and we understand both the G (Governance) and the C (Compliance) of GRC, the last element we need to spend time with is the R (Risk). For the remainder of the day, let us turn our attention to risk management and understand how this fits into the overall picture of GRC.

To begin, let us take a look at a working definition for risk management. We will take our definition this time from Committee of Sponsoring Organizations (COSO), who defines risk management as:

"Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." [1]

Like the definition of governance we discussed earlier, risk management also often times is better defined when considering the characteristics of risk management, rather than simply trying to give it a static, brief answer.

According to COSO, a more expanded definition of risk management is that Enterprise Risk Management (ERM) is: [1]

- A process, ongoing and flowing through an entity
- Effected by people at every level of an organization
- Applied in strategy setting

- Applied across the enterprise, at every level and unit, and includes taking an entity level portfolio view of risk
- Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite
- Able to provide reasonable assurance to an entity's management and board of directors
- Geared to achievement of objectives in one or more separate but overlapping categories

[1] Enterprise Risk Management Framework. (n.d.). The Committee of Sponsoring Organizations of the Treadway Commission . Retrieved February 1, 2011, from http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf.

NIST Risk Management Definition

NIST (800-30) defines risk management as:

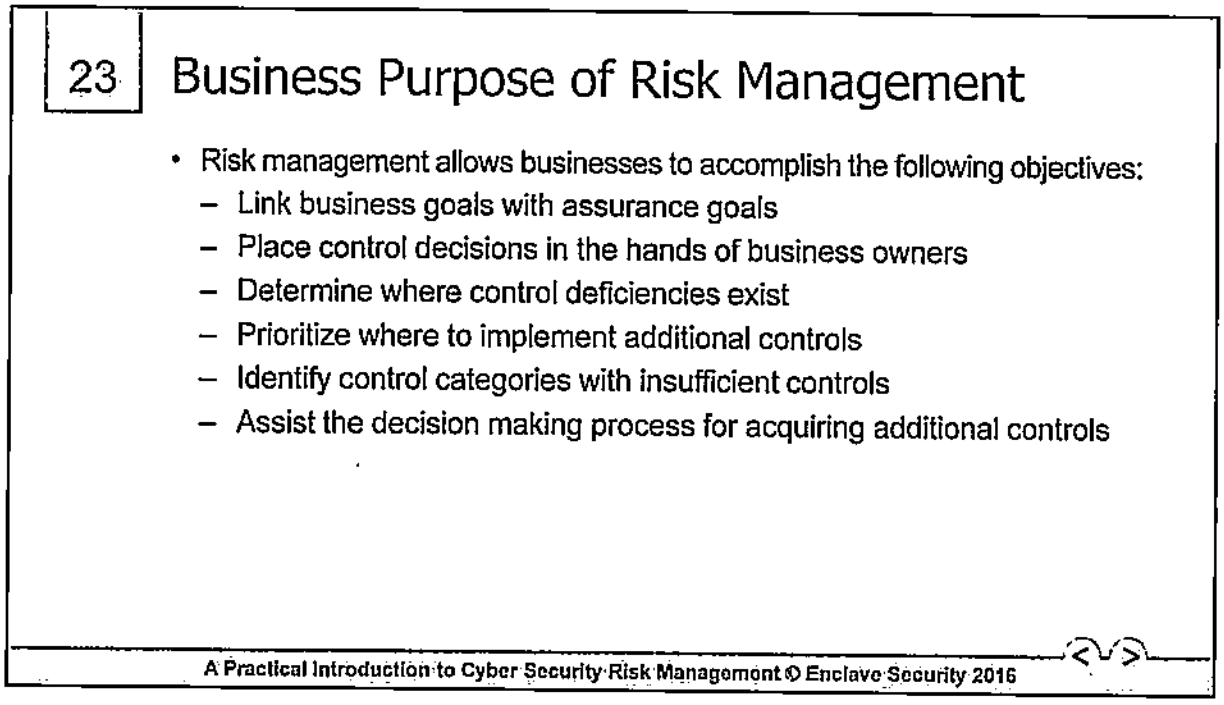
"The total process of identifying, controlling, and mitigating information system–related risks. It includes risk assessment; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws."

At the same time, let us get one more perspective. Other than COSO, there are a number of organizations that have defined risk management. The more of these definitions we examine, the more thorough a definition we will be able to develop. Our hope is that by spending time examining this definition we will be able to develop a comprehensive view on the subject and be able to analyze it from various angles.

NIST gives the following definition for risk management in their NIST 800-30 guide:

"The total process of identifying, controlling, and mitigating information system–related risks. It includes risk assessment; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws." [1]

[1] Risk Management Guide for Information Technology Systems. (n.d.). Computer Security Division Computer Resource Center. Retrieved February 1, 2011, from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf



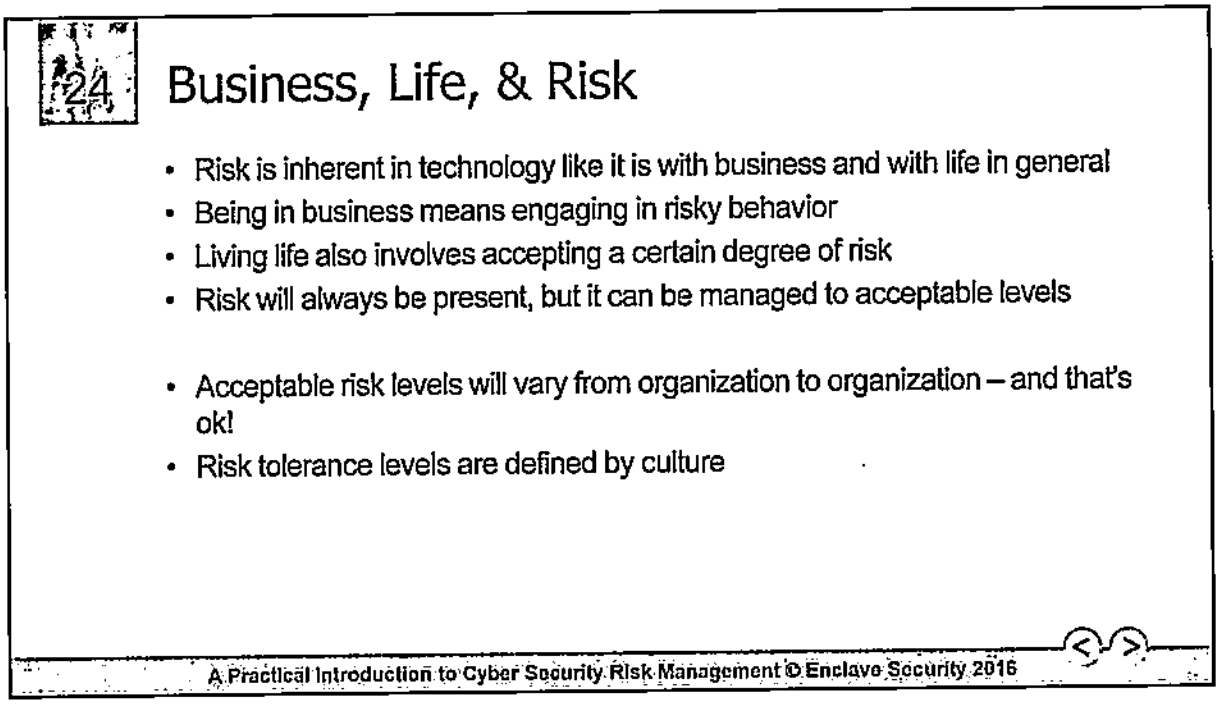
Other than the fact that risk management represents the R of GRC, there must be other, simpler reasons why risk management should be a part of an enterprise's overall business strategy.

Executives need to understand why they are engaging in activities such as policy writing and data classification. Without a proper understanding of the business value of these controls, they will simply become a checklist item to be marked off. When this happens the value of the control is often reduced. Enterprise Risk Management (ERM) helps an organization understand why certain controls are in place and what risks the controls are mitigating.

Specifically, a number of goals that exist for ERM are the following:

- Link business goals with assurance goals
- Place control decisions in the hands of business owners
- Determine where control deficiencies exist
- Prioritize where to implement additional controls
- Identify control categories with insufficient controls
- Assist the decision making process for acquiring additional controls

These are examples of the types of justifications that an you may want to provide to senior executives for why this type of program makes sense for a business. In short, ERM aligns business goals with technology controls and increases awareness of those links, which is just better business.



Business leaders need to understand that risk is inherent in technology systems, just as it is with business and even life in general. If an organization is going to engage in any business activities, then that means that they will have to engage in risky behavior, such is the nature of business. In addition, simply living life will also demand that we accept certain levels of risk. Avoiding all risk in life simply is not possible!

Therefore, if we accept that risk will always be a present factor in organizations, then we must determine how to handle this risk appropriately. Complete risk avoidance is impossible; instead we need to determine ways to manage risks to acceptable levels within the culture of the business. Acceptable risk levels will definitely vary from organization to organization.

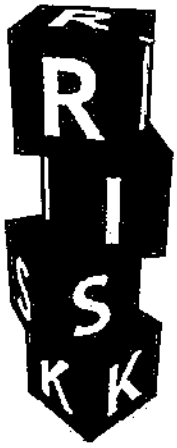
For example, new businesses and startups are often willing to accept a higher degree of risk than more established or traditional organizations. To be fair, more established organizations have more to lose typically than newer startups, and their risk tolerance levels will vary accordingly.

Different organizations will accept different levels of risk, and that is ok. You are not responsible for determining acceptable risk levels but rather ensuring that the risk levels set by the organization's strategy is actually the risk level being accepted in practice.

25

Example of Risk in Real Life

- In real life we live with risk every day
- For example, in real life it is risky:
  - To cross the street
  - To take an airplane to a conference
  - To eat lunch in an unknown restaurant
  - To exercise & engage in athletics
  - To not exercise & not engage in athletics
  - To sign up for a mortgage on a home



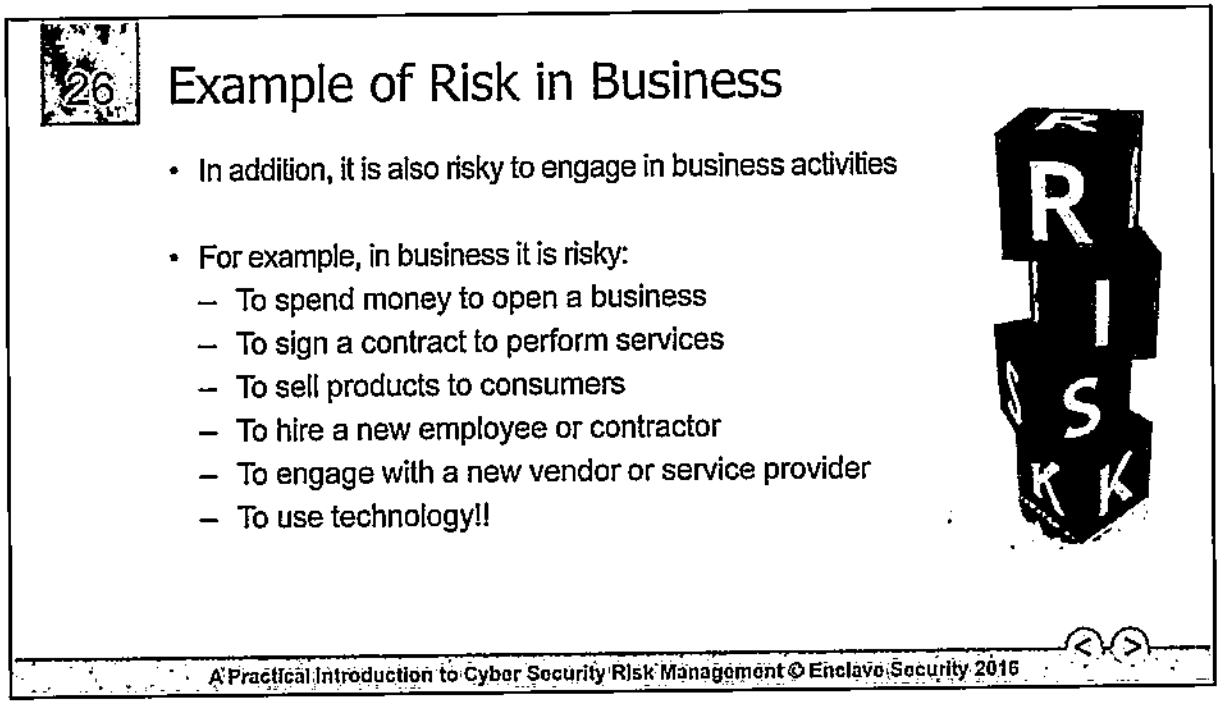
A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

Life itself (of course) is filled with risks. While day to day, we do not make decisions using risk management terms (ok – most of us don't), ultimately we go through every day making decisions about levels of risk based on an internal process. We do not walk in front of a car that is quickly accelerating for fear of getting hit by said car. But if the car was parked and the motor turned off, our internal assessment would tell us that it is safe to walk in front of the car. At a crosswalk we often have to make the same decision based on factors like the speed of the car, the color of a traffic light, and multiple other factors. All of this is risk assessment. We decide how to proceed based on our perspective on risk.

There are numerous examples like this of when we make risk management decisions on the fly in daily life. A few of these examples might be:

- To cross the street
- To take an airplane to a conference
- To eat lunch in an unknown restaurant
- To exercise and engage in athletics
- To **not** exercise and **not** engage in athletics
- To sign up for a mortgage on a home

In fact as parents we have often been told that parenting children is not about teaching kids to avoid risk, but rather to teach them what risks are worth taking in life and which are not.

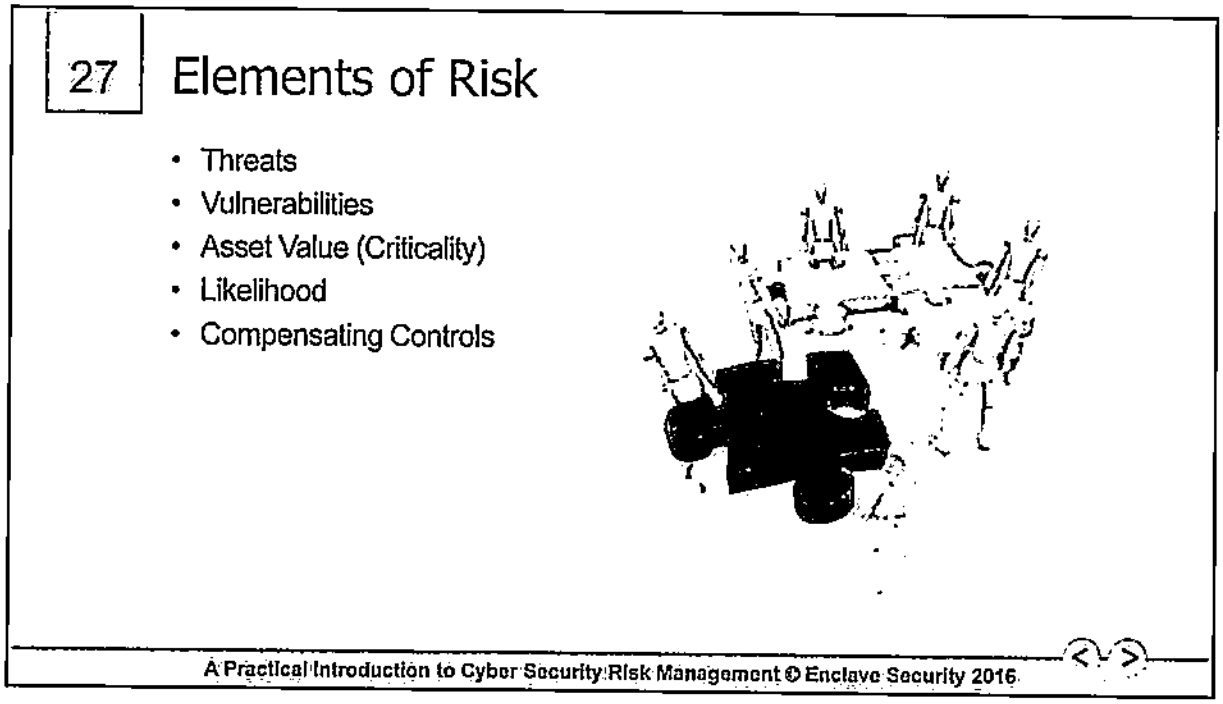


Just as in life, business is also involved in risk management as a part of its daily routine. In order to be in business, a business owner or entrepreneur decides that it is worth taking some risks in order to gain the potential reward down the road. Present pleasure or comfort can be postponed for the potential reward of future success. In fact it is almost a cliché to consider small business owners who take personal debt on things such as credit cards or mortgages against their personal homes in order to help a business to get started. Again, personal risk is worth the chance that the business may succeed. And, unfortunately, a large percentage of these businesses fail after only a short period of time.

In business some other examples of risky behaviors would include the following:

- To spend money to open a business
- To sign a contract to perform services
- To sell products to consumers
- To hire a new employee or contractor
- To engage with a new vendor or service provider
- To use technology!!

But business is in essence risk management. It is a decision-making process attempting to determine which risks are worth taking and which are not. This of course creates a culture of acceptable risk and helps the business to decide when to take risks and when not to take them. This will lead us later to a better understanding of risk treatment as it refers to assurance controls.

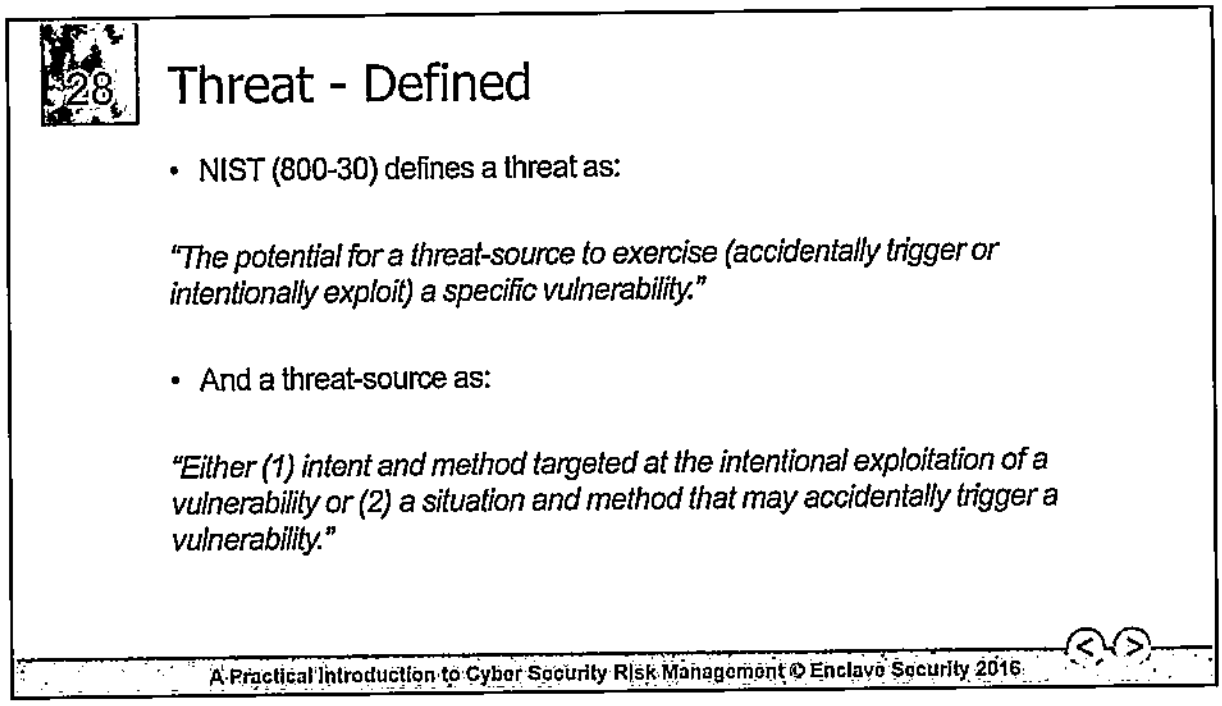


In this next section, we need to address more definitions and make sure we understand the elements of risk and how these elements work together to give an organization a complete picture of the risks facing the organization. Once we have successfully defined the elements of risk, the next step will be for us to determine how these elements can work together to create a simple risk assessment.

The elements of risk most commonly included in risk assessment programs are the following, each of which we will define in turn:

- Threats
- Vulnerabilities
- Asset Value (Criticality)
- Likelihood
- Compensating Controls

More complicated and established risk models may decide to use different terms, definitions, or even elements. But for most risk assessment methodologies, these are the common elements most often referred to.



If we return to NIST 800-30 for our definitions, we find some very good definitions to consider when defining threats. To start, they define a threat as:

"The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability." [1]

To further define this concept, they define a threat-source as:

"Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability."

The first component to understanding risk is to consider threats. A threat is any potential danger to a system, or anything that could potentially harm a system. Threats can be either intentional or unintentional, but in either case they carry the ability in some form or another to threaten a given information asset. Threats should also not be confused with vulnerabilities. We will discuss these on the next slide.

There are many different types of threats to consider during a risk assessment, for example:

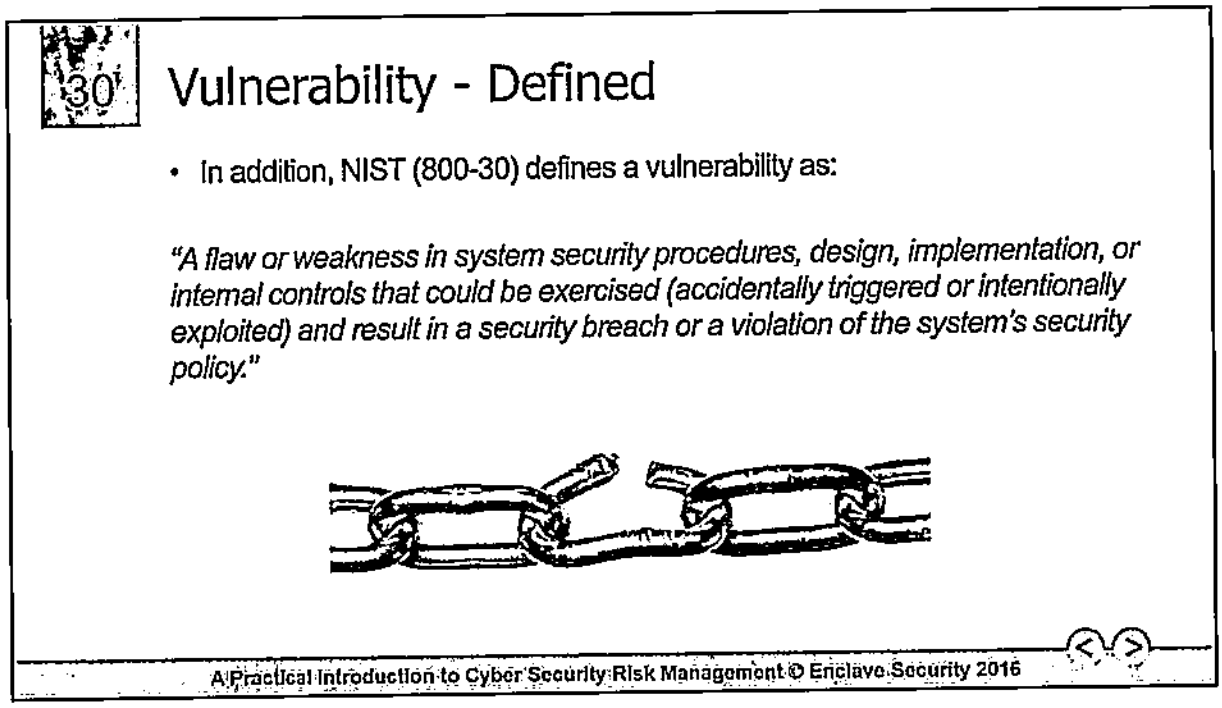
- Forces of nature
- Criminal activity
- Accidental threats

One specific model that is commonly used as a part of the threat assessment portion of a risk assessment is Bhaskar's Threat Matrix. This matrix can be used to help classify and define individual threats to a system and can serve as a solid aid for being creative with potential threats that face the system.

Bhaskar's model defines three separate categories for threats, which are:

- Active vs. Passive Threats
- Logical vs. Physical Threats
- Deliberate vs. Accidental Threats

1 Risk Management Guide for Information Technology Systems. (n.d.). Computer Security Division Computer Resource Center. Retrieved February 1, 2011, from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf



To continue our trend of using NIST definitions for our risk related terms, NIST 800-30 defines a vulnerability as:

"A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy." [1]

The second element of risk to consider is vulnerabilities. Vulnerabilities are potential system weaknesses, which could be exploited by threats to an information system. While threats focus on something that could harm a system (such as an electrical surge), a vulnerability focuses on the potential weakness that could be exploited by the threat (being plugged into an electrical outlet).

One thing to consider when performing a risk assessment is that in order to get an accurate picture of the risk to a system, you must do more than simply run a vulnerability assessment tool against a system. While that type of information could be helpful, it does not represent a comprehensive risk assessment. These tools should only be used to complement, not to replace, a solid risk management process.

Some samples of the different types of vulnerabilities an organization should consider are:

- Physical vulnerabilities
- Procedural vulnerabilities
- Personnel vulnerabilities

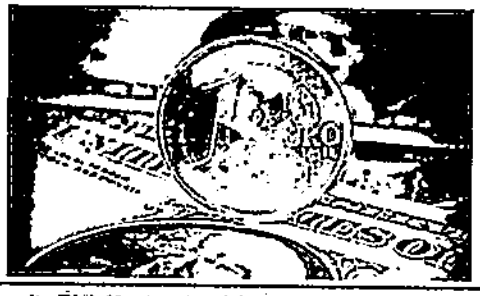
[1] Risk Management Guide for Information Technology Systems. (n.d.). Computer Security Division Computer Resource Center. Retrieved February 1, 2011, from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

31

Asset Value (Criticality) – Defined

- Enclave definition of asset value / criticality:

"The perceived or actual value of an information asset. This value can be reflected as either a financial metric (hard) or as a relative expression of worth (soft)."

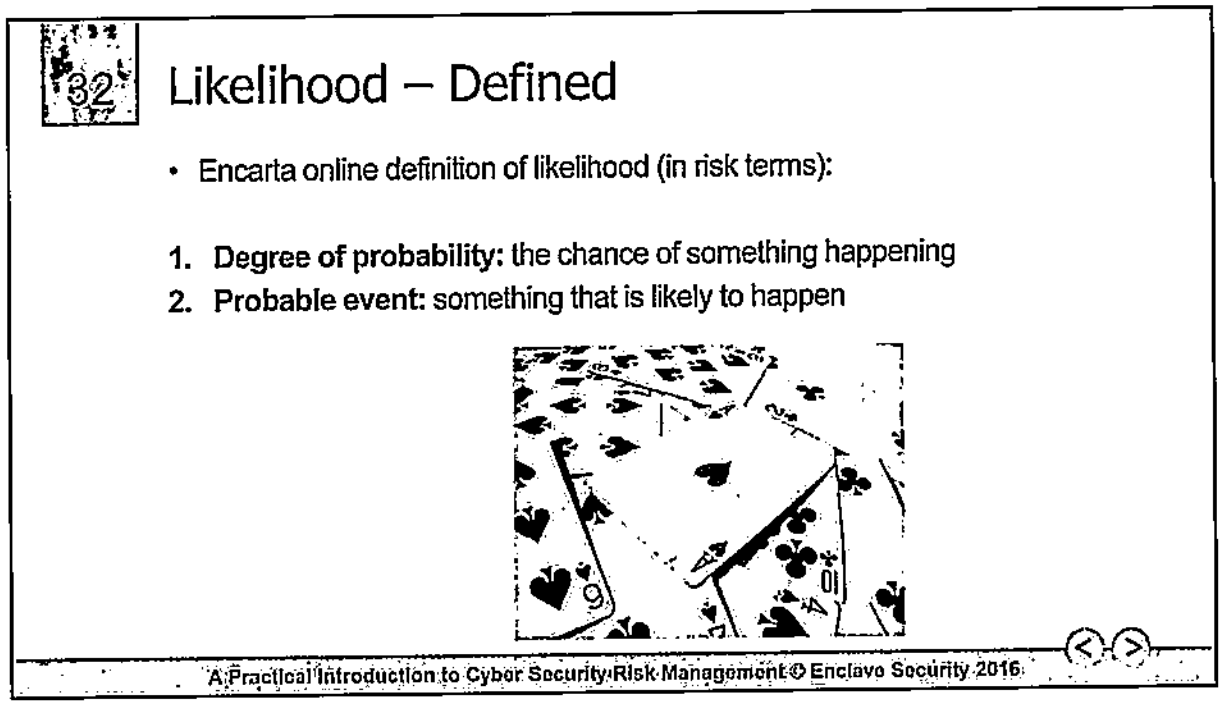


A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

Another term that is often associated with risk management is asset value, often referred to as "criticality." Criticality is often used as a replacement work for asset value in risk management terms because the word criticality invokes the idea of an asset having a certain critical value to the overall purpose of the business. An asset or system is critical to the functions of a business at various levels, depending on the asset. Therefore, during risk assessment we should give a score to the relative worth of a given asset in order to help us determine the value's relation to the controls that are later implemented.

Although there is no standard definition that we have been able to find for this term (at least not one that is agreed upon), we decided to give our own definition to this concept in order to give clarity to the nuances. Enclave's definition for asset value or criticality, therefore, is:

"The perceived or actual value of an information asset. This value can be reflected as either a financial metric (hard) or as a relative expression of worth (soft)."



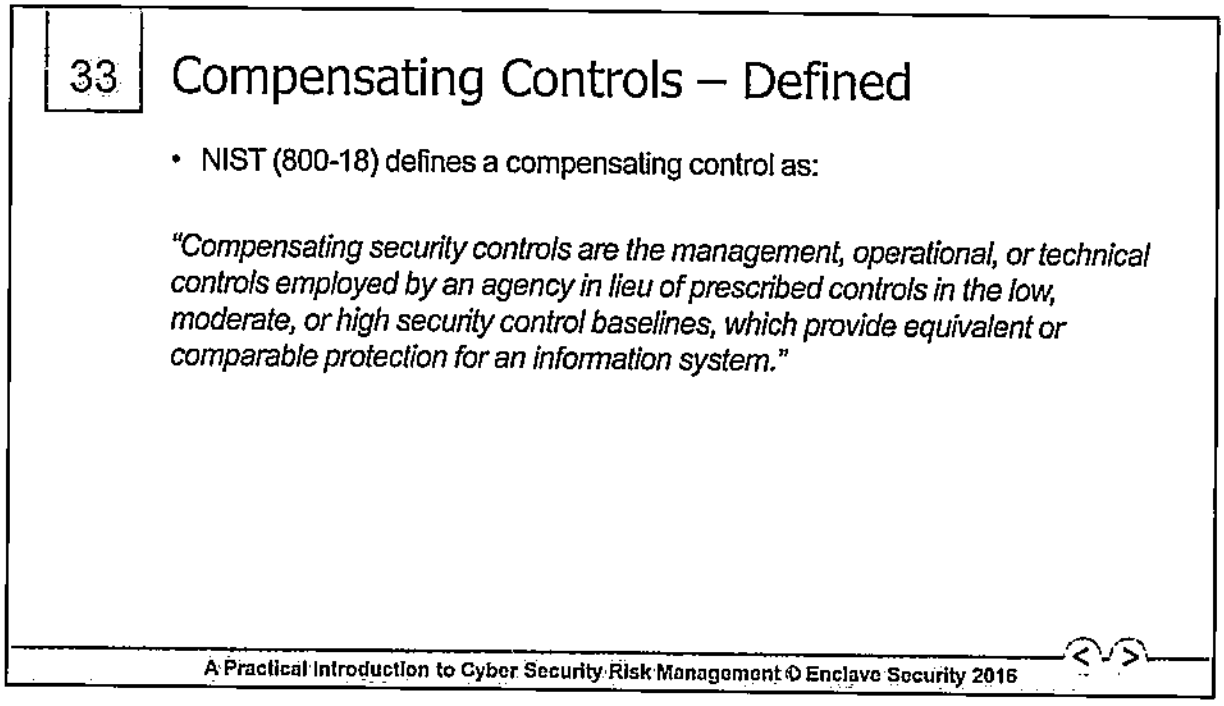
Another risk management term that we need to understand is the idea of likelihood. In other words, what is the probability of a particular event occurring? While we may not have specific quantifiable metrics that we can use to determine what this value is, like other elements of risks we can substitute qualitative values for this element in an attempt to determine the potential overall risk.

Encarta's definition of the term likelihood (when used in a risk-based context) is defined as two different meanings, which are:

1. **Degree of probability:** the chance of something happening or
2. **Probable event:** something that is likely to happen.

Since this term is more of a general phrase, rather than a risk management specific phrase, we simply used Encarta's online dictionary definition of the word. [1]

[1] define likelihood - Bing DICTIONARY. (n.d.). Bing. Retrieved February 1, 2011, http://www.bing.com/Dictionary/search?q=define+likelihood&FORM=DTPDIA&qpvt=definition+of+likelihood

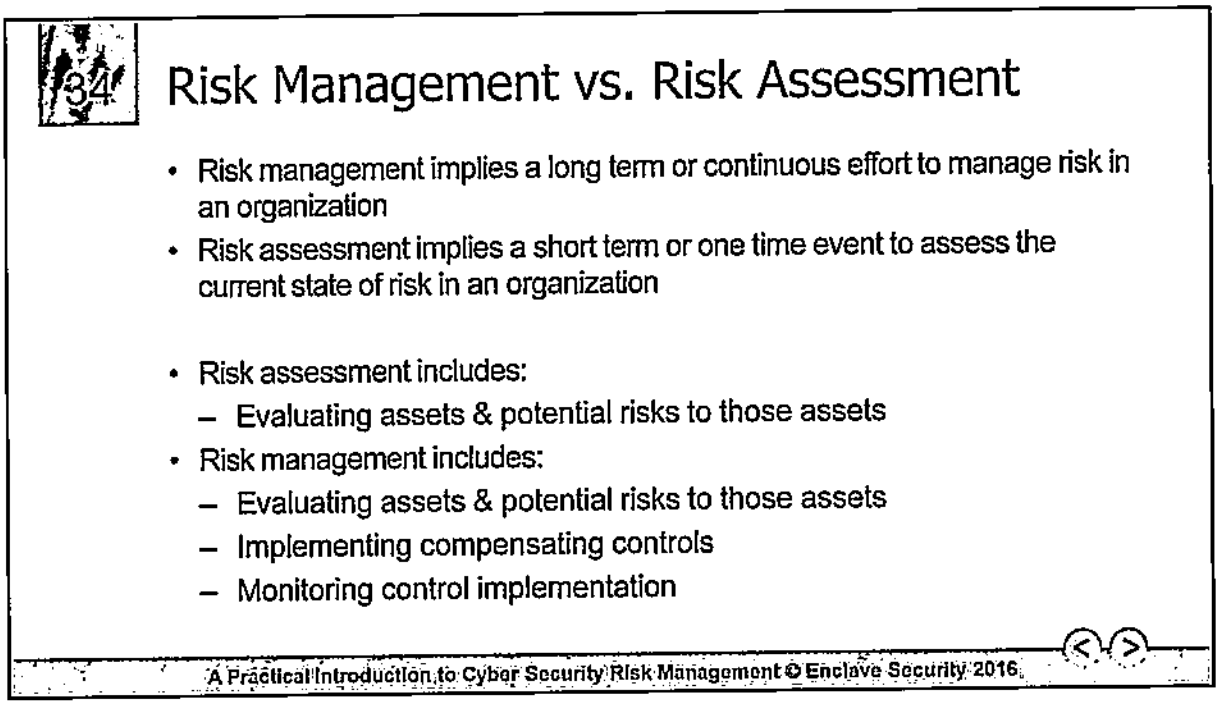


For one final NIST definition for the day, let us take a look at NIST 800-30 to obtain a definition of the term 'compensating controls':

"Compensating security controls are the management, operational, or technical controls employed by an agency in lieu of prescribed controls in the low, moderate, or high security control baselines, which provide equivalent or comparable protection for an information system." [1]

The important summary information to remember about compensating controls is that these controls are what are defined by information security policies (discussed earlier today) with the goal of lowering potential risk levels faced on a system. Most often these controls will either be used to eliminate potential threats, or more likely to eliminate potential vulnerabilities on a system.

[1] Risk Management Guide for Information Technology Systems. (n.d.). Computer Security Division Computer Resource Center. Retrieved February 1, 2011, from , from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf



We have two different ways of dealing with and measuring risk levels. One way is risk management and another is risk assessment. They both carry their own connotations and their own ideas with them.

Risk management implies a long-term or continuous effort to manage risk in an organization, but on the other hand risk assessment implies a short-term or one-time event to assess the current state of risk in an organization. Said another way, both risk management and risk assessment are concerned with evaluating assets and potential risks to those assets. Where risk management differs is that it is also concerned with implementing compensating controls and monitoring those compensating controls for effectiveness. It, therefore, becomes a cycle of assessment, implementing compensating controls, and then evaluating risks in light of those controls.

Next let us define a process by which we can perform each of these tasks. We will define one process for risk management and another for risk assessment. But although they are two processes, they are not mutually exclusive. Both are necessary for us to appropriately handle risk in our organizations.

35

ISO 27005: Risk Management Process

- The ISO 27000 series of documents define standards for Information Security Management Systems (ISMS)
- Published standards in the family include:
  - 27001 — ISMS requirements
  - 27002 — Code of practice
  - 27003 — ISMS implementation guidance
  - 27004 — ISMS measurement
  - 27005 — Information security risk management
- ISO 27005 was released in 2008 to define a standard risk management process
- Latest update was released in 2011 (ISO 27005:2011)

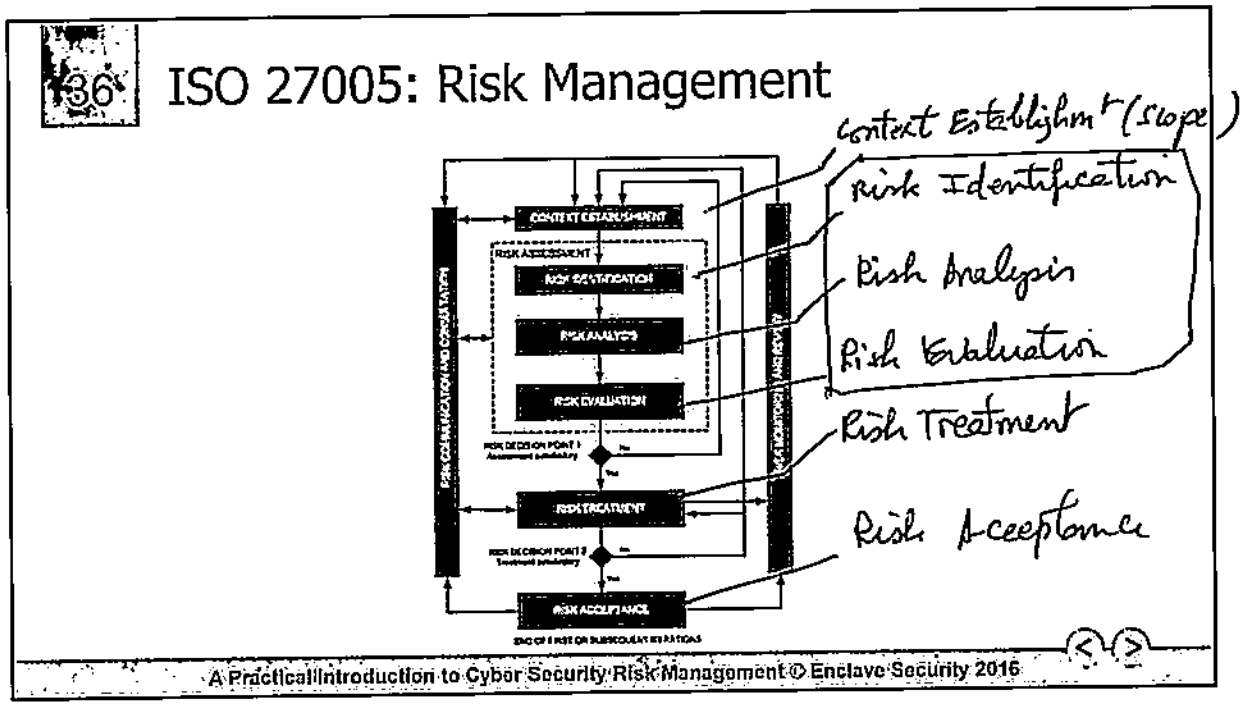
A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

One example of a process for risk management is defined by ISO/IEC 27005. This is one of a number of published standards in the ISO/IEC 27000 family of standards built around the concept of defining an organizations Information Security Management System (ISMS).

Presently there are a number of published standards in this family of standards and a number of proposed standards which have yet to reach final approval. A few examples of the standards in this family of standards are the following:

ISO /IEC 27001 — ISMS requirements
ISO /IEC 27002 — Code of practice
ISO /IEC 27003 — ISMS implementation guidance
ISO /IEC 27004 — ISMS measurement
ISO /IEC 27005 — Information security risk management

The ISO / IEC 27005 standard was originally published in 2008 (later revised in 2011) to define a lifecycle process for risk management. This standard outlines a way for an organization to defines a process that can be followed in order to perform each of the necessary steps included in a standard risk management process.



ISO / IEC 27005 defines an entire lifecycle for performing risk management. The goal of this process is to define the activities necessary in order to achieve a state of protection that is consistent with the overall goals of the business.

FBI IP Protection Summit
<YouTube>
Squirrelspike
Jeffrey Johnson

The overall defined process follows the following steps:

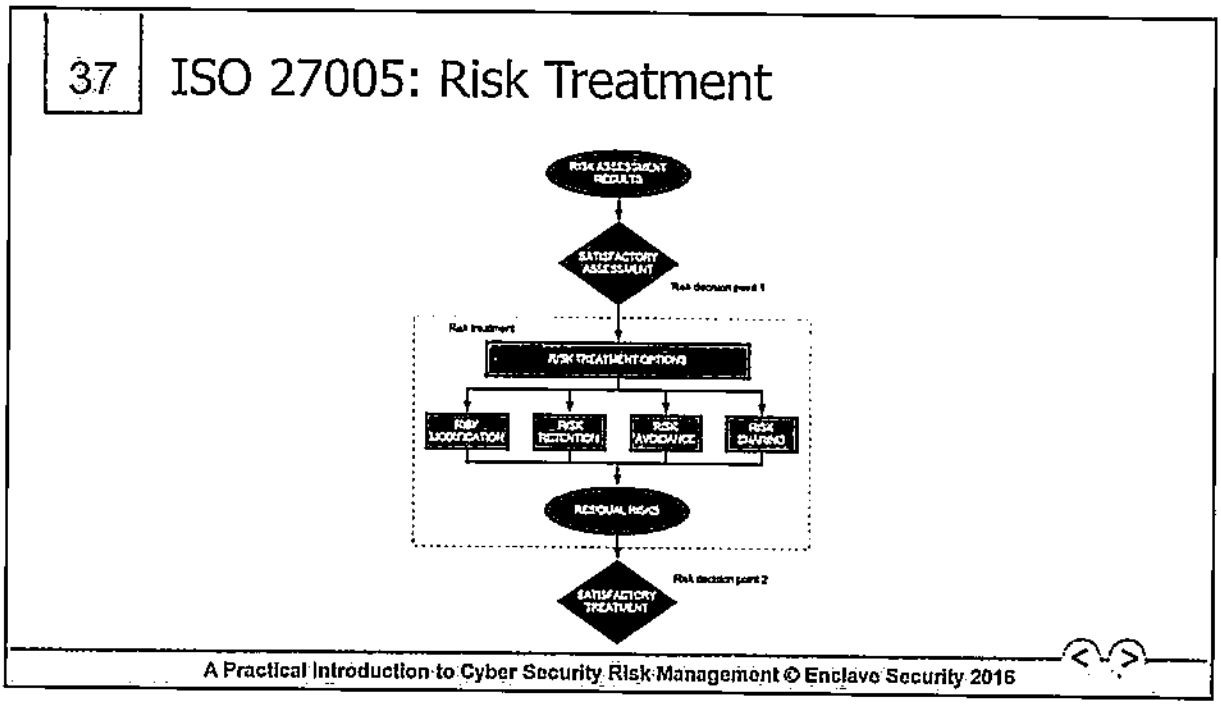
1. Context Establishment
2. Risk Assessment
3. Risk Treatment
4. Risk Acceptance
5. Risk Monitoring & Review
6. Risk Communication & Consultation

Within the context of the risk assessment process they define three primary steps. These steps are:

1. Risk Identification
2. Risk Analysis
3. Risk Evaluation

We will be focusing in this class on the steps involved in risk assessment and will practically walk through each of the steps necessary to achieve this objective.

The graphics in this slide were taken from the SANS Internet Storm Center (http://isc.sans.edu/diary.html?storyid=14332) and originally published at:
(2011). *ISO/IEC 27005 - Information technology - Security techniques - Information security risk management* (ISO/IEC 27005:2011). Geneva, Switzerland: International Standards Organization



The risk treatment process can also be further broken down into individual sub-steps which further define the process. Once a risk assessment has been performed then an organization can take the necessary steps to determine the most appropriate response to the risks that have been identified.

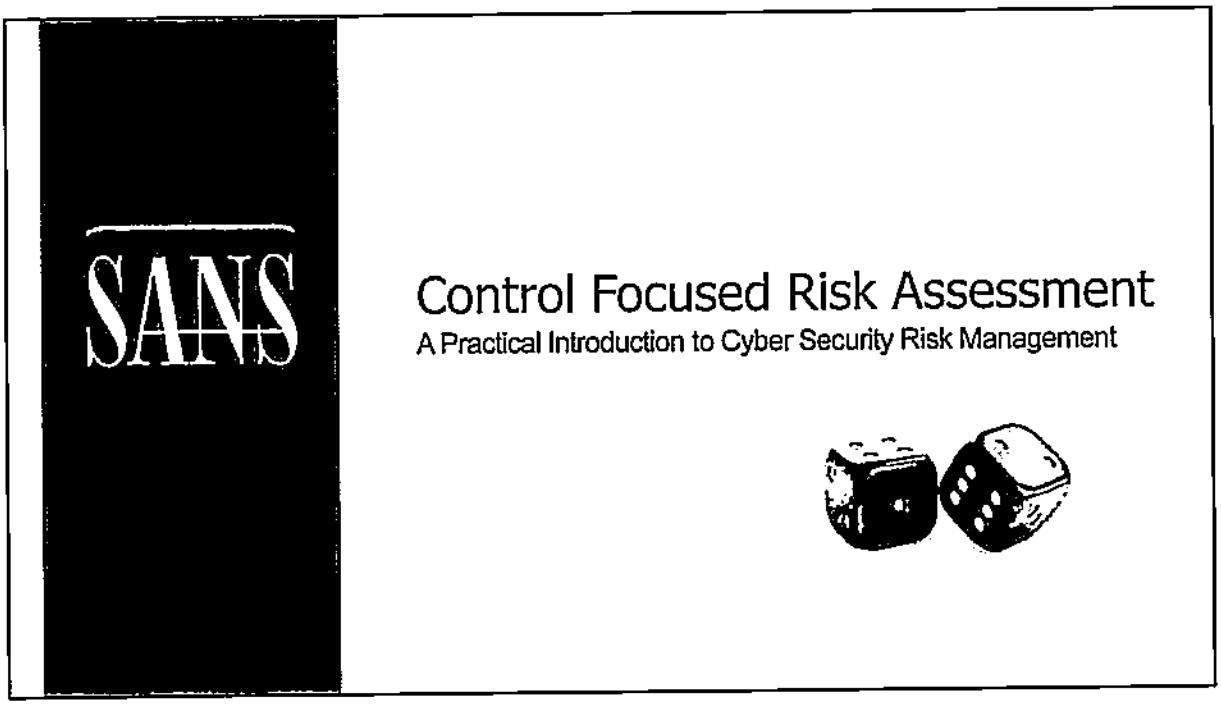
According to the ISO / IEC 27005 model, the following are potential responses to risks:

1. Risk Modification
2. Risk Retention
3. Risk Avoidance
4. Risk Sharing

Risk treatment is what we do with risk. After we have the results of the risk assessment, we can respond with one of the four ways we discussed. We will explore the process of risk treatment in more depth later in the course.

The graphics in this slide were taken from the SANS Internet Storm Center (http://isc.sans.edu/diary.html?storyid=14332) and originally published at:

(2011). *ISO/IEC 27005 - Information technology - Security techniques - Information security risk management* (ISO/IEC 27005:2011). Geneva, Switzerland: International Standards Organization



This page intentionally left blank.

39

Course Module Roadmap

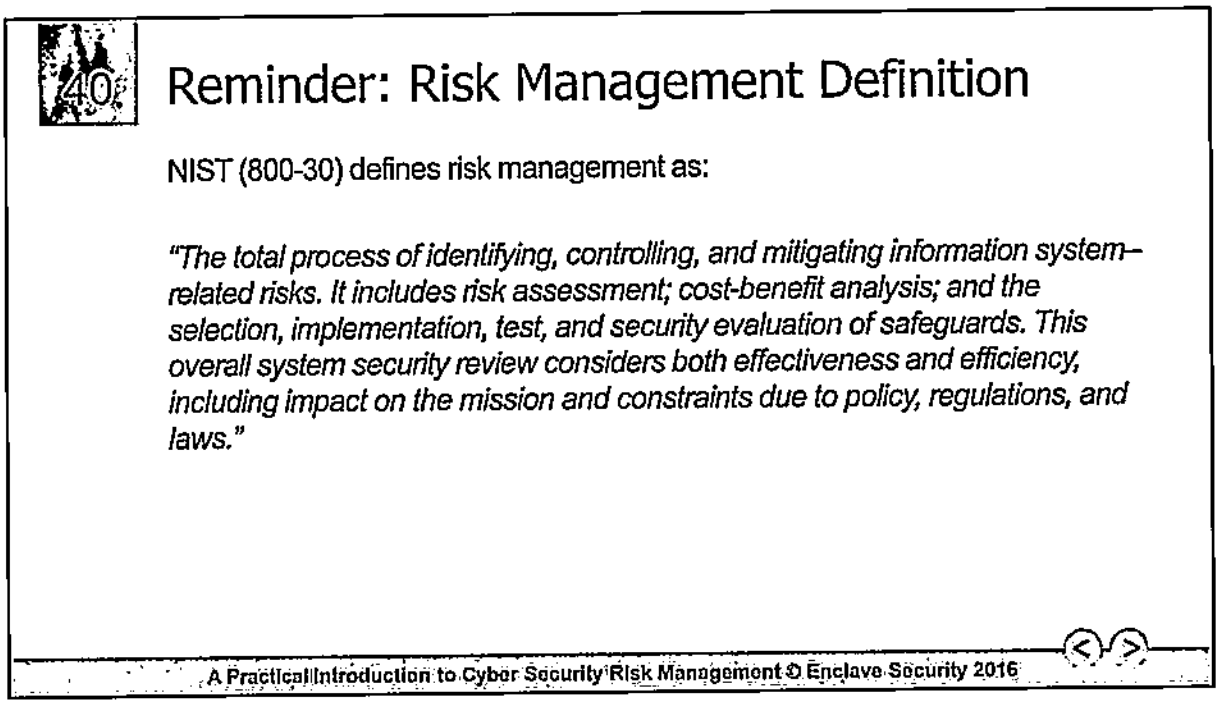
- Understanding Risk ✓
- Control Focused Risk Assessment
- How to Perform a Simple Risk Assessment
- Risk Assessment Case Study
- Formal Risk Management Models & Tools
- Event Focused Risk Management
- Risk Management Case Study
- Risk Management Software
- Risk Remediation & Response

A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

In this course we will explore the concept of risk and its practical impact on an organization. Ultimately the goal of this course is to prepare students to effectively utilize risk assessment as a tool for enterprise defense. Too many times organizations think of risk assessment and risk management as academic tools with little to no practical application. These concepts are often viewed as a formal task to pursue when an organization has free time rather than as a core business activity that drives other enterprise security efforts. In today's course students will have the opportunity to learn about the proper place of risk assessment and risk management in an enterprise. They will also be given practical skills for how to perform a risk assessment on a step by step basis, from data collection to the point of presenting their findings to business leaders. Students with a desire to perform more in depth analysis will also be given tools and formal models to consider to empower them to create a long term / formal risk management program.

Specifically today we will cover the following subjects:

- Understanding Risk
- Control Focused Risk Assessment
- How to Perform a Simple Risk Assessment
- Risk Assessment Case Study
- Formal Risk Management Models & Tools
- Event Focused Risk Management
- Risk Management Case Study
- Risk Management Software
- Risk Remediation & Response

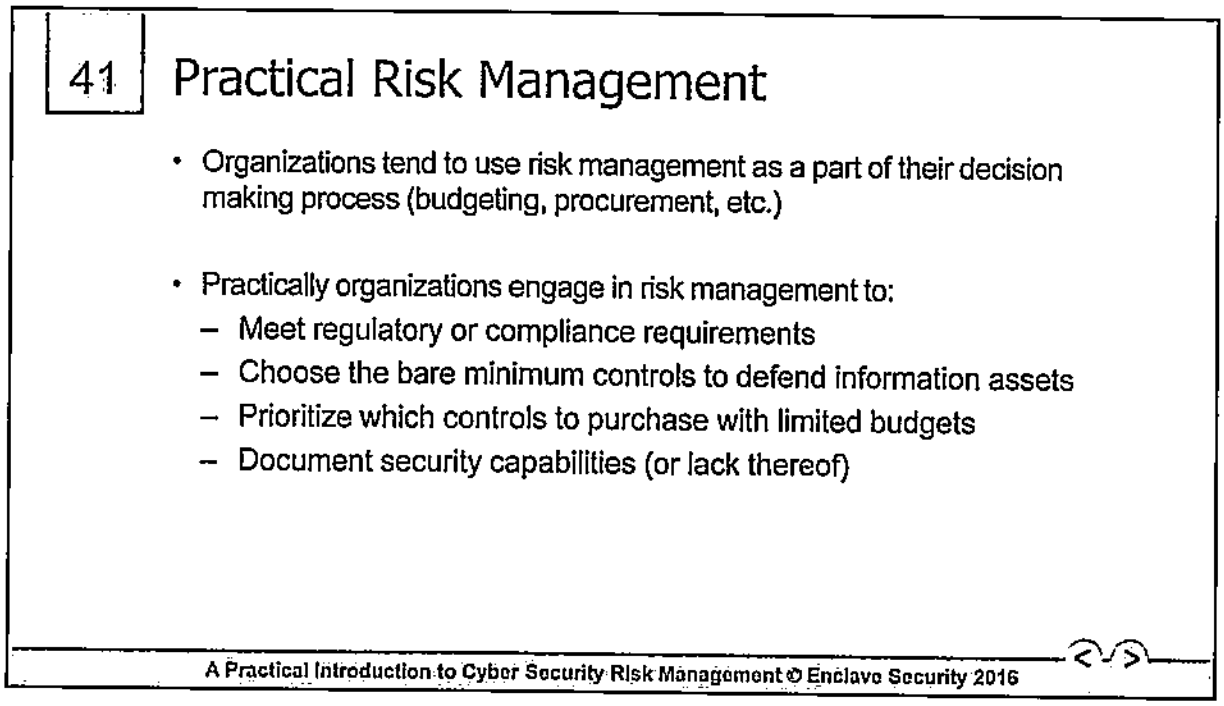


As we stated earlier, NIST gives the following definition for risk management in their NIST 800-30 guide:

"The total process of identifying, controlling, and mitigating information system–related risks. It includes risk assessment; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws." [1]

We will be coming back to this definition many times as a baseline for understanding risk management throughout this course. We pause on it here again to give context to the discussion of controls and practically why we engage in this endeavor.

[1] Risk Management Guide for Information Technology Systems. (n.d.). Computer Security Division Computer Resource Center. Retrieved February 1, 2011, from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf



Earlier in the course we noted a number of practical reasons why an organization would want to engage in the process of risk management. Practically most organizations use this discipline as a part of their decision making and reporting processes. Sometimes this is a budgeting effort, other times it is used in procurement decisions, alongside many others. There must be a practical aspect to the discipline though if it is to be worthwhile. Security practitioners are too busy to engage in purely academic exercises.

Every organization is going to have their own purpose for engaging in this practice. Depending on their business needs at the time, the purpose for pursuing risk measurements may even vary within the same company. But most will engage this process for one of the following reasons:

- Meet regulatory or compliance requirements
- Choose the bare minimum controls to defend information assets
- Prioritize which controls to purchase with limited budgets
- Document security capabilities (or lack thereof)

Due Care Due Diligence

Risk Management & Risk Likelihood

- Is an organization less likely to implement a control to defend against an attack that is less likely to occur?
- If so, how does an organization establish their threshold?

- Even with threat & vulnerability intelligence services, do we really know which control is best:
  - Host based firewalls
  - Intrusion detection systems
  - Security awareness training
  - Incident management plans

A Practical Introduction to Cyber Security Risk Management © Enclavo Security 2016

The question then has to be asked – is it any less important for an organization to implement a control to defend against an attack if that attack is less likely to occur? And if the organization should be less likely to implement the control, the follow up question has to be – where does the organization establish the threshold for when to implement a control and when not to implement a control.

For example, let's say that during an average day an organization observes 50,000 web based attacks against their web servers. As a result they choose to implement a Web Application Firewall (WAF) to defend against the attacks and buy an annual support agreement on the WAF. The next year when it comes time to renew the support agreement, the organization looks at their average web based attacks and observes that the number has fallen to 20,000 web based attacks each day. Should the organization stop paying for support on the WAF?

It is our argument that even with the more advanced threat and vulnerability intelligence services available to us that we simply do not have sufficient metrics to determine quantitatively which controls make the most sense for an organization. The best most of us can do is to implement good hygiene security controls.

43 Odds of Death for United States Residents

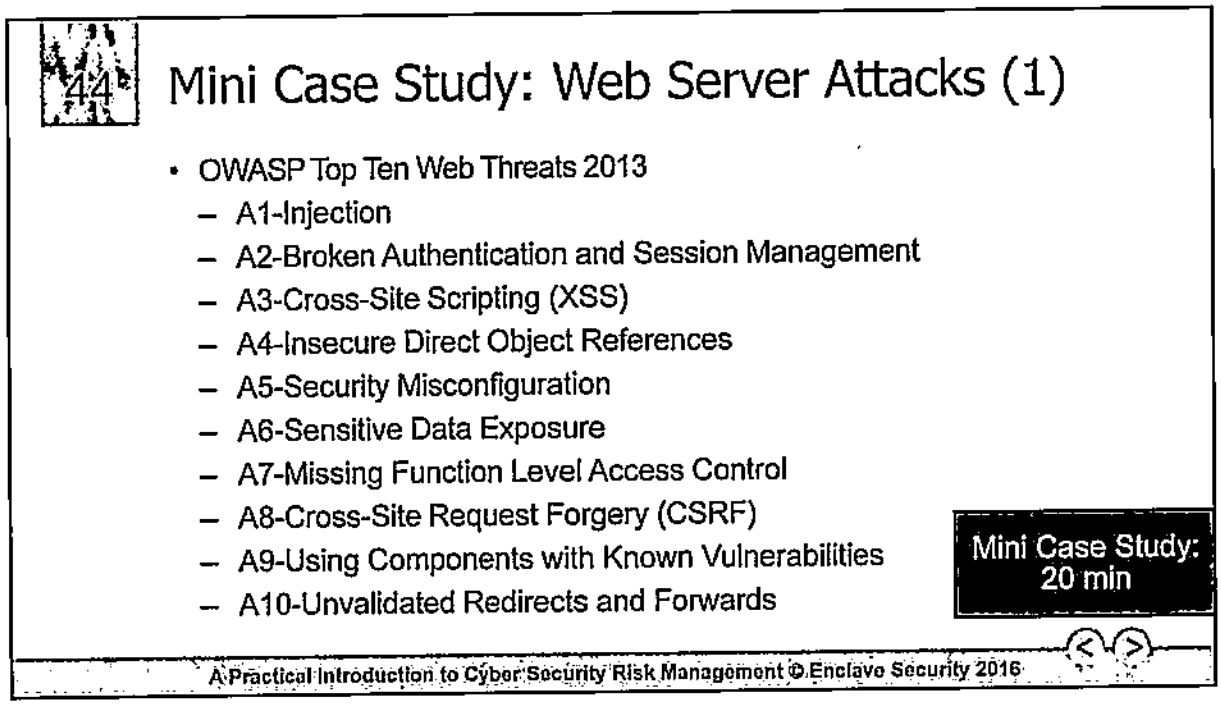
- According to LiveScience.com, people have the following chances of death (by event):
  - Heart Disease (1-in-5)
  - Cancer (1-in-7)
  - Stroke (1-in-23)
  - Accidental Injury (1-in-36)
  - Motor Vehicle Accident (1-in-100)
  - Asteroid Impact (1-in-200,000)
  - Fireworks Discharge (1-in-615,488)

- So should everyone stop trying to live healthy lives?
- Should we try to prevent heart disease, but not strokes?

It turns out that in the United States statistics are kept every year on the likelihood that a person will die from a specific event. LiveScience.com has posted the results of this research on their website (http://www.livescience.com/3780-odds-dying.html). They have reported on this site a full list of reasons why someone might die. A partial list of these events and their likelihood is listed on the above slide.

The question though should be asked: if these likelihoods are real, should people stop trying to live healthy lives? If we're just all going to die eventually anyways, why bother eating healthy, exercising, or taking care of yourself in any way? The answers of course have to do with quality of life and longevity. But in risk management terms it's a question worth considering.

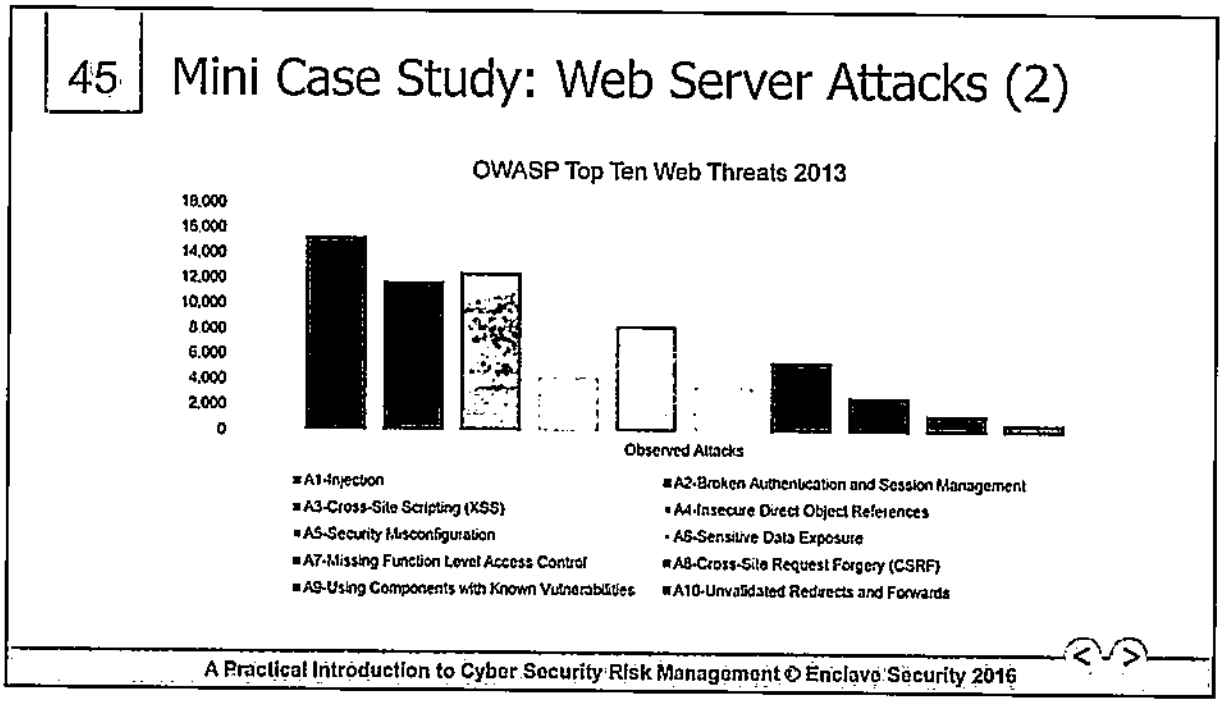
We should also ask, should we try to prevent hear disease, but not stroke, based on these figures? Is there an arbitrary line we should draw to determine which causes of death are worth addressing based on the likelihoods of those events coming to pass? Certainly the scientific community has limited resources. Should we tell them to only focus on the top percentage of the causes of death? We ask this question because we believe it is a solid analogy for information assurance and cyber security controls. Risk assessment does not give us license to simply ignore controls because we do not want to invest the resources necessary to prevent an attack. Whether we believe in the threats or not, they still exist an can cause harm to our organization.



Every few years the Open Web Application Security Project (OWASP) defines what they believe to be the top web application specific threats facing organizations are. In 2013 they defined their most recent list of threats to include all of the following:

A1-Injection
A2-Broken Authentication and Session Management
A3-Cross-Site Scripting (XSS)
A4-Insecure Direct Object References
A5-Security Misconfiguration
A6-Sensitive Data Exposure
A7-Missing Function Level Access Control
A8-Cross-Site Request Forgery (CSRF)
A9-Using Components with Known Vulnerabilities
A10-Unvalidated Redirects and Forwards

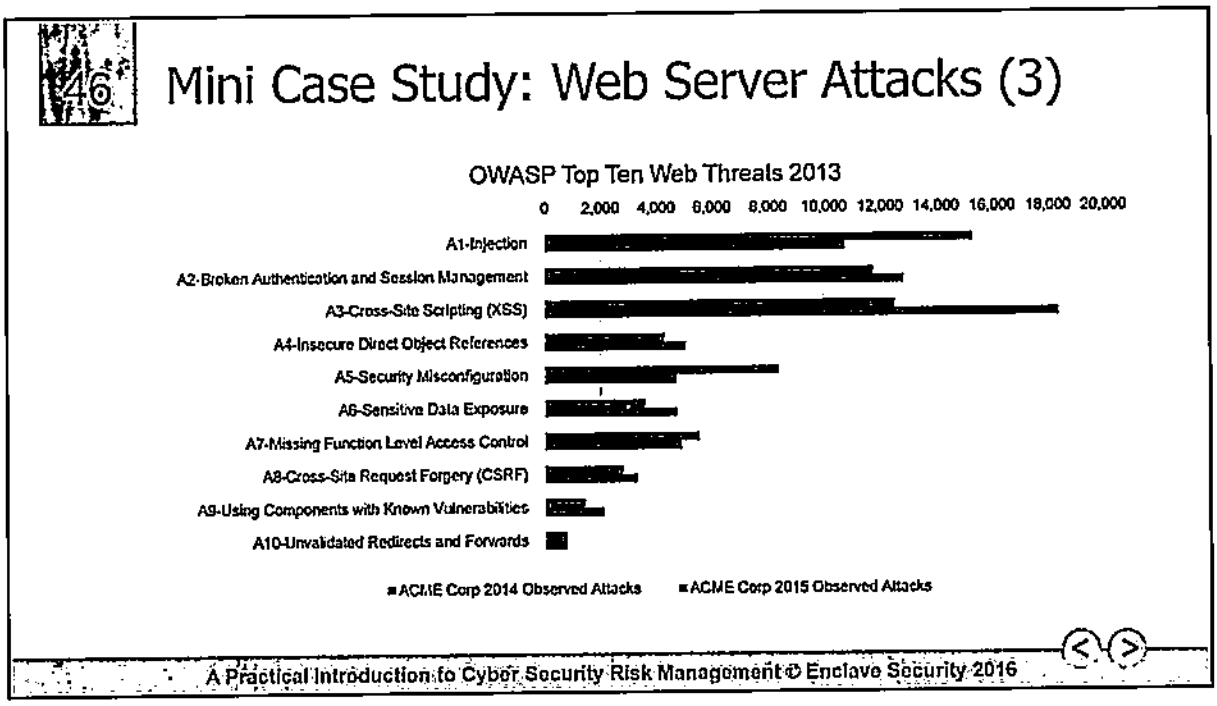
In this case study we would like to examine what an organization's response to these threats should be. Based on event data collected by an organization, should they adjust their defensive strategy? Before we can answer these questions though we need to examine all the data.



Let's say that the organization we are assessing has controls in place which give them the ability to defend and monitor for the attacks described in the OWASP Top Ten list from 2013. As a result of their monitoring capability they notice an average daily set of web based attacks similar to the numbers observed in the above graph.

Based on this information let's start our discussion by asking the following questions:

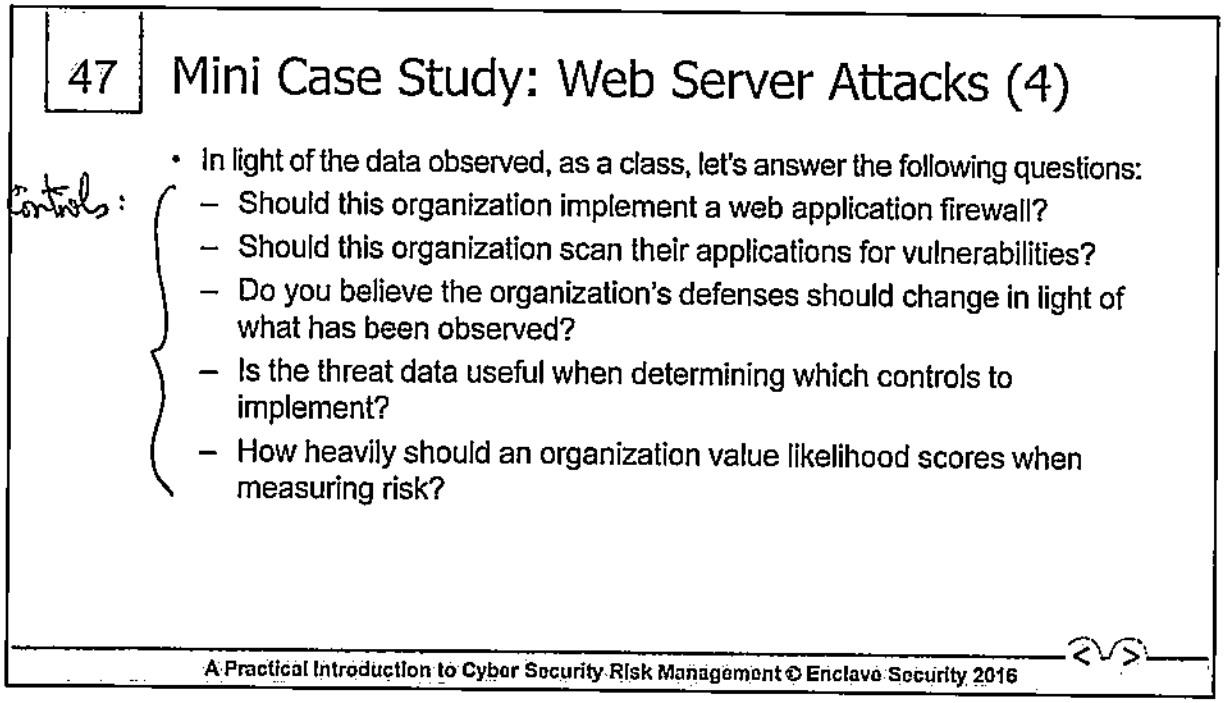
1. What are some controls that we believe could help protect this organization?
2. Because the instances of observable attacks we have observed does not exactly match OWASP's list, should we re-prioritize the implementation of our controls?



After more time goes by our organization is now able to gather more data and over a longer period of time we are able to observe attacks. We now have a daily average of attacks from 2014 and 2015 that we can compare against the OWASP Top Ten list from 2013. The above graph illustrates what we have observed on our systems. As you can see from these reports, again our observed attacks do not exactly match the priority list that OWASP has provided us. In addition it appears that some attacks are becoming less frequent against our organization and some are becoming more frequent.

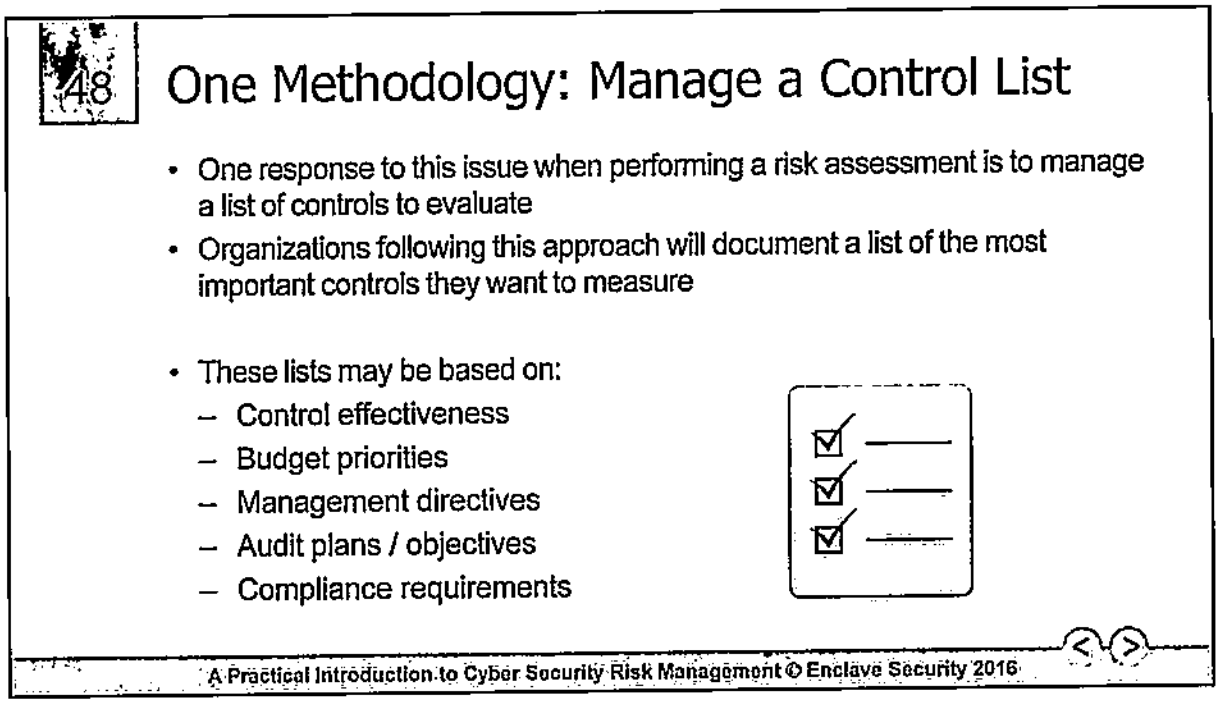
Based on this information let's start our discussion by asking the following questions:

1. Do we believe the list of controls our organization should implement has changed based on the new data?
2. Because the instances of observable attacks we have observed does not exactly match OWASP's list, should we re-prioritize the implementation of our controls?
3. Should we consider implementing new controls because of the new data? If so, which ones?
4. Should we consider decommissioning certain controls because of the new data? If so, which ones?



In fact, in light of the data provided over the previous slides, as a class let's try to answer some very specific questions:

1. Should this organization implement a web application firewall?
2. Should this organization scan their applications for vulnerabilities?
3. Do you believe the organization's defenses should change in light of what has been observed?
4. Is the threat data useful when determining which controls to implement?
5. How heavily should an organization value likelihood scores when measuring risk?

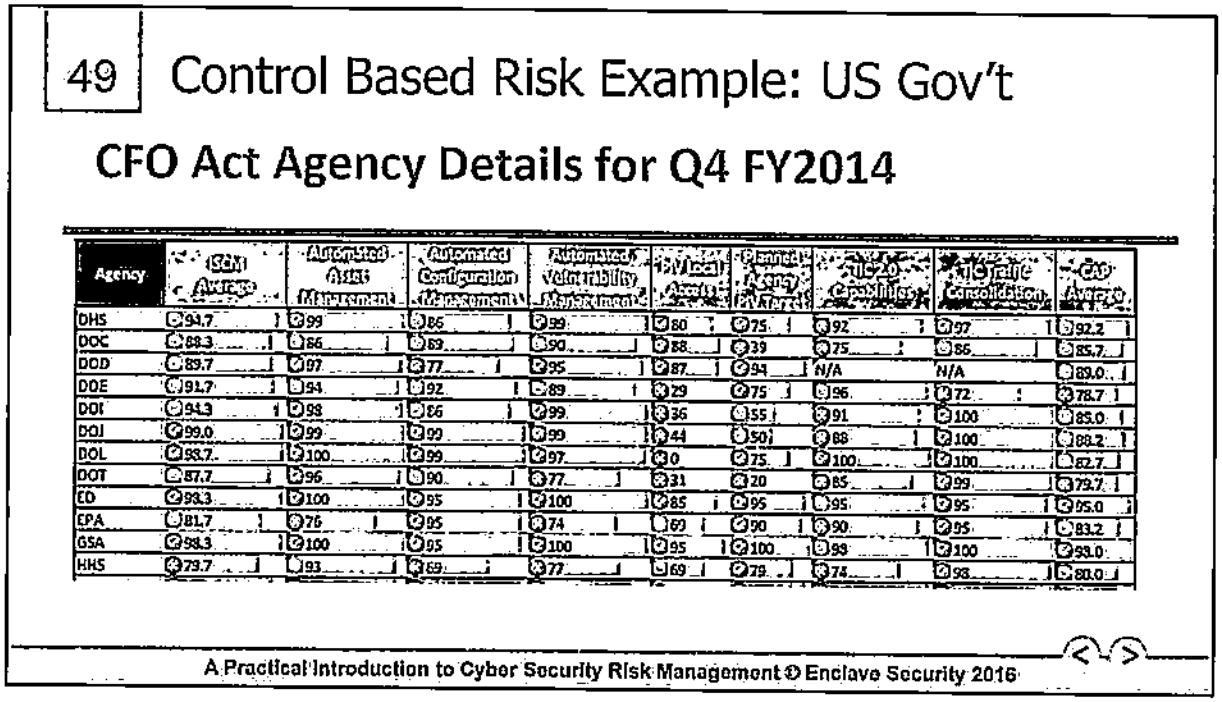


So one response to this issue in terms of risk management is to simply create a list of controls that are especially important to an organization and measure whether the organization has successfully implemented those controls or not. First the organization documents a list of what is important. Next they perform fieldwork to determine whether or not they are actually doing the things they said they want to do. Then they report on their findings. Finally if financial resources are available they can implement the control in the areas where it was observed to be missing.

Organization base these lists of controls on a number of factors. In most cases it's written and maintained by a list of the smartest cyber security professionals available to the organization at the time. Although we have observed many organizations driven by the "control of the day" promoted in the most recent trade magazines or conference. Normally these control lists are based on:

- Control effectiveness
- Budget priorities
- Management directives
- Audit plans / objectives
- Compliance requirements

But many times these lists are simply based on gut feelings and the opinions of smart people.



Agency	CAG Average	Automated Asset Management	Automated Configuration Management	Automated Vulnerability Management	PIV Local Access	PIV Remote Access	TIC 2.0 Capabilities	TIC Traffic Consolidation	CAG Average
DHS	94.7	99	86	99	80	75	92	97	92.2
DOC	88.3	86	89	90	88	39	75	86	85.7
DOD	89.7	97	77	95	87	94	N/A	N/A	89.0
DOE	91.7	94	92	89	29	75	96	72	78.7
DOI	94.3	98	86	99	36	55	91	100	85.0
DOJ	99.0	99	99	99	44	50	88	100	88.2
DOL	98.7	100	99	97	0	75	100	100	82.7
DOT	87.7	96	90	77	31	20	85	99	79.7
ED	98.3	100	95	100	85	95	95	95	95.0
EPA	81.7	76	95	74	69	90	90	95	83.2
GSA	98.3	100	95	100	95	100	99	100	98.0
HHS	79.7	93	69	77	69	79	74	98	80.0

For example, as a part of their reporting requirements for the Federal Information Systems Management Act (FISMA) of 2002, US government agencies are responsible for reporting whether they have implemented particular controls or not within their agency. In the fourth quarter of 2014 each agency reported what percentage of completion they were at on the following controls:

- Automated Asset Management
- Automated Configuration Management
- Automated Vulnerability Management
- PIV Local Access (Authentication)
- Trust Internet Connection (TIC) 2.0 Capabilities
- Trust Internet Connection (TIC) Traffic Consolidation

The above graphic shows many of the agencies' completion percentages as a part of their risk assessment. Risk is measured by whether or not the agency had implemented the particular control listed in the report.

Another Methodology: Manage a Framework

- Another methodology would be to manage a framework of controls that a third-party group has established
- This approach allows an organization to rely on the experience, research, and data of other entities
- This may also be a compliance requirement for organizations in regulated industries
- Control frameworks allow organizations to "outsource" the control list definitions, and focus on implementation instead

Another way to approach this issue is to subscribe to a particular information assurance control framework. Rather than simply documenting a list of important controls, an organization can determine which control framework they believe best meets their business needs and implement those controls. As the framework is updated they can then choose to update their control list to match the controls indicated by the framework.

This approach allows the organization to rely on the research and experiences of the body maintaining the control framework. In regulated industries this may even be a requirement. This is especially true for the financial services, healthcare, and industrial control system environments. Basically using this approach the organization outsources the control selection component of risk management and everything that leads to that process, and allows the organization to focus on control implementation and assessment.

51 Control Frameworks

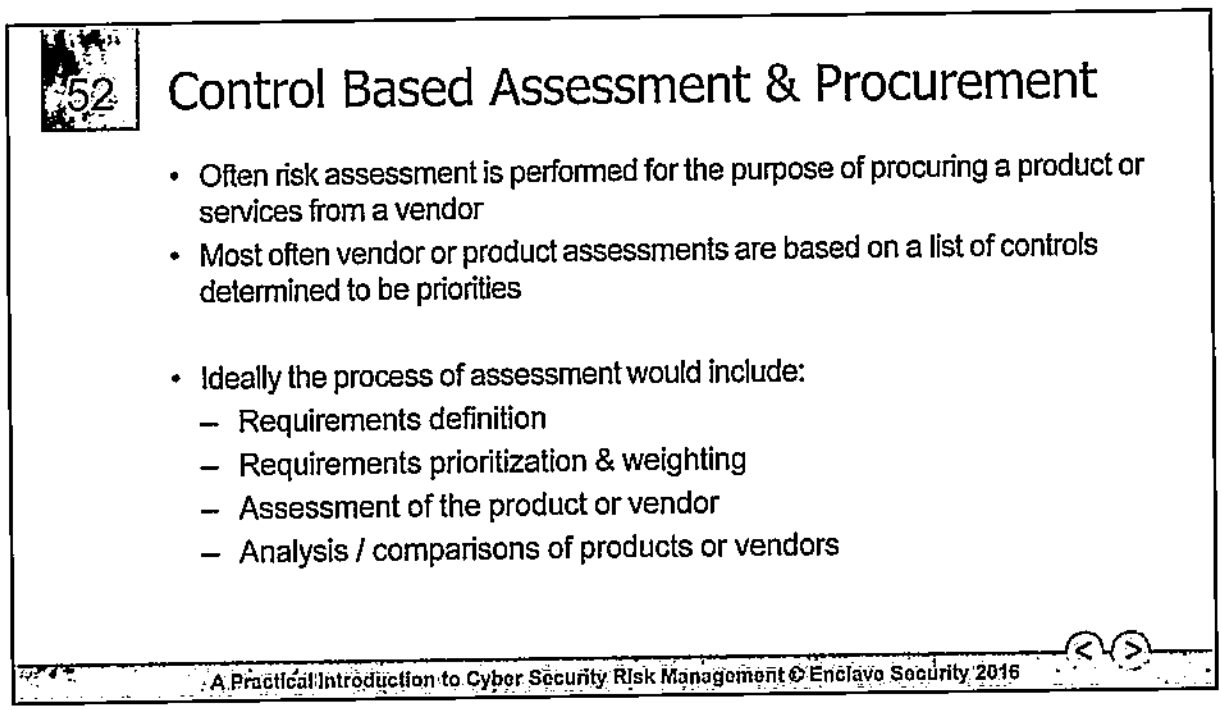
- There are numerous examples of control frameworks an organization might consider, including:
  - The Critical Security Controls (CIS)
  - NIST Cyber Security Framework (US Government)
  - NIST 800-53 (US Government) (> 1,000 controls)
  - The 27000 Series (ISO)
  - CoBIT (ISACA)
  - PCI Data Security Standard (PCI Council) ← Credit Card
  - IT Examiners Handbook (FFIEC) ← Finance
  - HIPAA / HITECH (US Government) ← Health

A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

There are a number of very solid information assurance control frameworks that an organization can choose from when trying to determine which controls to implement. There are good reasons for implementing each different framework and there is no right answer to which an organization should choose. Everyone will have biases, but ultimately each organization will need to make this decision for themselves. Some of the more common frameworks organization choose are:

- The Critical Security Controls (CIS)
- NIST Cyber Security Framework (US Government)
- NIST 800-53 (US Government)
- The 27000 Series (ISO)
- CoBIT (ISACA)
- PCI Data Security Standard (PCI Council)
- IT Examiners Handbook (FFIEC)
- HIPAA / HITECH (US Government)

There are also many organization that for regulatory reasons especially may find themselves needing to implement more than one of these frameworks. These organizations will want to reflect each of the necessary guides into their own individualized policies.

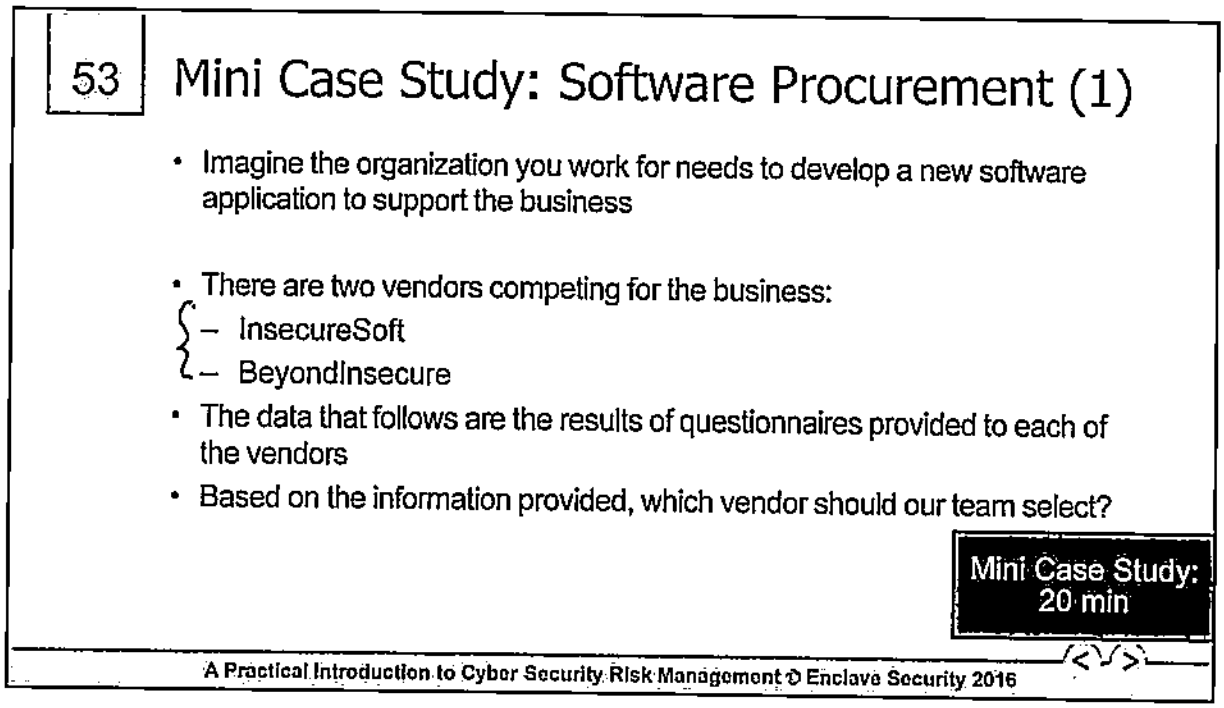


Another reason why organizations will often endeavor to pursue risk assessment is as a part of their procurement lifecycles. They perform a risk assessment as a part of procuring a product or services from a vendor. When an organization does business with another organization they want to know that the other organization is going to protect their data and provide quality services. By evaluating the security posture of the other organization, it can help determine which vendor should be preferred.

As with the other control centric risk assessment techniques discussed already, procurement teams may want to consider a few additional steps in their process. At a high level, these steps would include:

- Requirements definition
- Requirements prioritization & weighting
- Assessment of the product or vendor
- Analysis / comparisons of products or vendors

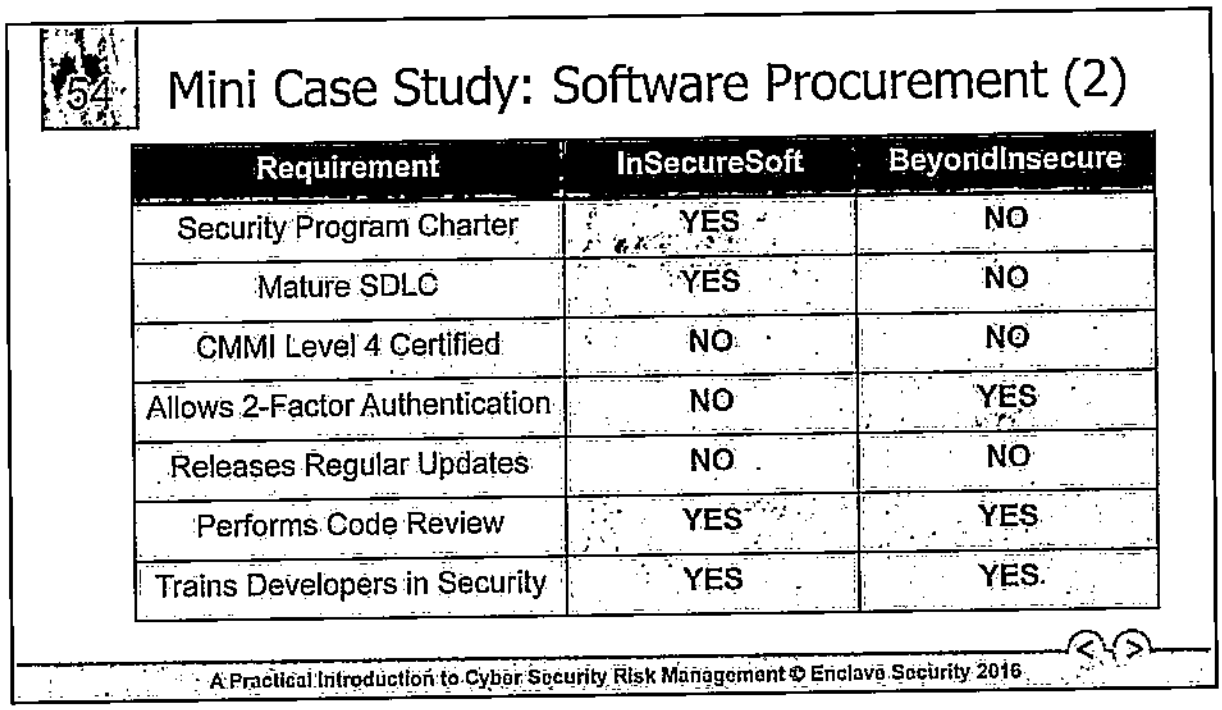
Each procurement team should develop an assessment lifecycle that feeds into their vendor management system.



In our next case study we are going to take more of a procurement point of view for risk assessment. Whether you are a part of a professional procurement or product evaluation team or not, the time will likely come when you are responsible for making a recommendation on which software vendor to use for a particular project.

In this case study our organization has decided that we would like to develop a new application to support one of our organization's critical business processes. In this case we have narrowed the field of vendors down to two companies competing for the contract: InsecureSoft and BeyondInsecure. We have provided risk assessment questionnaires to each of the vendors to better understand their security processes and determine which company will best meet our needs.

In the slides that follow we will see the results of the questionnaires that were provided to them regarding their security capabilities. Considering security as the only business requirement our team needs to evaluate, let's examine their responses.



In the above graph we can see the responses from both of the vendors we are considering. In some cases they have answered yes to our questions and in others they have answered no. In the questionnaires the marketing teams from each vendor gave very long explanations for each of the questions, but we have boiled down their responses to the above graph for a more fair comparison.

As you can see InsecureSoft seems to be more mature in the governance component of information assurance, while BeyondInsecure seems to be better technically equipped.

Is this information enough for us to make a decision on which vendor we should select? If not, what additional information might help us to make a decision?

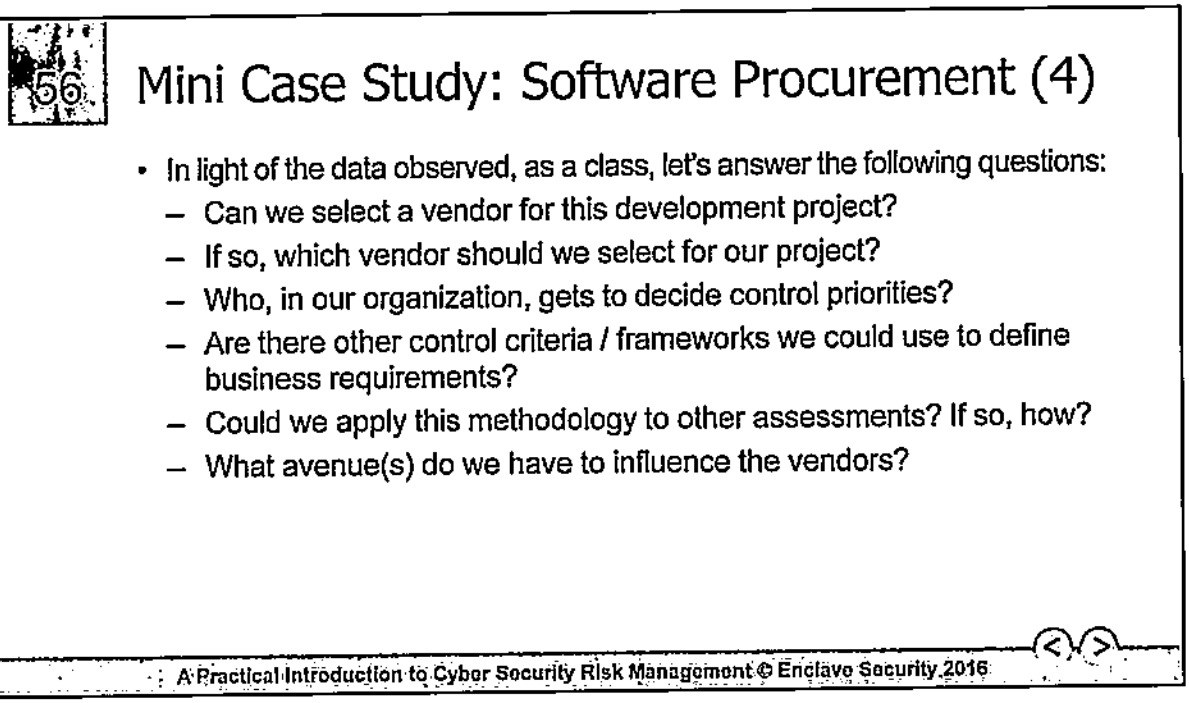
55 Mini Case Study: Software Procurement (3)

Requirement	Weight	InSecureSoft	BeyondInsecure
Security Program Charter	10%	YES	NO
Mature SDLC	20%	YES	NO
CMMI Level 4 Certified	10%	NO	NO
Allows 2-Factor Authentication	20%	NO	YES
Releases Regular Updates	15%	NO	NO
Performs Code Review	15%	YES	YES
Trains Developers in Security	10%	YES	YES
Overall Score:	100%	55%	45%

In the above graph our team decided to provide business requirement focused weights to each of the questions that we asked the vendors. The above graph illustrates the answers to the same questions we considered in the previous slide. However in this case we have added weight values to each of the questions. This enables us to score each vendor based on the requirements list that we developed.

With this information available to us, does this make it easier for us to choose a vendor?

Is the difference between the vendors significant enough to sway the decision one way or another?



In light of the data we have collected so far, it is now time for us to make a decision which vendor to recommend based on the security requirements we have defined and the data received from each of the vendors. In light of the information gathered let's answer the following questions:

1. Can we select a vendor for this development project?
2. If so, which vendor should we select for our project?
3. Who, in our organization, gets to decide control priorities?
4. Are there other control criteria / frameworks we could use to define business requirements?
5. Could we apply this methodology to other assessments? If so, how?
6. What avenue(s) do we have to influence the vendors?

SharedAssessments.org ← contracting
→ list of questions / controls for outsourcers
"free version?"

57

Control vs. Event Based Risk Management

- Another way to calculate risk is to include values based on events that occur
- Rather than basing all calculations on what an organization is or is not doing securely, we include events as well

- For example, relevant events might include:
  - Application attacks against a web server
  - Vulnerabilities discovered in an application
  - Failed logon attempts detected on a server
  - Malicious binaries discovered on a workstation
  - Phishing attacks detected on an e-mail system

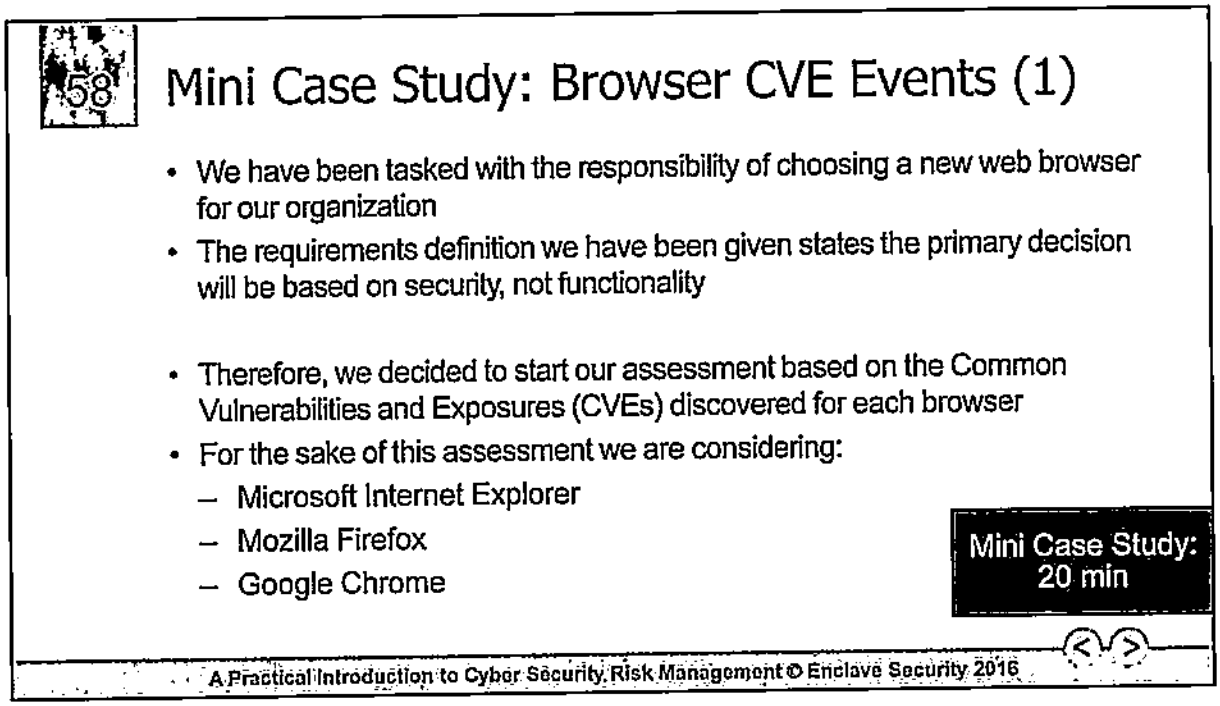
A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

When performing risk assessments, there are two primary datasets an organization can use as inputs to the process. They can calculate risk values based on the presence or absence of controls and they can evaluate the volume of specific events occurring on a system. Rather than basing all risk decisions on the presence of a control, they can also consider the events occurring as indicators of risk that may be faced on a system.

For example, an organization may want to consider any of the following events as indicators of potential risk on a system:

- Application attacks against a web server
- Vulnerabilities discovered in an application
- Failed logon attempts detected on a server
- Malicious binaries discovered on a workstation
- Phishing attacks detected on an e-mail system

We will discuss event based risk management more later in the course.



For our next case study let's examine a more event based approach to risk assessment.

In this case we have been tasked with the responsibility to choose which web browser we are going to standardize on for the organization. There are multiple teams working on this project and each is evaluating a different set of business requirements for the browsers. Our team's responsibility is to evaluate the security of each browser in order to determine which browser makes the most sense for our organization.

Assuming we have already evaluated the security functionality of the browsers, in this case study we will be evaluating the likelihood that a browser will have coding based weaknesses in the browser. We will do this by comparing the Common Vulnerabilities and Exposures (CVEs) for each of the three major browsers – IE, Firefox, and Chrome.

59 Mini Case Study: Browser CVE Events (2)

Consider the vulnerabilities (CVEs) published for Microsoft IE:

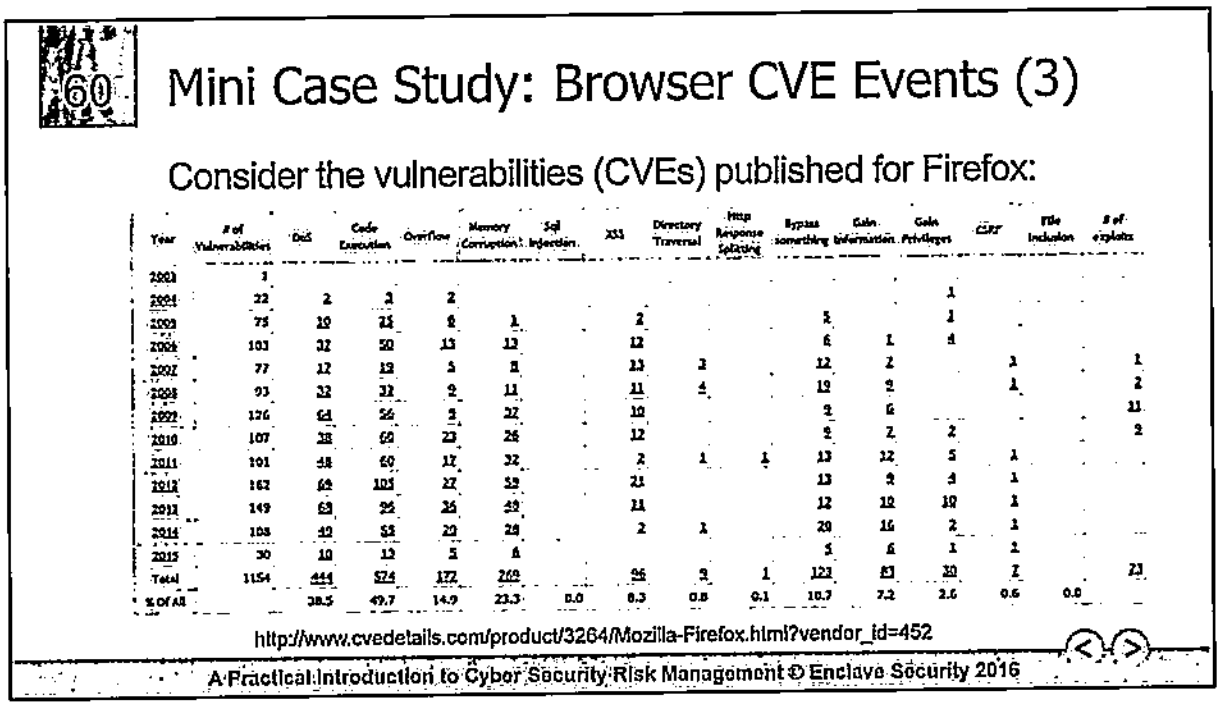
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2002	2	1	2	1	1										1
2003	37	6	24	6	17		6			10	5				5
2009	33	7	21	7	13		1								2
2010	2		2		1										1
2012	18		18	2	2										
2013	129	77	117	61	77		2			2	6	2			1
2014	243	213	220	181	213		8			10	2	6			3
2015	52	44	44		44		1			4	1	3			
Total	516	348	448	258	368		18			29	19	12			29
% Of All		67.4	86.8	50.0	71.3	0.0	2.7	0.0	0.0	5.6	3.7	2.3	0.0	0.0	

http://www.cvedetails.com/product/9900/Microsoft-Internet-Explorer.html?vendor_id=26

The above data is from cvedetails.com and outlines the CVEs or software based weaknesses that have been discovered for Microsoft's Internet Explorer browser.

As you can see from the above graph, we can analyze the number of vulnerabilities discovered by year and by the type of vulnerability discovered. Aggregate counts of each vulnerability are also listed at the bottom of each graph for comparative purposes.

Take a minute to peruse these numbers and familiarize yourself with the volume of weaknesses detected for this browser.



Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2003	1											1			
2004	22	2	2	2											
2005	75	10	23	8	1		2			5		1			
2006	103	32	50	13	13		12			6	1	4			
2007	77	12	13	5	8		23	3		12	2		3		1
2008	93	32	33	9	11		11	4		19	9		1		2
2009	126	64	56	9	22		10			9	6				11
2010	107	38	60	23	26		12			9	7	2			9
2011	101	48	60	17	32		2	1	1	13	12	5	1		
2012	162	69	103	27	59		21			13	9	9	1		
2013	149	63	95	26	49		11			12	10	10	1		
2014	108	49	58	20	28		2	1		20	16	2	1		
2015	30	10	13	5	6					5	6	1	1		
Total	1154	444	574	172	269		96	9	1	123	83	30	7		23
% of All		38.5	49.7	14.9	23.3	0.0	8.3	0.8	0.1	10.7	7.2	2.6	0.6	0.0	

The above data is from cvedetails.com and outlines the CVEs or software based weaknesses that have been discovered for Mozilla's Firefox browser.

As you can see from the above graph, we can analyze the number of vulnerabilities discovered by year and by the type of vulnerability discovered. Aggregate counts of each vulnerability are also listed at the bottom of each graph for comparative purposes.

Take a minute to peruse these numbers and familiarize yourself with the volume of weaknesses detected for this browser.

61

Mini Case Study: Browser CVE Events (4)

Consider the vulnerabilities (CVEs) published for Chrome:

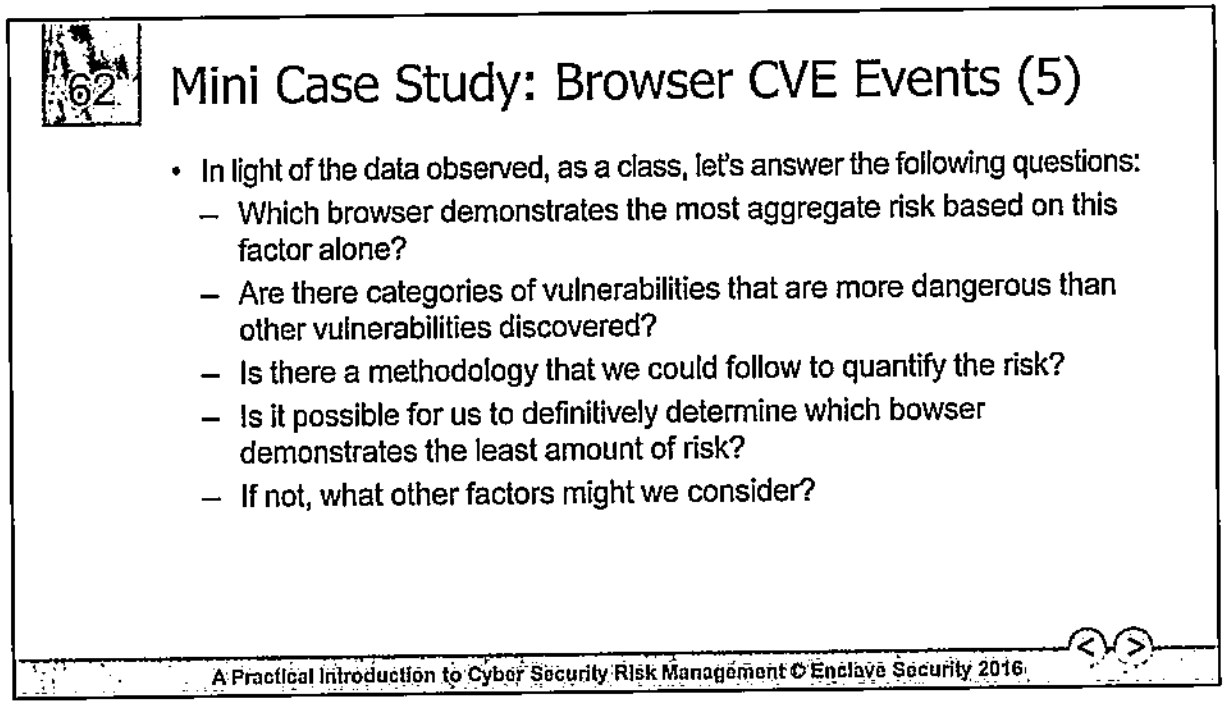
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2008	3	1	1				1								2
2009	39	15	11	8	3		2			1	3		1		8
2010	152	82	22	26	27		4			14	14		1		2
2011	266	188	11	62	12		3			21	8	1			
2012	249	195	13	63	9		8			14	8	2			
2013	175	121	6	42	13		3	1		9	7				
2014	127	86	3	19	4		8	2		14	6		1		
2015	62	51		16	6		1			3		2			
Total	1073	740	68	235	74		35	6		79	55	5	3		12
% of All		69.0	6.3	22.0	6.9	0.0	3.3	0.6	0.0	7.4	4.3	0.5	0.3	0.0	

http://www.cvedetails.com/product/15031/Google-Chrome.html?vendor_id=1224

The above data is from cvedetails.com and outlines the CVEs or software based weaknesses that have been discovered for Google's Chrome browser.

As you can see from the above graph, we can analyze the number of vulnerabilities discovered by year and by the type of vulnerability discovered. Aggregate counts of each vulnerability are also listed at the bottom of each graph for comparative purposes.

Take a minute to peruse these numbers and familiarize yourself with the volume of weaknesses detected for this browser.



In light of the event data we have at our disposal now we can begin to evaluate each of the browsers in our list. Again, let's assume that security events is the only criteria being considered at this time and that other business requirements, including security functionality, is being addressed at a later point. Based on the information we have collected so far in our event focused risk assessment, let's answer the following questions:

1. Which browser demonstrates the most aggregate risk based on this factor alone?
2. Are there categories of vulnerabilities that are more dangerous than other vulnerabilities discovered?
3. Is there a methodology that we could follow to quantify the risk?
4. Is it possible for us to definitively determine which bowser demonstrates the least amount of risk?
5. If not, what other factors might we consider?

63

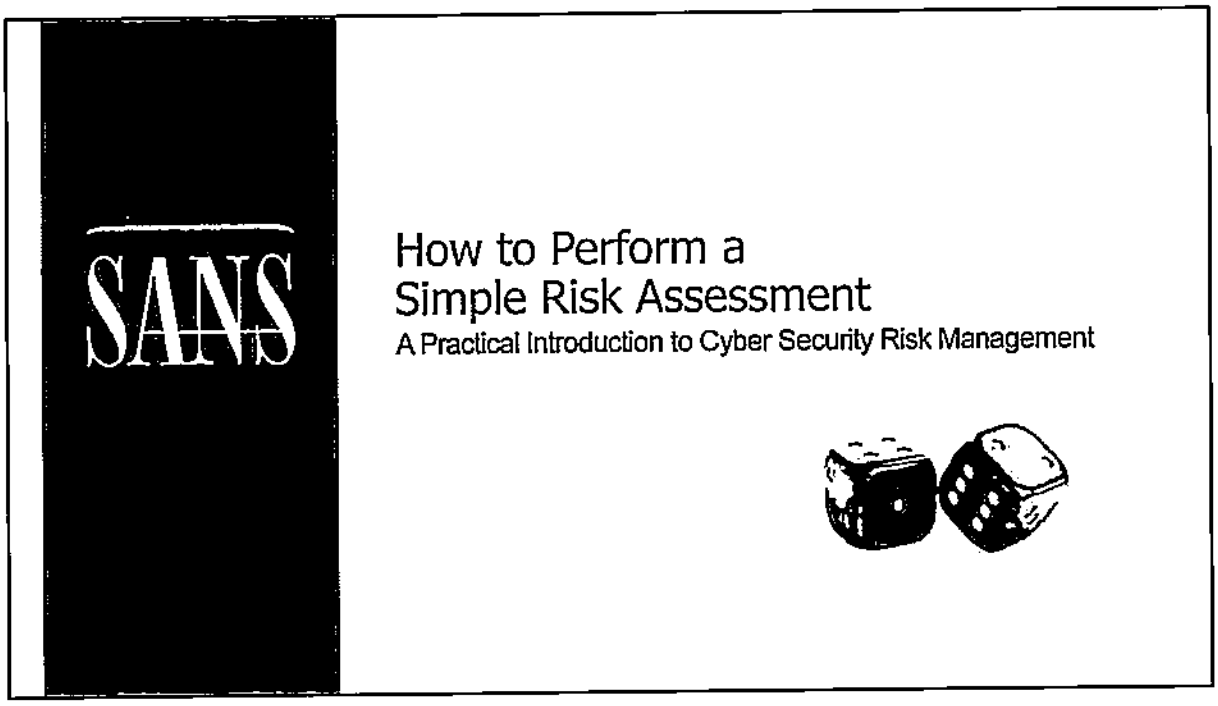
Where to go from Here?

- The focus of today's class is to define a process for performing a risk assessment
- Risk assessment is simply one piece in the bigger puzzle of risk management
- Therefore let's spend the majority of the day focusing on how to perform a single risk assessment

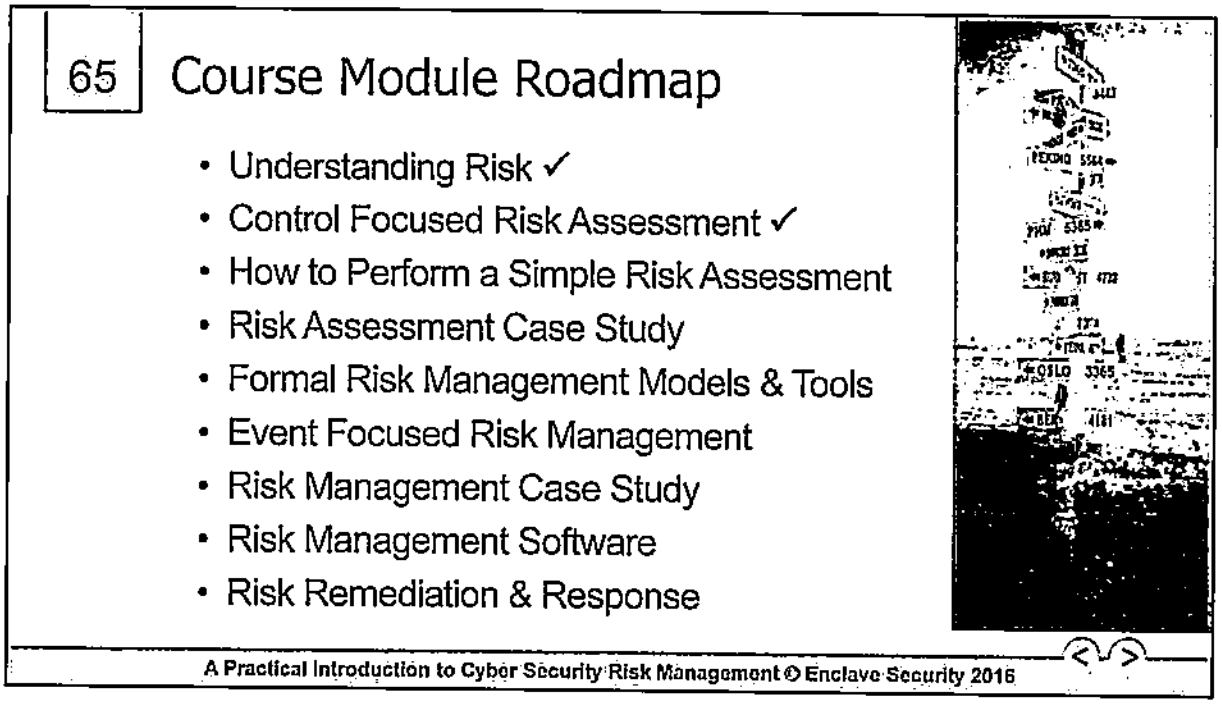
A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

At this point we have discussed a background and context for performing a risk assessment and how risk assessment fits into the overall process of performing risk management. Although it would be great to cover the entire risk management process in depth, at this point due to time constraints we will be focusing only on performing a single risk assessment.

Therefore for the remainder of the class we will be focusing our attention on how to specifically and practically perform a simple risk assessment. Let's get started!



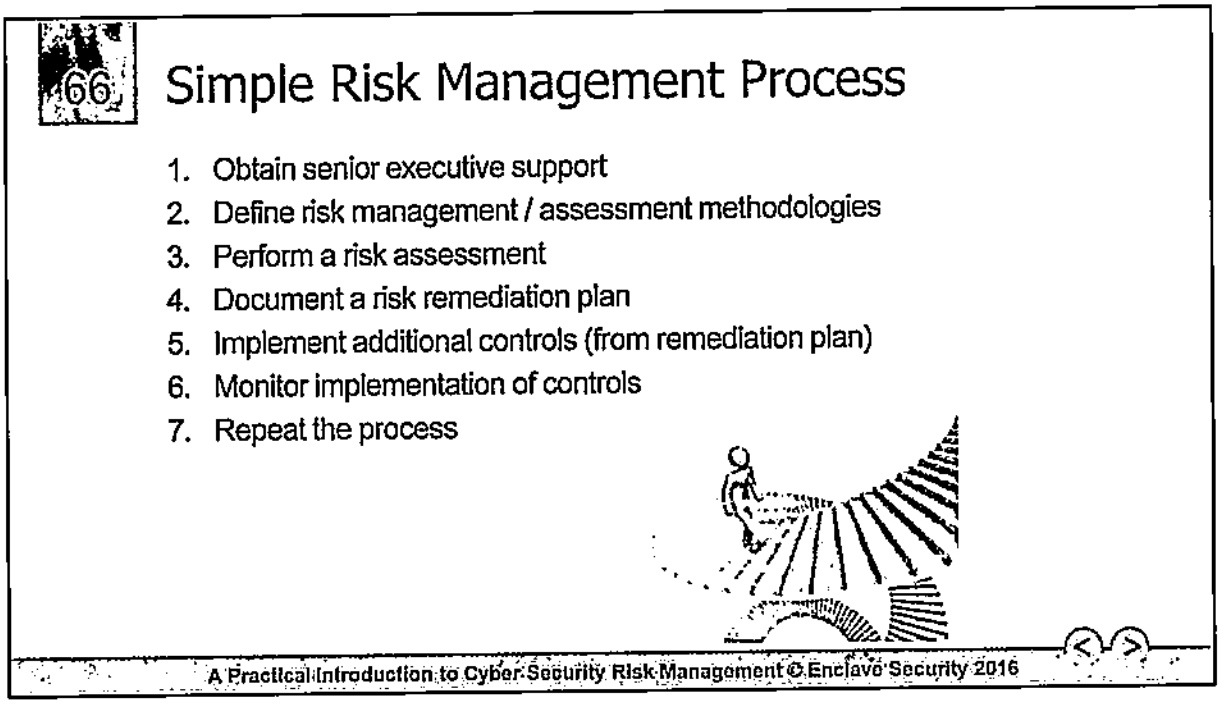
This page intentionally left blank.



In this course we will explore the concept of risk and its practical impact on an organization. Ultimately the goal of this course is to prepare students to effectively utilize risk assessment as a tool for enterprise defense. Too many times organizations think of risk assessment and risk management as academic tools with little to no practical application. These concepts are often viewed as a formal task to pursue when an organization has free time rather than as a core business activity that drives other enterprise security efforts. In today's course students will have the opportunity to learn about the proper place of risk assessment and risk management in an enterprise. They will also be given practical skills for how to perform a risk assessment on a step by step basis, from data collection to the point of presenting their findings to business leaders. Students with a desire to perform more in depth analysis will also be given tools and formal models to consider to empower them to create a long term / formal risk management program.

Specifically today we will cover the following subjects:

- Understanding Risk
- Control Focused Risk Assessment
- How to Perform a Simple Risk Assessment
- Risk Assessment Case Study
- Formal Risk Management Models & Tools
- Event Focused Risk Management
- Risk Management Case Study
- Risk Management Software
- Risk Remediation & Response

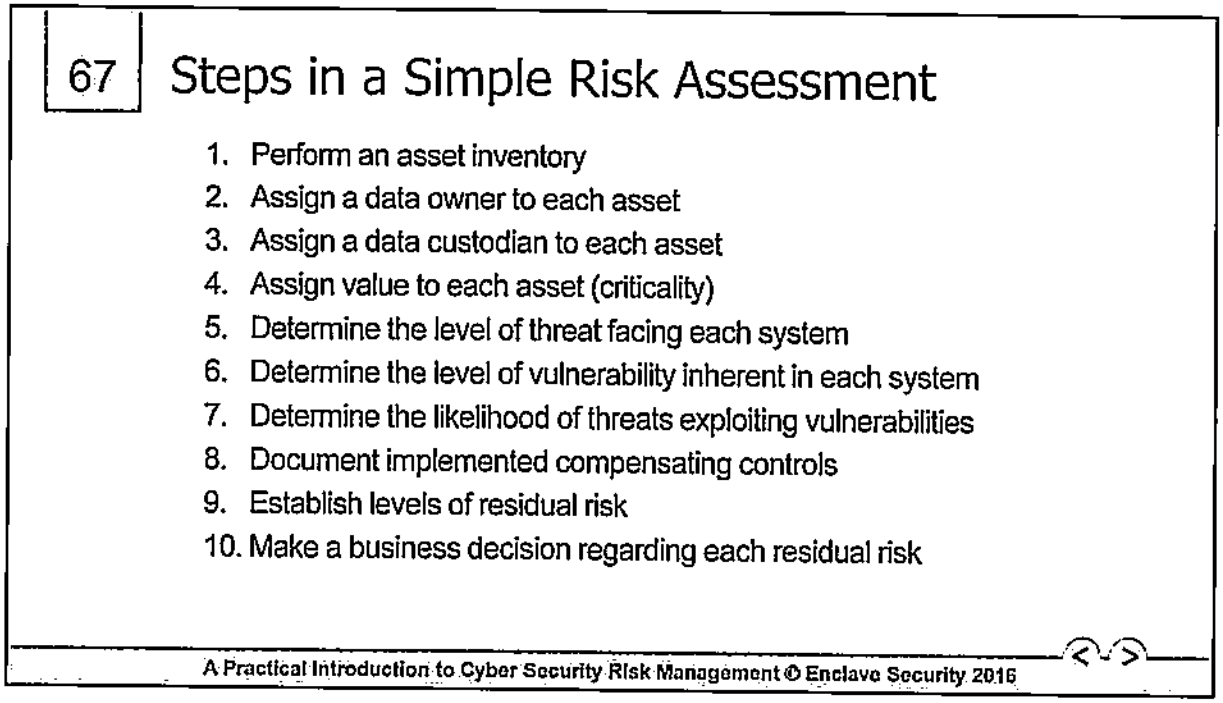


If we assume that risk management is not the same as risk assessment, then we should be able to define two separate processes, one for risk management and one for risk assessment. We will start with risk management.

Risk management implies that we will be approaching risk from a long-term perspective and evaluating risk over time. Risk management is also more focused on risk remediation than risk assessment.

Therefore, for the sake of our discussion, a simple risk management process would look something like this:

1. Obtain senior executive support
2. Define risk management / assessment methodologies
3. Perform a risk assessment
4. Document a risk remediation plan
5. Implement additional controls (from remediation plan)
6. Monitor implementation of controls
7. Repeat the process



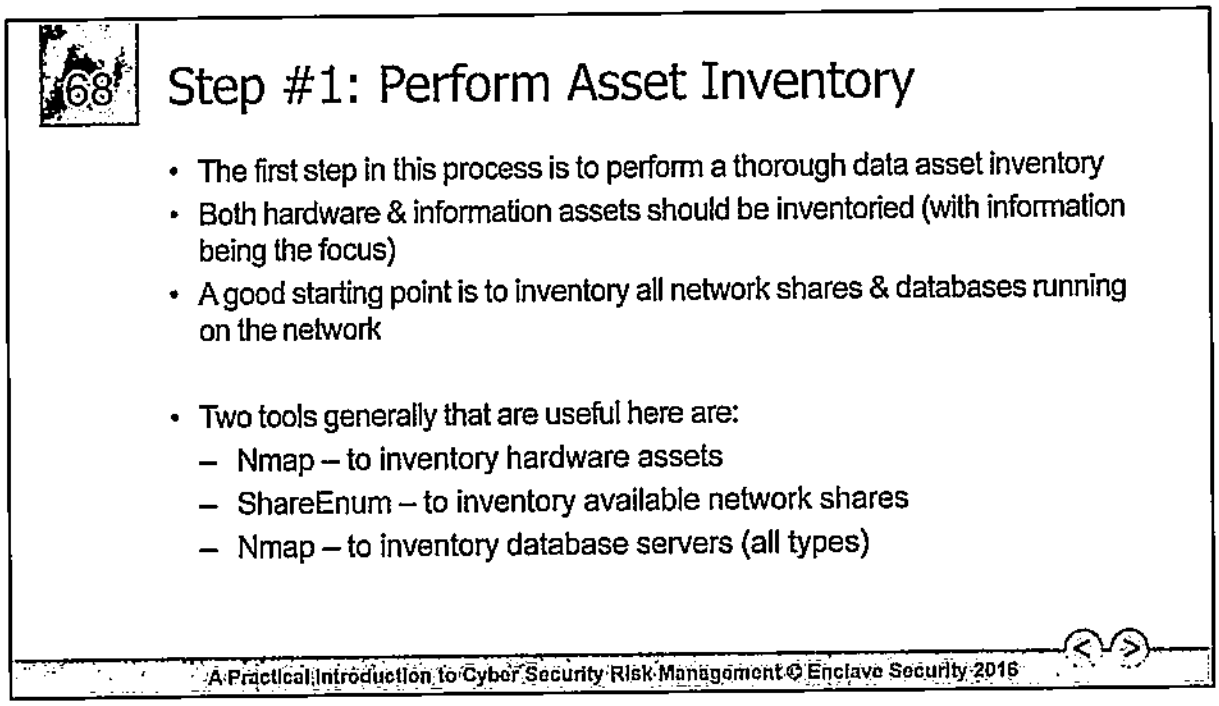
If the previous page defines a risk management process, and a sub-component of risk management is risk assessment, what would a risk management process look like?

The answers to this question are varied. There are a number of different risk assessment models that are available in the information assurance industry. Many of these models we will investigate in more depth in the next section of the course.

For now though, let us utilize a simple risk assessment methodology that can serve as a foundation for more complicated assessments later. In our opinion, the following practical steps will help get us started with a simple assessment:

1. Perform an asset inventory
2. Assign a data owner to each asset
3. Assign a data custodian to each asset
4. Assign value to each asset (criticality)
5. Determine the level of threat facing each system
6. Determine the level of vulnerability inherent in each system
7. Determine the likelihood of threats exploiting vulnerabilities
8. Document implemented compensating controls
9. Establish levels of residual risk
10. Make a business decision regarding each residual risk

Let us investigate each step in more detail now...



The first practical step in the process would be to perform a thorough data asset inventory. Or said another way, this step should be the creation of a comprehensive inventory of all of the organization's data sets. In this inventory, both hardware and information assets should be inventoried, but the purpose and focus of the inventory is to document what pieces of information exist within the organization.

So how can organizations, especially large organizations, do this kind of assessment? We have a few practical tips that we believe help as you perform this inventory. Generally when we do this we start by gathering a list of all network devices, network shares, and databases running on the network.

One tool that is often useful during this inventory is nmap or zenmap. If we run the following command (assuming 10.1.1.x is our network) we should come up with a fairly comprehensive list of devices on the network (or at least those in our subnet range with a TCP/IP stack):

Nmap –sn 10.1.1.0/24

This is known as a "Ping Sweep" or "No Port Scan" and can be used to document which devices are on our network (we will talk more about specific nmap commands and nmap parsing later in the class). [1]

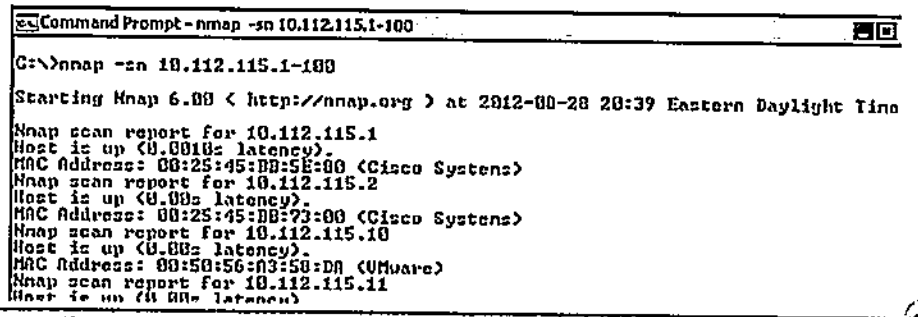
Now that we have a list of devices, the next scan would be to inventory all network shares currently available on the network. Our favorite tool for performing this type of scan is ShareEnum by Microsoft (formerly of Sysinternals). This will allow the organization to create a list of all network shares, which can later be added to the list of discovered devices.

[1] http://nmap.org/book/man-host-discovery.html

69

Asset Inventory Tool: Nmap (1)

- Nmap specifically can be used for identifying all listening nodes on a network
- An Nmap "ping sweep" can be used to generate a list of most all nodes on a network as in the following screen capture:



One technical tool that can be used to inventory the assets in an organization is the nmap tool. This is a common, popular open source security scanning tool, maintained by Fyodor, and can be downloaded for free at http://www.insecure.org. Nmap as a tool has the ability to perform many different types of tasks, and is commonly used for tasks such as port scanning, asset identification, service version detection, operating system fingerprinting, and many other similar tasks.

One scanning capability of the tool is the ability to perform a "Ping Sweep" which identified all of the network hosts in a network scope. By running the following command, an administrator will be able to list all of the listening systems in a network scope by IP address and MAC address:

Nmap –sn <IP address range>

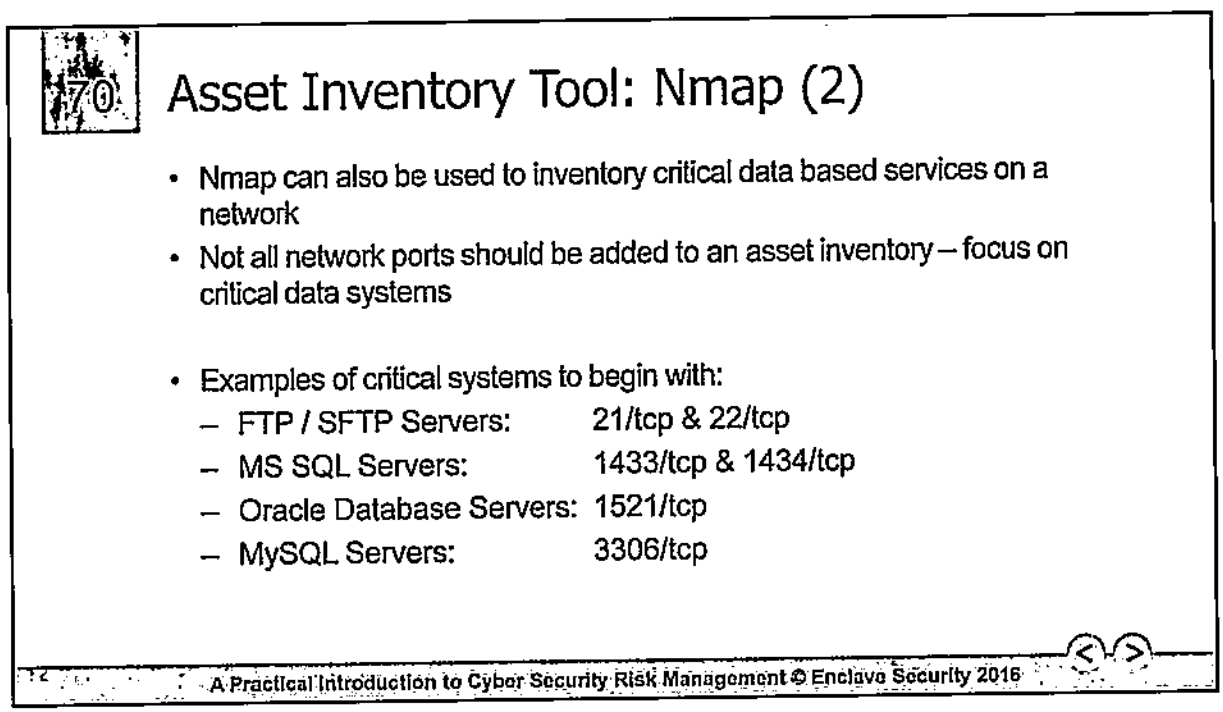
By running this command you will be able to extract a list of all of the systems in a given network range. Although paperwork asset inventories are helpful, often times it is helpful to validate such a list with a network tool. Nmap provides a method of scanning that will enable the person performing a risk assessment to validate the list of assets maintained by the organization being assessed.

An example of the nmap command in action can be found in the above screen capture.

Finally, we would run the Nmap command one final time with the following command:

Nmap –sS –P0 –p1-4000 10.1.1.0/24

This command will perform a basic port scan of the systems on our network and help us to identify any systems running database listening ports. These also should be added to our inventory as data assets.



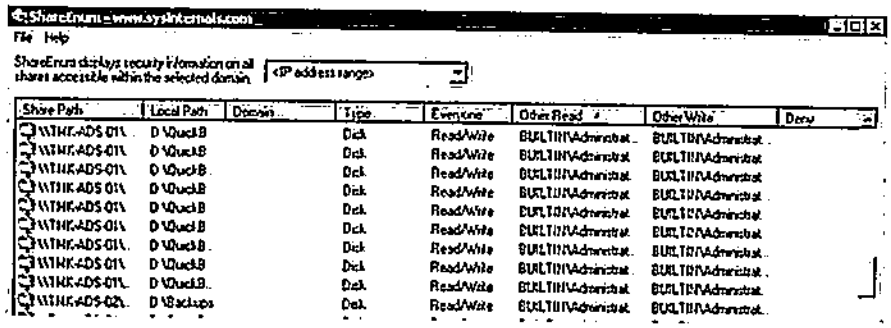
In addition to being able to identify individual network nodes that can be added to an asset inventory, Nmap also gives the ability to identify critical locations where data is being stored on a network. Using Nmap we can scan for more than vulnerabilities, we can also scan for locations where data might be stored. Which network services are listening will indicate the type of data being stored on that system.

The focus of addition Nmap scans is to find data, not simply to inventory listening ports. The focus of additional scans is to identify assets protecting data. The following ports are examples of listening ports likely to indicate that data is being stored on that system:

FTP / SFTP Servers:	21/tcp & 22/tcp
MS SQL Servers:	1433/tcp & 1434/tcp
Oracle Database Servers:	1521/tcp
MySQL Servers:	3306/tcp

71 Asset Inventory Tool: ShareEnum

- ShareEnum from Microsoft (formerly SysInternals) has the ability to identify Windows network shares (file shares)
- Microsoft shares host data which should be defined as assets in a risk assessment



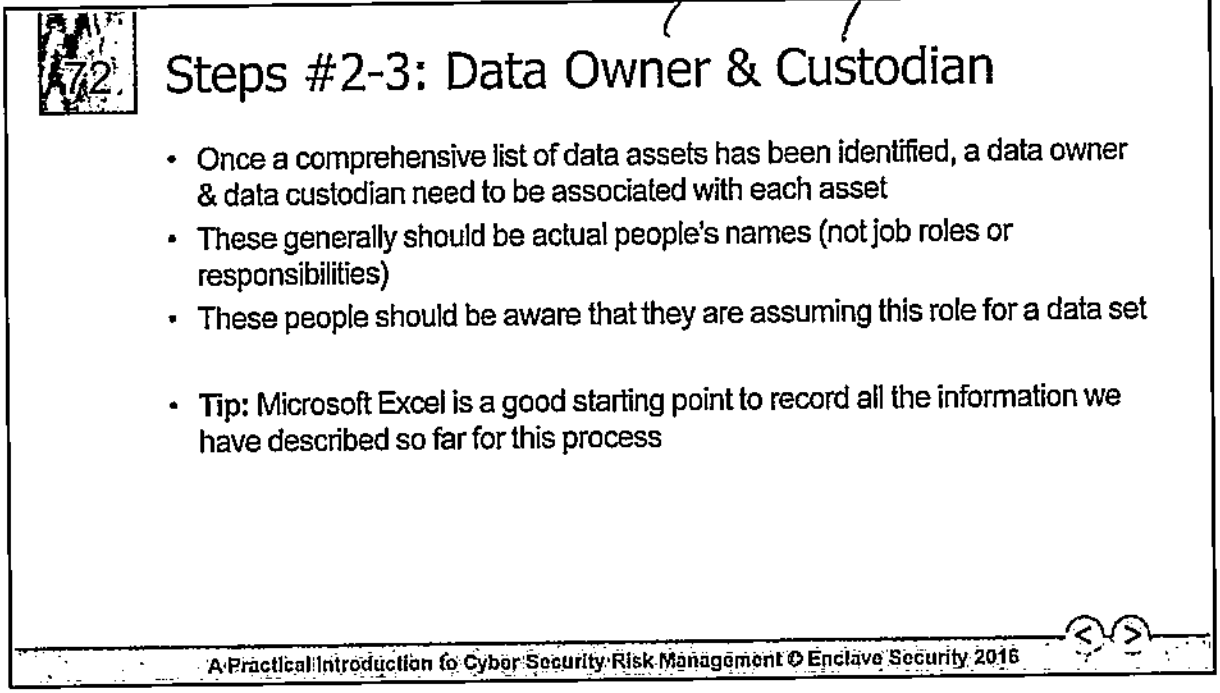
A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

Another tool that is useful for network scanning and for identifying data sets residing on a network is the ShareEnum tool from Microsoft (formerly SysInternals). This tool gives administrators the ability to identify network shares that exist on a scanned network.

Remember, part of asset identification is to identify the type of data that is being protected by a system. By identifying the data, we can then classify it and label it, public, confidential, or high confidential. If a file server is detected, often there are multiple file shares on that server which all may or may not have the same data owner or classification level. Therefore each share should be listed as a separate data asset and assigned a data owner and classification level as appropriate.

ShareEnum gives administrators the ability to discover such systems and also the ability to export the data to a format that can be understood by Microsoft Excel or a similar spreadsheet tool, and thus makes the process of documenting data assets easier.

(Manage Engine) Desktop Central
→ Dashboard, Inventory (hw + sw)



With the data collected from the previous step, we are now able to move on to the next stage in the process. Before you leave the previous step, however, consider consolidating all of your results into one spreadsheet (Microsoft Excel is great for this). At this point, we should have a spreadsheet that includes a list of all hardware assets, along with a second column that indicates which data sets exist on each of these assets – specifically network file shares and database systems. For your reference, a sample of this spreadsheet is included on the course USB.

Now it is time to add another column to our spreadsheet – two actually. One of these fields should be for the data asset's owner and the other should be for the data asset's custodian. Both of these fields should be an actual person's name. This is not the time for a job role or title to be included. This should be a person's name, and those people should know what role they are assuming for a particular data asset. The information should be kept up to data on a regular basis and be included in the change or configuration management process. So, there really is no excuse for the data to become stale, except through neglect.

73

Who Participates in a Risk Assessment?

- An organization must also decide who should participate in a risk assessment
- Groups of individuals can determine scores based on:
  - A consensus score from all participants
  - An average of all participants' scores
- Possible solutions include:
  - The data owner only
  - The data owner & data custodian
  - A group of representative stakeholders
  - The entire IS Steering Committee

A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

One decision that an organization will also need to make is the decision regarding who the appropriate stakeholders are to participate in a risk assessment. There are different approaches organizations will take, based on the goals of the assessment, issues of expediency, and more. If a group of individuals is assigned to this task, then a scoring system will have to be developed for considering everyone's input. One common approach is to obtain a consensus risk score for each element of the assessment. However this approach may prove tedious and time consuming for large groups of stakeholders. Another approach would be to have each of the participants provide a risk score and then obtain an average score from the results.

While certainly there are many ways an organization might approach this decision, there are a few common methods that are often employed. A few of the options for who should participate in a risk assessment are:

1. The data owner only
2. The data owner and data custodian
3. A group of representative stakeholders
4. The entire IS Steering Committee

Option #1: A Single Data Owner

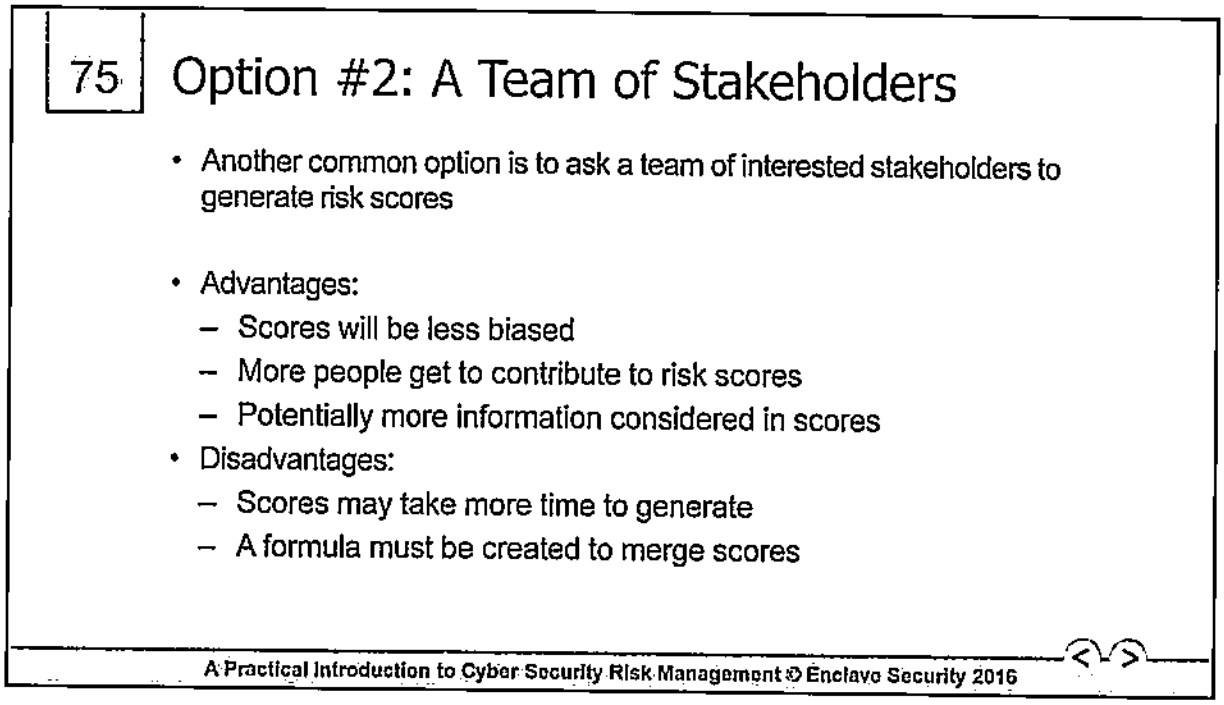
- A common option for scoring during a risk assessment is simply to ask the data owner to produce scores

- Advantages:
  - Faster score generation
  - Simpler scores are created
- Disadvantages:
  - Scores heavily influenced by one person
  - Not all information may be considered
  - Scores may be overly biased

A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

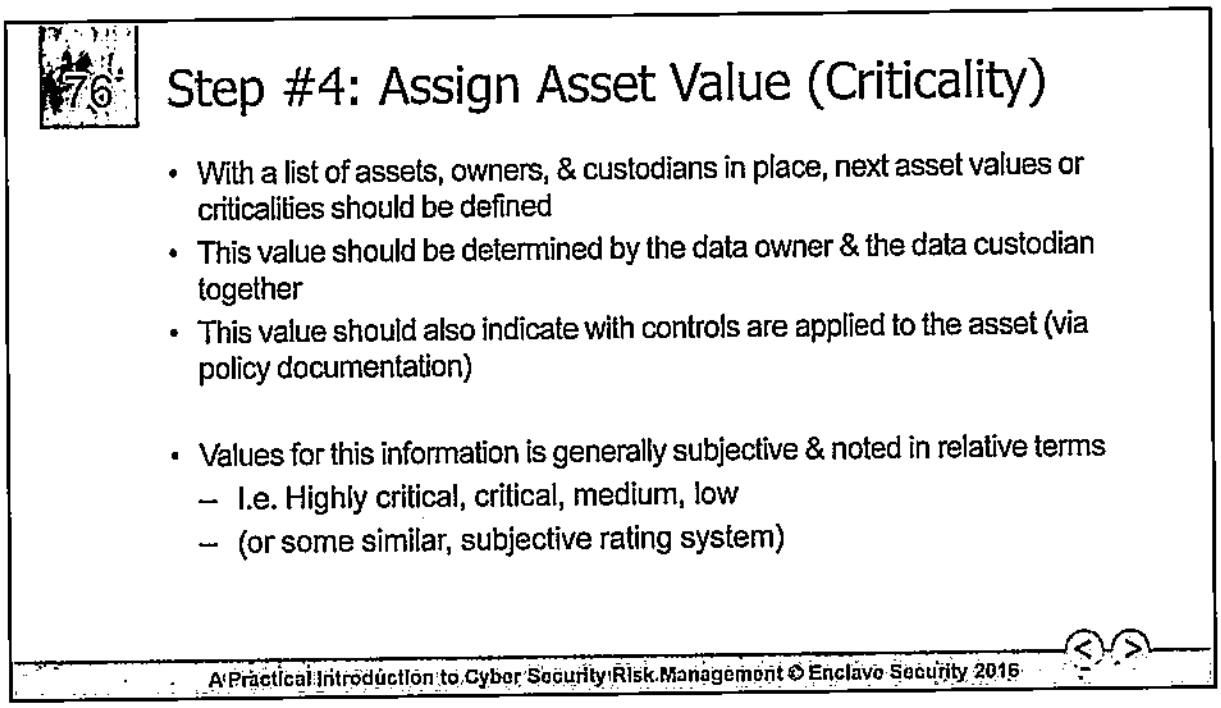
One common option when determining who should be allowed to participate in the scoring process of a risk assessment is to have the person performing the assessment simply interview the data owner(s) for the asset being assessed and to ask them to provide a risk score. Each data owner will therefore have the opportunity to provide feedback on their assets.

The primary advantages to this system are that obtaining scores are a much faster process and the scores will be much simpler as a result. However with simplicity also comes disadvantages as well. Unfortunately this process also leads to scores being heavily influenced by one person in the process. As a result not all of the information may be considered and the scores may be overly biased by the one person providing feedback. That is not to say this is a bad method of data collection, but like any method there are pros and cons to the method.



Another possible approach would be to gather a team of interested stakeholders who all have knowledge of the asset being assessed and ask them to generate risk scores as a team. As was mentioned already, this might be a consensus effort or utilize some other formula for taking everyone's feedback into consideration.

The primary advantage to this method is that the scores will be less biased than if simply one person was providing the scores. In this method more people have the opportunity to contribute to risk scores and potentially more information will be considered as a part of the data collection process. The primary disadvantage, however, is that scores will take longer to generate and more complexity is now introduced into the process. If this approach is taken a formula will also need to be created to merge everyone's scores and properly reflect such scores in the composite score that is generated.



Now that we have a list of data owners and data custodians in place, it is time to ask those people some questions. We have some qualitative risk values that we plan on asking them to define for us. Remember, they are responsible for the asset. They assume all risk for the asset; therefore they should be the ones to make these scoring decisions. In fact, both the data owners and the data custodians should coordinate the score together and collaborate on what an appropriate score should be for each asset.

Also, please do not forget our earlier discussion that the level and types of controls applied to each asset will be determined by the scores they are given by their owner during this phase.

The first score that needs to be assigned is a subjective asset value or criticality score. Ultimately the goal is for each asset to have an assigned value given to it – likely one of the following labels shown below:

- Highly Critical
- Critical
- Medium
- Low

77

Sample Criticality Model: IIA

Score	Classification Matrix	Definition
4	Highly protected	Information is considered to be very sensitive and distribution is limited to a few known people. Examples include: • Special security briefings • Strategy papers • Highly sensitive market briefings.
3	Sensitivity	Confidential material with access restricted to a level of users and known individuals. Examples include: • Position papers on specific topics. • Audit committee papers. • Results of fraud investigations.
2	Commercial-in-confidence	Information is of a general business nature and is typically produced in day-to-day business operations. Examples include: • Routine management reports. • General personnel information. • Health information. • Customers' banking details.
1	Public domain	Information suitable for wide public distribution, such as: • Information on the organization's websites. • Media releases. • Internal general staff information, including newsletters and staff information broadcasts.

A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

One criticality model that an organization might want to consider is the model promoted and published by the Institute of Internal Auditors (the IIA). Their four level classification matrix can be found at http://www.theiia.org/intAuditor/itaudit/2011-articles/data-classification/.

In their model, they define four classification levels: Highly Protected, Sensitivity, Commercial-in-Confidence, and Public Domain. A brief explanation they provide from their website for each level follows:

"**Highly Protected.** Information is considered to be very sensitive and distribution is limited to a few known people. Examples include:

- Special security briefings
- Strategy papers
- Highly sensitive market briefings."

"**Sensitivity.** Confidential material with access restricted to a level of users and known individuals. Examples include:

- Position papers on specific topics.
- Audit committee papers.
- Results of fraud investigations."

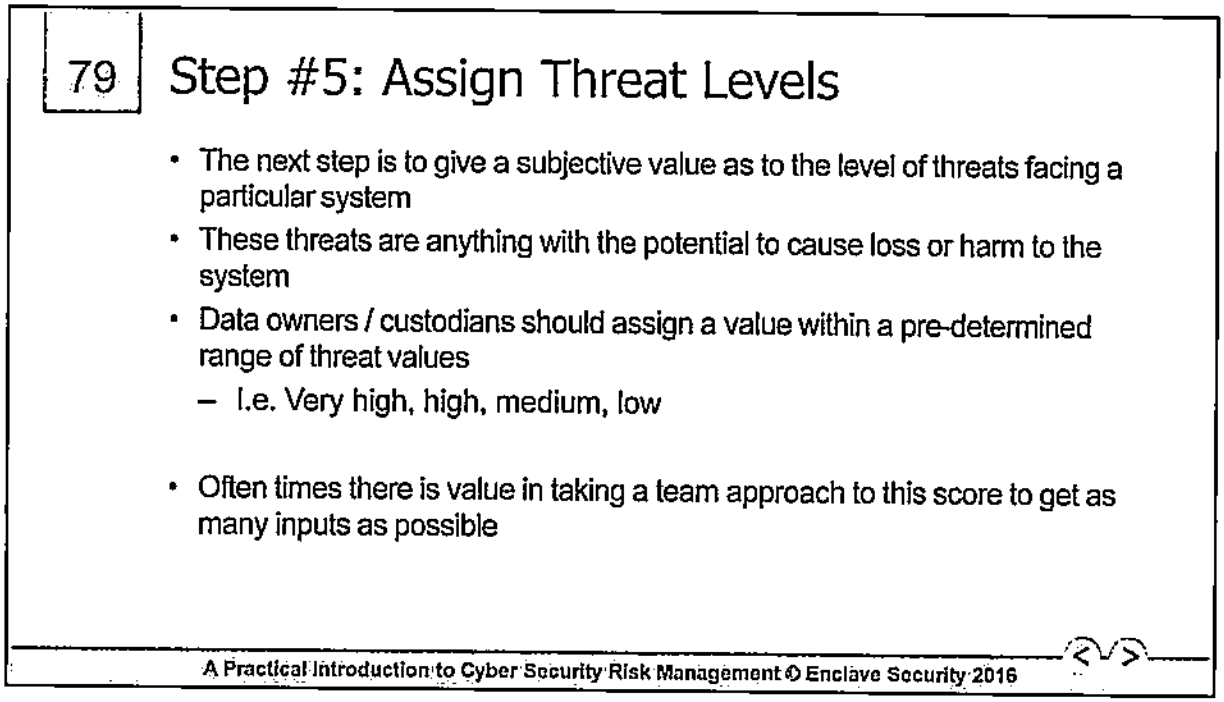
"**Commercial-in-Confidence.** Information is of a general business nature and is typically produced in day-to-day business operations. Examples include:

- Routine management reports.
- General personnel information.

- Health information.
- Customers' banking details."

"**Public Domain.** Information suitable for wide public distribution, such as:

- Information on the organization's websites.
- Media releases.
- Internal general staff information, including newsletters and staff information broadcasts."



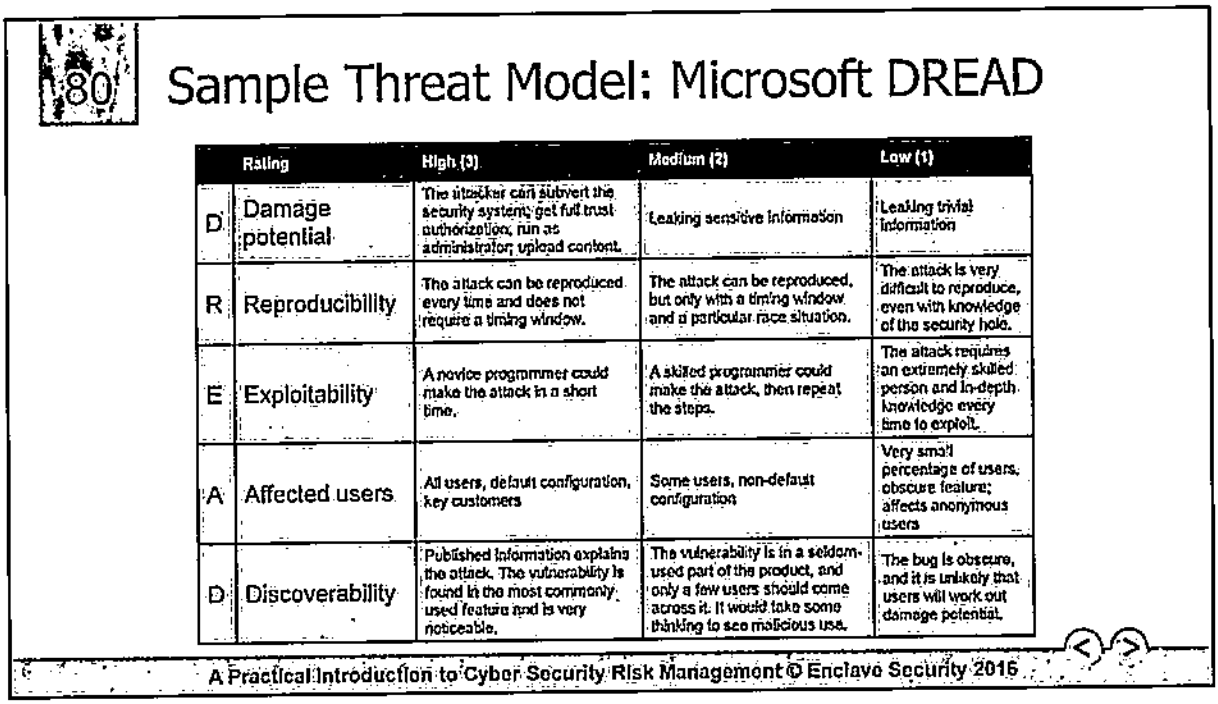
Another thing to consider when performing a risk assessment is the various threats that face the existing system. Organizations should use this opportunity to answer the question, "What are the potential threats to the system?" This process is not always clear and concise, and it will often require the assessor to be creative in his or her approach to the problem. One of the best ways to approach this issue is to look at the information asset and determine where all of the possible system failures could lie. Ask the questions:

1) What could go wrong with this system, and
2) If something did go wrong, what would cause this particular failure?

Brainstorming this process with others or system administrators is a good opportunity to generate a comprehensive list of threats which face the system. Once the list is generated, the likelihood of each of the threats occurring must be recorded as part of the risk assessment.

In this step, a subjective value should be assigned as the threat value facing a particular system. Again, at this point in the process we will use subjective values to define the level of threat – possibly using values such as Very high, High, Medium, and Low.

It may also make sense to approach this process from a team point of view. Have everyone on the team give a threat rating for a particular system, and then create an average score as a result of the collective ratings given by the group, and use that as the relative threat level for the system.



Microsoft provides a sample threat model that organizations may want to consider as a template as they develop their own model for scoring threats to assets. Their DREAD model defines potential threats to an asset and provides an explanation for the score that would be applied to each asset. DREAD represents the following threat areas:

D – Damage potential
R – Reproducibility
E – Exploitability
A – Affected Users
D - Discoverability

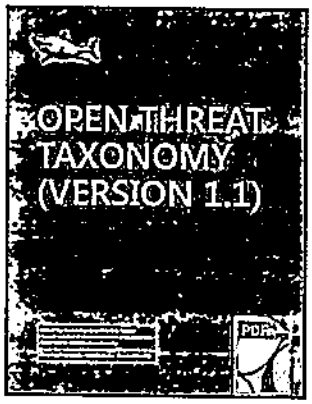
The risk assessment team would therefore score each of these threat classification areas on a scale of 1 to 3 and then combine the threat scores from each of the five areas.

A full explanation of their model can be found at: http://msdn.microsoft.com/en-us/library/ff648644.aspx.

81

Sample Threat Model: Open Threat Taxonomy

- Maintained by Enclave Security and distributed by the Center for Internet Security
- Hundreds of organizations have contributed
- One of the latest efforts is the release of a community threat model, the Open Threat Taxonomy (v1.1), which will be used to document and prioritize threats
- OTT will be used to define threats to define controls
- Will help standardize risk assessments, make one less paperwork step for organizations to complete

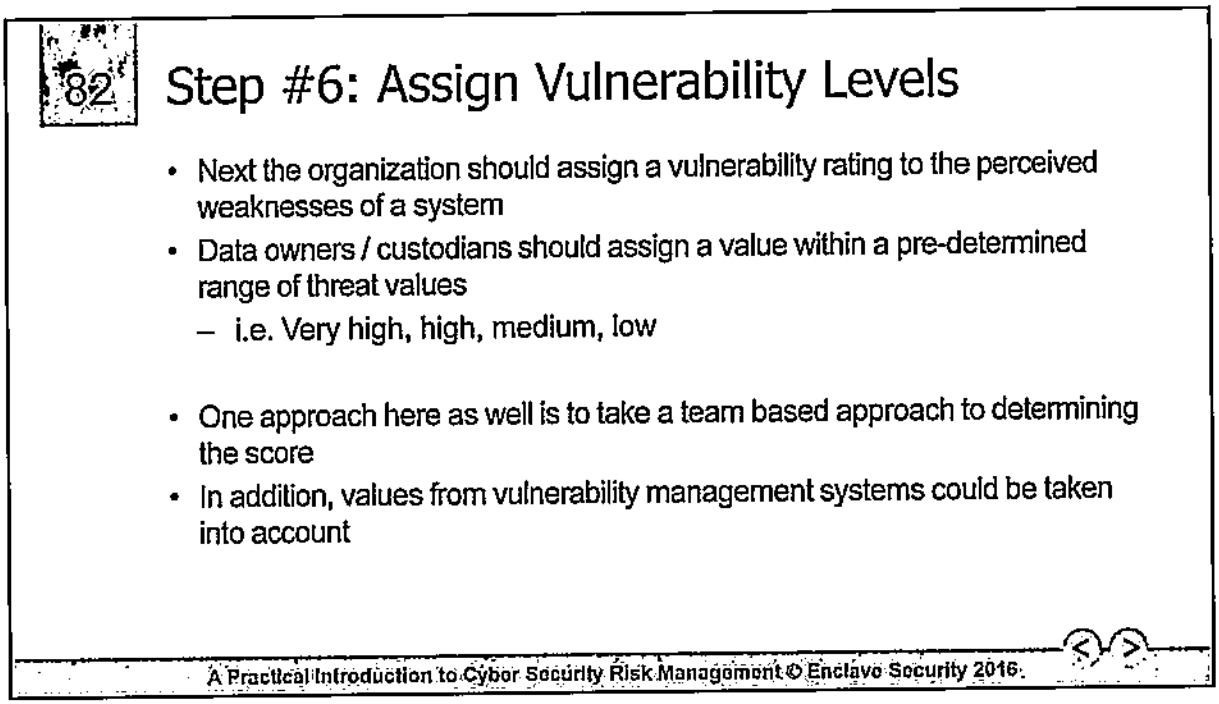


AUDITSCRIPTS

Another threat model to consider is the Open Threat Taxonomy (OTT) which is maintained by James Tarala and Kelli K. Tarala of Enclave Security and distributed by groups such as the Center for Internet Security. This model was designed to be a threat taxonomy in the spirit of MITRE's CAPECs which could identify and catalog all potential threats to an organization's information or information systems. Over 150 different international organizations contribute to this ongoing effort and new versions are being released all the time.

The goal of this project is to catalog all potential threats in this area as a precursor to control selection. When an organization understands the threats facing it, they can better determine which controls can be used to defend against such threats. The model focuses on threat actions, but does not try to focus on all threat sources or actors – which does not provide as much useful intelligence for the purpose of control selection. The model is designed to be a community effort that will save organizations the effort of having to catalog this information themselves. It is also presently being used as an input to the Critical Security Controls project which is often viewed as a community risk assessment methodology.

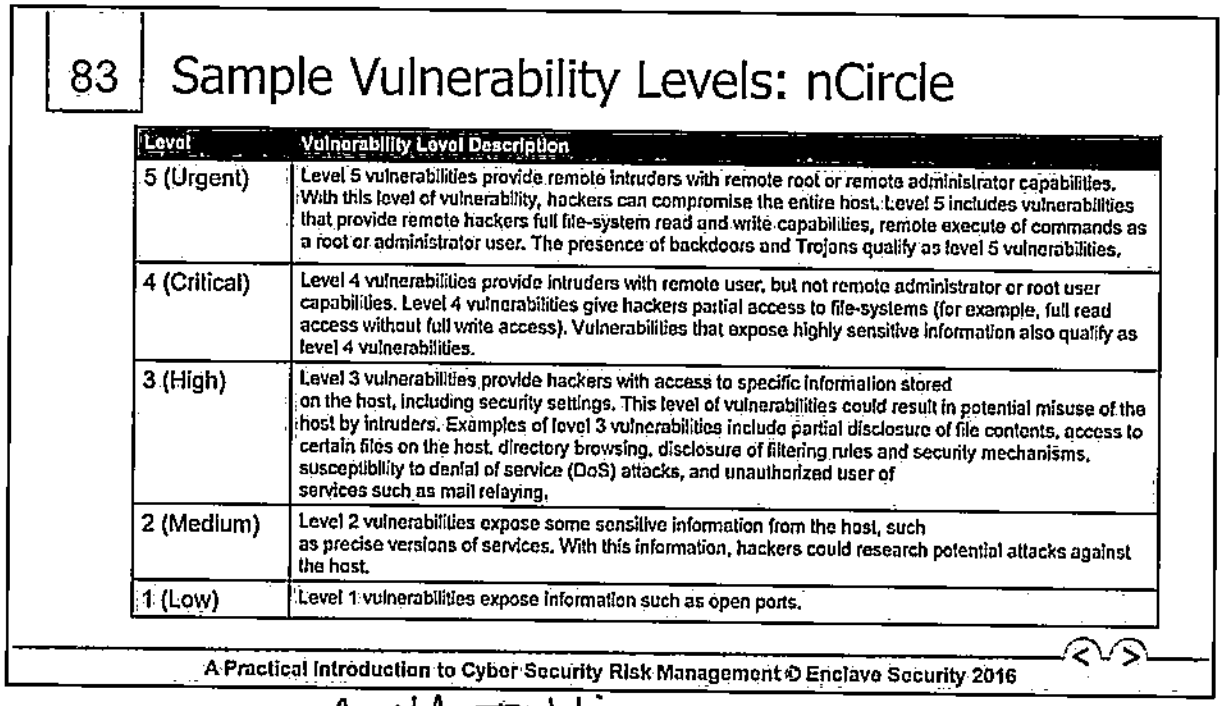
THREAT: danger
VULNERABILITY: weakness subject to threat



Once a threat assessment has been performed, the next step is to perform a vulnerability assessment on the system being evaluated. In this stage rather than performing a more academic, creative assessment of all possible threats, the goal is to determine any actual vulnerabilities that exist on the system. Normally this assessment will be a part of a larger vulnerability assessment program and the data will be fed from the vulnerability assessment program into the risk assessment program. However, both operational and technical vulnerability assessment results will prove valuable during this process.

Each vulnerability should be assigned an impact value during this process as well. This is important, as some vulnerabilities will have a different effect than others. While one vulnerability may simply disclose information about the system to an attacker, another may lead to an entire system compromise. The severity of the vulnerability should definitely be considered during this process. Not only should you consider technical vulnerabilities though, but procedural vulnerabilities as well.

At this point it should go without saying, but before performing this type of assessment (especially if technical tools are involved), make sure that you have explicit permission in writing from system owners! In the next section we will discuss more specifics regarding how to perform this type of assessment.



bought by TripWire

One sample set of vulnerability levels that an organization may want to consider, is the list of vulnerability levels defined by nCircle, the vulnerability management software vendor. They define a five level classification system, which defines vulnerabilities as being Urgent, Critical, High, Medium, or Low.

At the following website, a full description of these levels can be found as described below:
http://www.ncircle.com/htmldatasheets/Vulnerability_Scoring_System/Vulnerabilit-and-Risk-Analysis_pg2.html

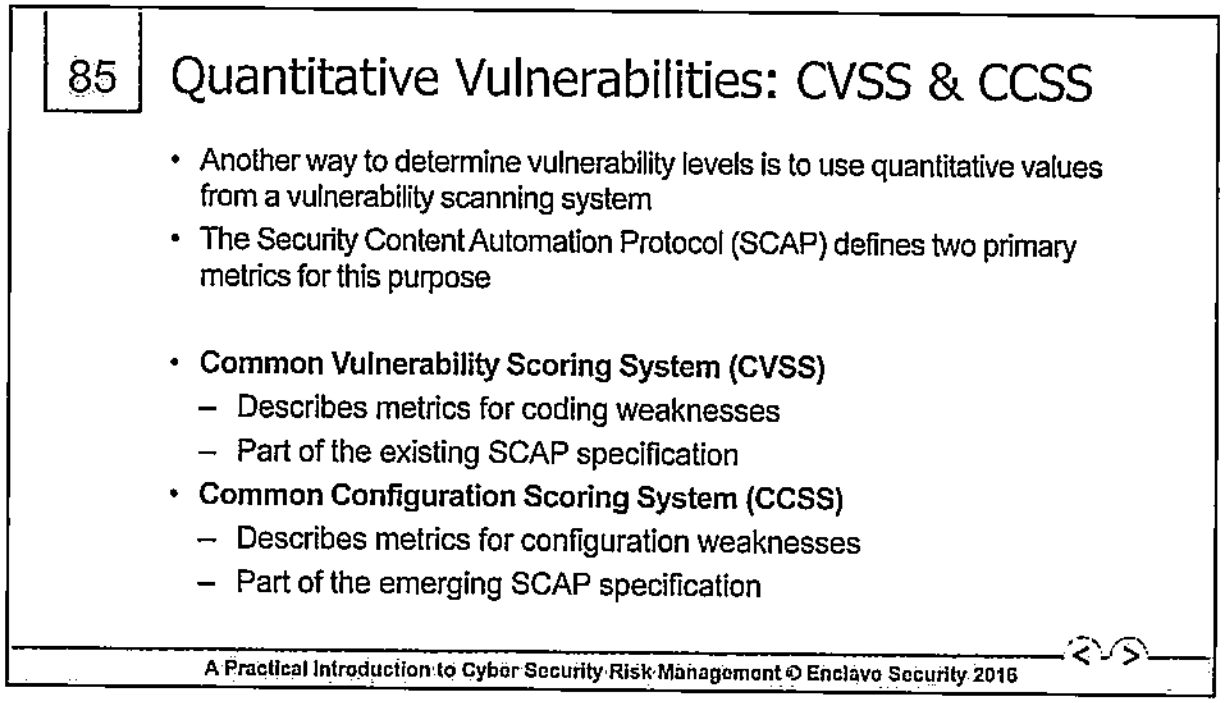
"Level 5 (Urgent): Level 5 vulnerabilities provide remote intruders with remote root or remote administrator capabilities. With this level of vulnerability, hackers can compromise the entire host. Level 5 includes vulnerabilities that provide remote hackers full file-system read and write capabilities, remote execute of commands as a root or administrator user. The presence of backdoors and Trojans qualify as level 5 vulnerabilities."

"Level 4 (Critical): Level 4 vulnerabilities provide intruders with remote user, but not remote administrator or root user capabilities. Level 4 vulnerabilities give hackers partial access to file-systems (for example, full read access without full write access). Vulnerabilities that expose highly sensitive information also qualify as level 4 vulnerabilities."

"Level 3 (High): Level 3 vulnerabilities provide hackers with access to specific information stored on the host, including security settings. This level of vulnerabilities could result in potential misuse of the host by intruders. Examples of level 3 vulnerabilities include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, susceptibility to denial of service (DoS) attacks, and unauthorized user of services such as mail relaying."

"Level 2 (Medium): Level 2 vulnerabilities expose some sensitive information from the host, such as precise versions of services. With this information, hackers could research potential attacks against the host."

"Level 1 (Low): Level 1 vulnerabilities expose information such as open ports."



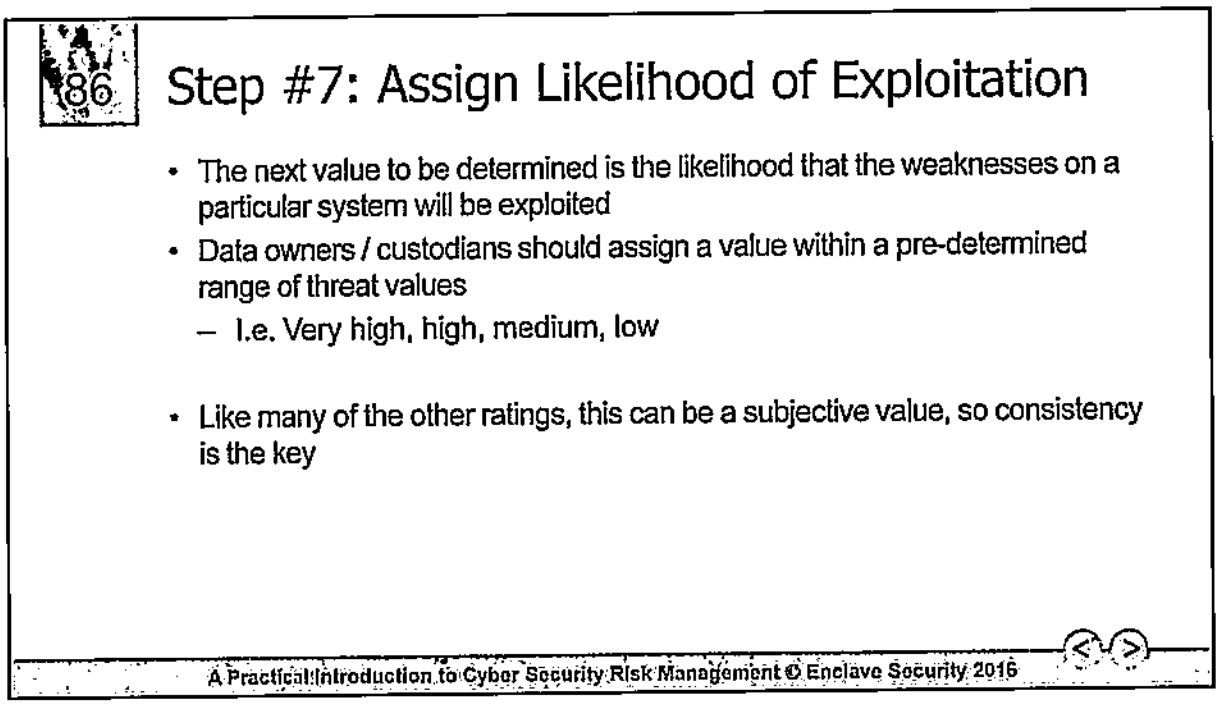
Another, more quantitative approach to vulnerability scoring, is the NIST approach to vulnerability scoring that is defined by the Security Content Automation Protocol (SCAP). Specifically SCAP defines two primary scoring systems for vulnerabilities:

Common Vulnerability Scoring System (CVSS). This scoring system describes metrics for coding weaknesses and is a part of the existing SCAP specification.

Common Configuration Scoring System (CCSS). This scoring system describes metrics for configuration weaknesses and is a part of the emerging SCAP specification.

Many vulnerability assessment / management systems rely on the scores provided by vendors, NIST, or US-CERT in the form of CVSS or CCSS ratings to determine the vulnerability levels associated with a specific asset. Unfortunately at this time not every vulnerability is given an official CVSS or CCSS rating that is universally accepted and often times vulnerability assessment vendors or organizations are left to define their own ratings. Regardless, this is still a viable scoring system that one can only hope will mature over time.

For more information regarding the Security Automation Protocol (SCAP), please consult the NIST website: http://scap.nist.gov/

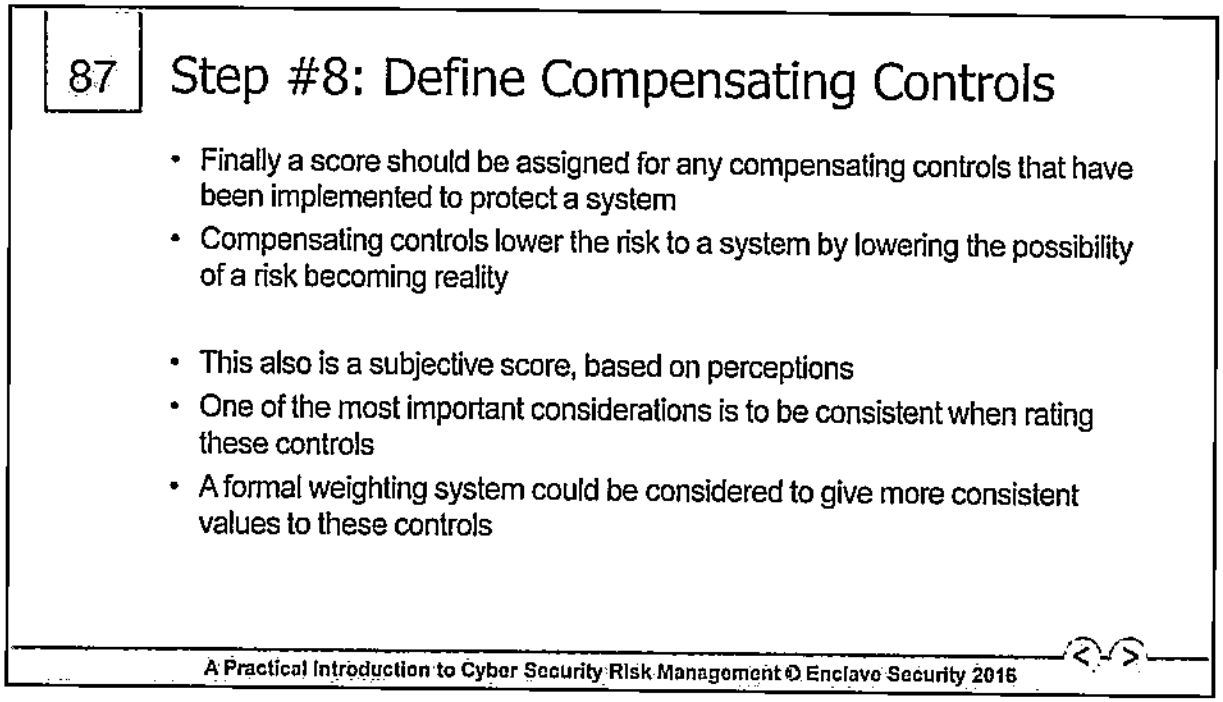


The next value that has to be added into our equation is a score, which indicates the likelihood of a particular weakness on a system will be exploited. Again, this will be a subjective rating, based on the input from data owners and custodians.

For this value, data owners and custodians should assign a value within a pre-determined range of threat values. This score will be based on the opinions of those parties when scoring their system and likely will use a scale of something such as:

- Very High
- High
- Medium
- Low

It should be remembered too with all of these scores, that these are subjective scores, and high degrees of varied subjectivity can skew our results. Therefore, groups should endeavor to be as consistent as possible during this process of defining values.



Compensating controls can be a tricky part of risk assessments. They can either be a legitimate fix to a vulnerability or they can be a short-term workaround. Sometimes a short risk assessment may need to be completed when evaluating a compensating control itself. Compensating controls should be documented along with a legitimate technological reason or business reason why a compensating control was needed.

Once the organization has defined a need for compensating controls, then they must be scored as part of the risk assessment. This last score that will be assigned indicates the type of compensating controls that have been implemented in order to protect the system. Ideally this score would reflect actual controls with dedicated objectively assigned values. Try not to be too ambitious when starting out. To start, simply assign a subjective value to what you think the quality of compensating controls are that have been implemented to protect the system. The hope is that these compensating controls should lower the overall risk level of the system by lowering the possibility of a risk becoming a reality.

Again, remember this will be a subjective control, and, therefore, it is imperative that there is consistency in the scoring methods used. Ideally a formal or more objective system could be used, but that should wait until we reach the more formal risk assessment models later today.

Sample Compensating Control Levels

Control Type	Control Level	Control Score
Preventive	High	3
	Medium	2
	Low	1
Detective	High	3
	Medium	2
	Low	1
Corrective	High	3
	Medium	2
	Low	1

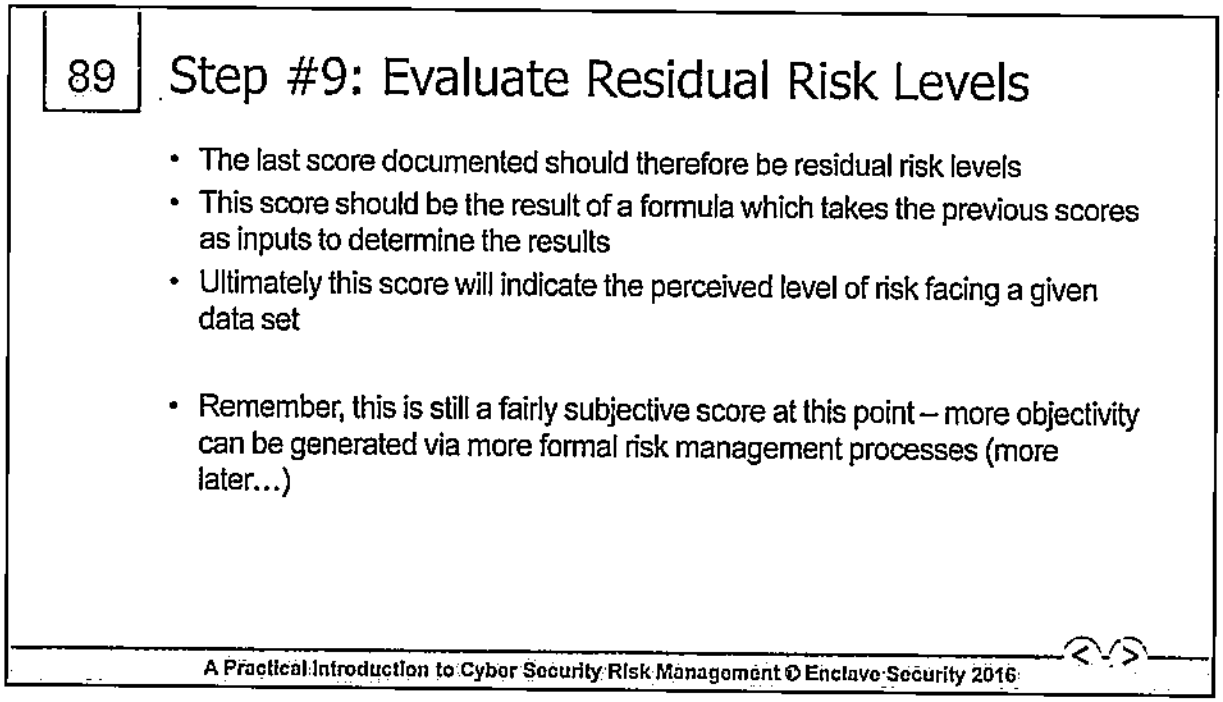
Preventive Score + Detective Score + Corrective Score = Comprehensive Score

When defining compensating control levels, an organization must define how they will score the compensating controls that they are evaluating. A sample set of compensating control levels might be to define the presence of preventive, detective, or corrective controls and then to assign a control level to each as seen in the above graphic. Then the score from each of these levels could be combined to form a simple composite score.

Ideally this process would utilize a list of specific compensating controls and provide a score for each asset as to whether or not a compensating control has been implemented for the asset. However this becomes a much longer effort of determining an appropriate list of controls, their priority levels, and their applicability to a particular type of asset. Most often commercial Governance, Risk, and Compliance (GRC) software tools are used by organizations for this purpose.

Preventive, detective, and corrective controls are the most common categories used to define controls, but other another less common category of controls is deterrent controls. These are controls that discourage a threat from acting upon a vulnerability. An example of a deterring control is the United States' Cyber Strategy that emphasizes the possibility of offensive cyber activities. [1]

[1] http://infosecisland.com/blogview/22534-Offensive-Cyber-Capabilities-Need-to-be-Built-and-Exposed-Because-of-Deterrence.html



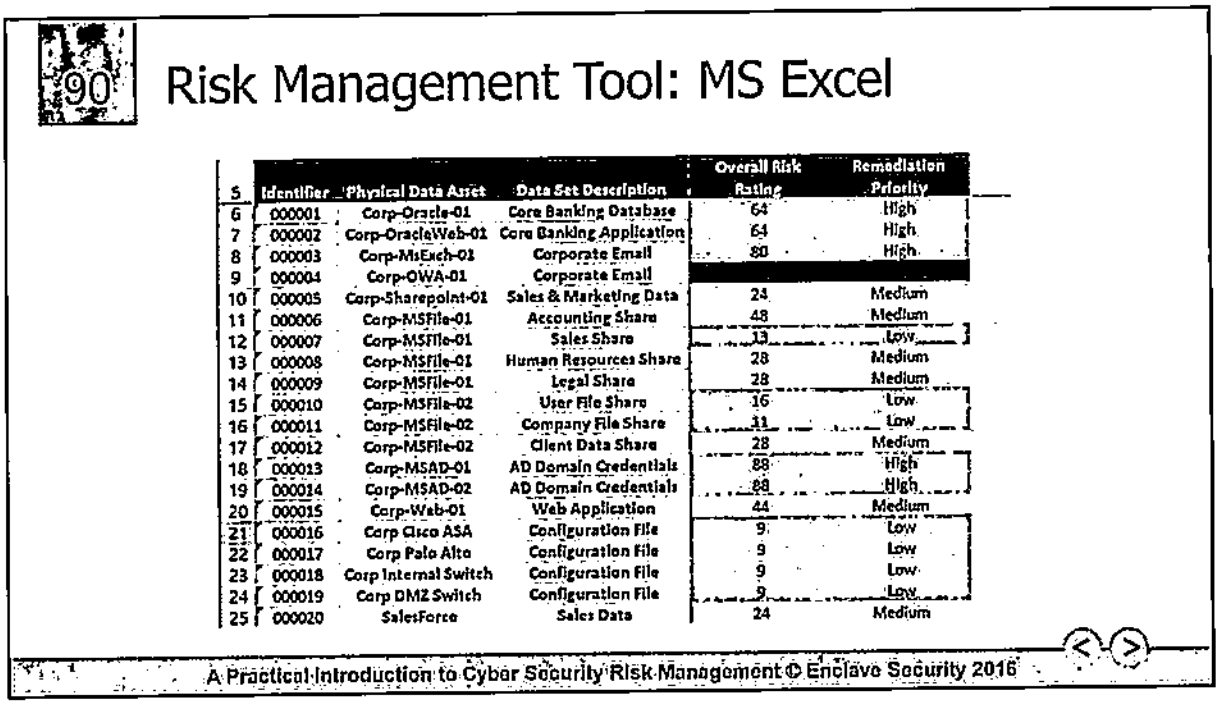
The last value we will include is the residual risk level to the system. This is not so much a defined score as it is the result of a calculation performed against the previous values that have been inputted.

Having discussed each of the parts, it is now time to consider how we address each of these elements together in order to form a comprehensive formula for determining risk. A generally accepted formula for evaluating risk is:

Threat x Vulnerability x Likelihood > Risk

Or said another way, threats to a system, plus vulnerabilities to a system, combined with the potential impact to the system, yields the overall risk to the system. All three of these factors must be considered individually in order to come up with a comprehensive picture of the risk to a system. It should also be considered that if there is no threat, no vulnerability, or no potential impact to a system, then there is no risk to that system either. All three elements must be present in order for there to be an element of risk.

It is also important to recognize that this formula should be considered a generic framework for understanding risk, not necessarily for creating qualitative or quantitative measurements for evaluating risk within an organization. Instead, we will address specific methodologies for quantifying and measuring risk a little later.

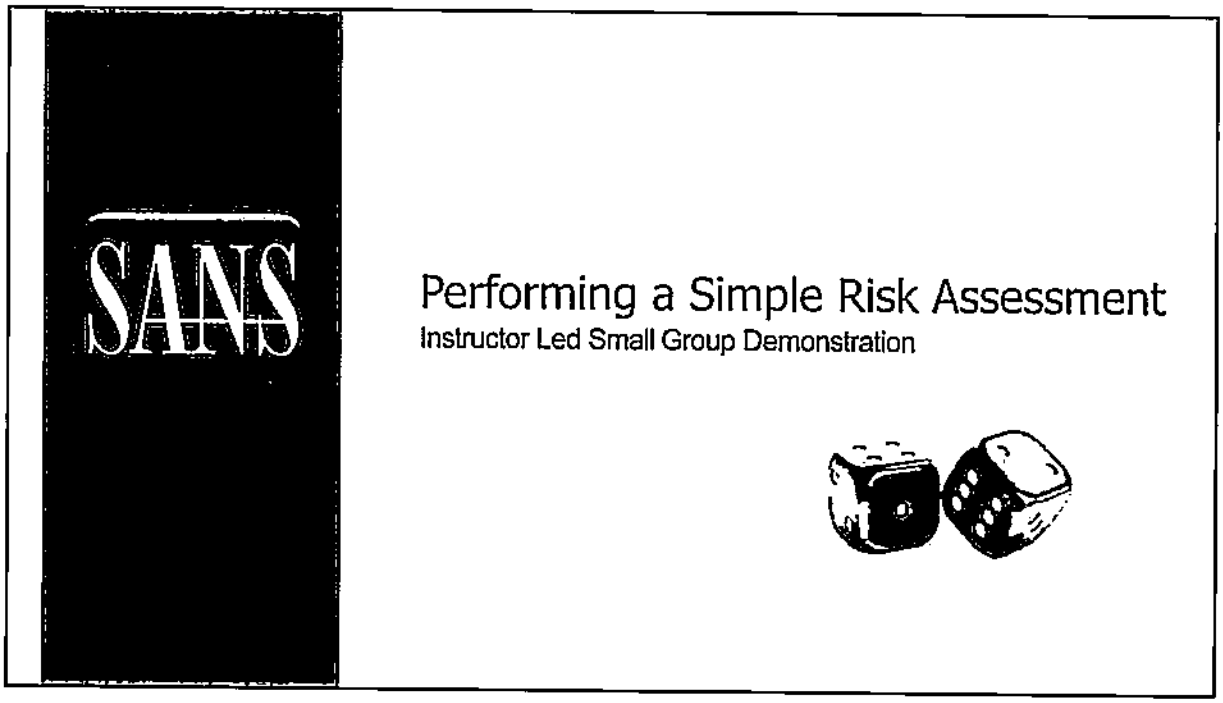


	Identifier	Physical Data Asset	Data Set Description	Overall Risk Rating	Remediation Priority
6	000001	Corp-Oracle-01	Core Banking Database	64	High
7	000002	Corp-OracleWeb-01	Core Banking Application	64	High
8	000003	Corp-MsExch-01	Corporate Email	80	High
9	000004	Corp-OWA-01	Corporate Email		
10	000005	Corp-Sharepoint-01	Sales & Marketing Data	24	Medium
11	000006	Corp-MSFile-01	Accounting Share	48	Medium
12	000007	Corp-MSFile-01	Sales Share	13	Low
13	000008	Corp-MSFile-01	Human Resources Share	28	Medium
14	000009	Corp-MSFile-01	Legal Share	28	Medium
15	000010	Corp-MSFile-02	User File Share	16	Low
16	000011	Corp-MSFile-02	Company File Share	11	Low
17	000012	Corp-MSFile-02	Client Data Share	28	Medium
18	000013	Corp-MSAD-01	AD Domain Credentials	88	High
19	000014	Corp-MSAD-02	AD Domain Credentials	88	High
20	000015	Corp-Web-01	Web Application	44	Medium
21	000016	Corp Cisco ASA	Configuration File	9	Low
22	000017	Corp Palo Alto	Configuration File	9	Low
23	000018	Corp Internal Switch	Configuration File	9	Low
24	000019	Corp DMZ Switch	Configuration File	9	Low
25	000020	SalesForce	Sales Data	24	Medium

One simple tool for analyzing the data sets gathered during this process is a tool such as Microsoft Excel. The benefit of using a tool such as this is that it gives a team the ability to quickly gather data from the systems being analyzed and the ability to enter in formulas for comparing the risk levels discovered on such assets. These formulas do not need to be complex, yet at the same time they can compare risk ratings from multiple assets.

The goals of such a tool are to give the team performing the assessment the ability to compare risk scores for multiple assets simply, prioritize risk remediation efforts, and give teams the ability to visualize the effects of remediation efforts.

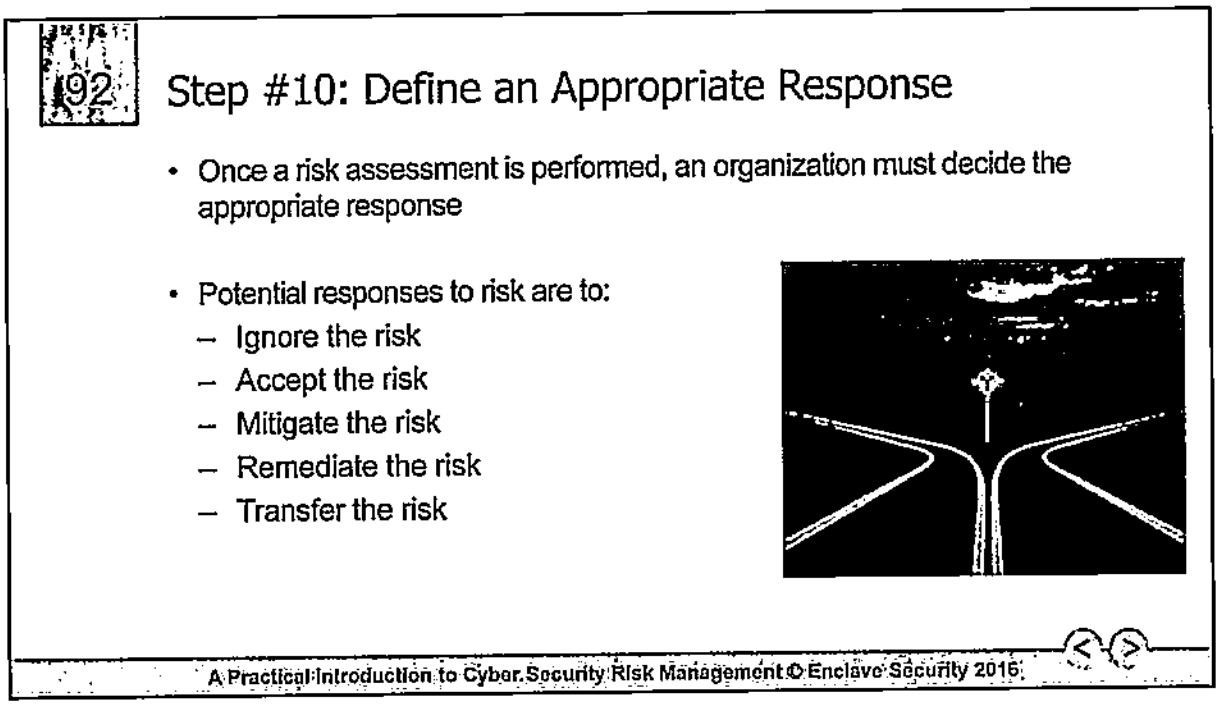
A sample Microsoft Excel spreadsheet has been included with the course USB and can be used by students who want a simple way to start this process.



Now it's time to put what we've learned into practice. The purpose of the lab activities that we are engaging in during this class is to give the student an opportunity to put into practice what we have been learning about from the instructor. The hope is that by working through the exercises in this lab that you will be better prepared to take this information back to your company in order to put it into practice.

Some of these lab exercises specifically call on students to work as teams. Even if the lab specifically does not call for you to work as a team, in a conference setting you will likely get the most from this activity if you do work as a group with friendly students sitting around you. Not only will you be networking and building relationships with smart students sitting around you, but you will also be able to benefit from their ideas and experiences as well. Every student brings a wealth of information to the class, and participating as a group is one of the better ways to be able to take advantage of those experiences.

At this point, it's time to turn to the section of the book where this lab is described in more detail. Listen to the specific instructions given by your instructor and follow the instructions in the lab exercises step by step. If you have any technical challenges or questions, don't hesitate to ask, the instructor and/or teaching assistants are here to help.

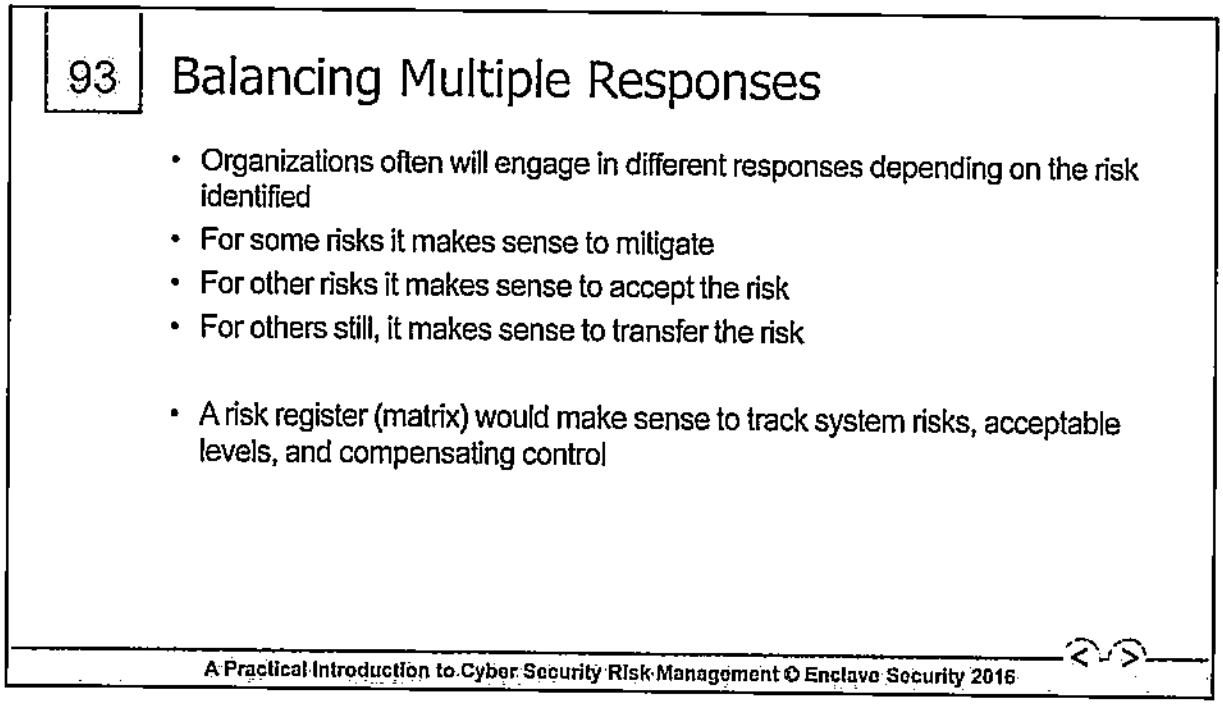


Assuming that we now have a solid understanding of the various components to risk and we now understand a formula for potentially calculating risks to an organization's information assets, what choices do an organization have when it comes to responding to risks that are discovered in the risk management process?

There are five primary choices an organization has when determining how to respond to risk. The choices are to:

- Ignore the risk
- Accept the risk
- Mitigate the risk
- Remediate the risk
- Transfer the risk

Depending on the risk being considered, organizations will have to determine how to proceed once a risk has been discovered. Ultimately though, this is a business decision that should be addressed by executives, auditors, and business owners. In any case, a conscious decision should be made in this regard, and ignoring the risk should never be considered a proper response in this scenario!

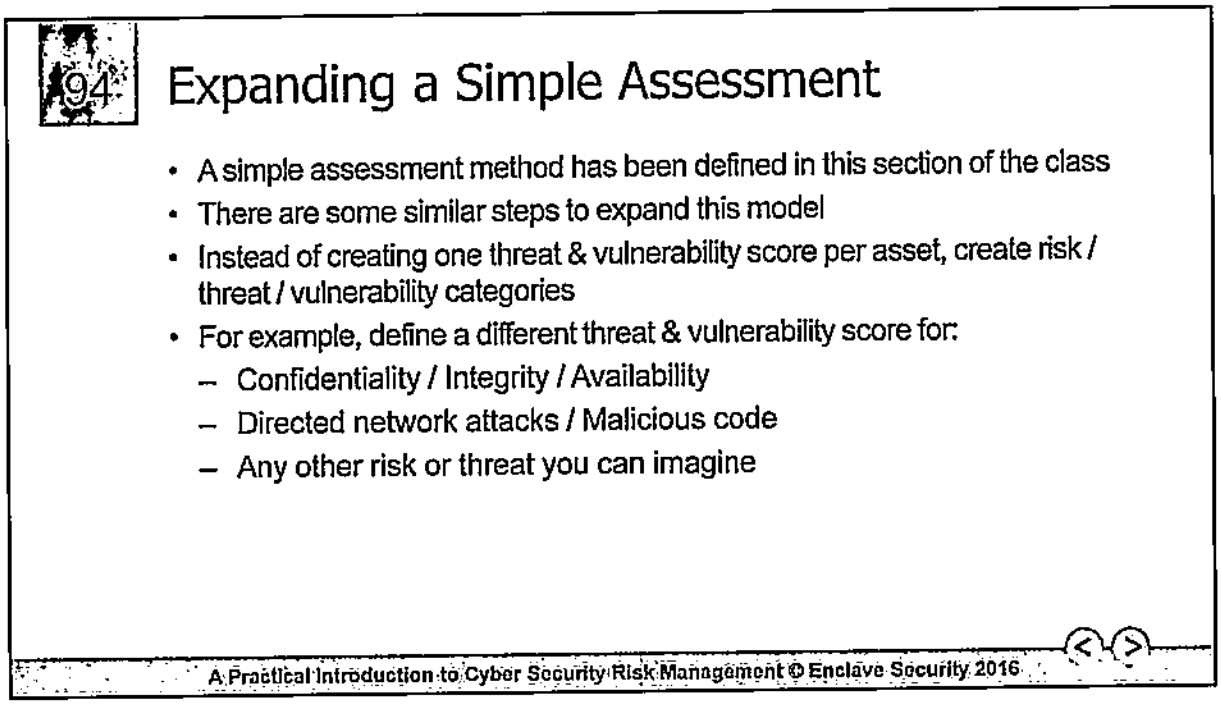


Depending on the risk that is identified, organizations may often times choose different responses to the risks.

In some cases it might make the most sense to mitigate a discovered risk. In other cases it might make the most sense to accept the risk (and of course document that risk acceptance). In other cases it might make the most sense to transfer the risk.

One way or another, organizations need to make appropriate decisions on the risks they have identified in accordance with available resources, compliance requirements, overall business goals, and more. But each risk may be responded to differently by the organization, and that is a normal and healthy response.

One recommendation would be to develop a risk register, which tracks the risks an organization has identified and matches them with acceptable risk levels and compensating controls. This way at a glance it is easy for executives, auditors, and data owners to see their systems, the risks facing them, and which systems are accepting levels of risk that are higher than acceptable. This then can help organizations determine where resources are best utilized when it comes to implementing controls.

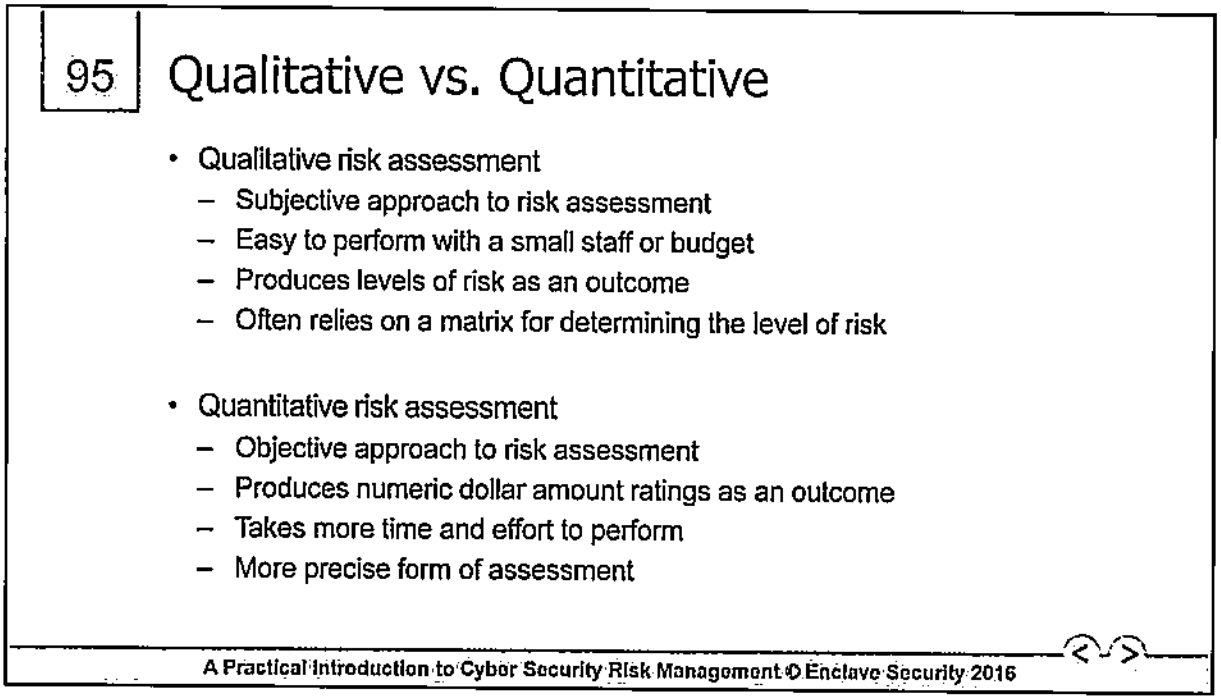


If this simple method of risk assessment is appealing to your organization, you might want to consider a few tweaks to this model as a way to get slightly more value from it and to make it easier to identify the types of controls that will be the most useful and comprehensively lower risk in the organization.

For example, one way an organization might expand this model is by creating multiple threat and vulnerability scores. In the original model that we described above we told you to define one score for vulnerabilities to the system and one score for risk. The next step in a more detailed analysis may be to create categories for each of the risk, threat, or vulnerability categories.

One specific way might be to assign a threat and a vulnerability score as a rollup of three scores; one based on confidentiality, one based on integrity, and one based on availability. Define threats and vulnerabilities for each of those areas, and then average the three scores for each and determine an aggregate threat and vulnerability score. Then consider compensating control values that match. This way as you implement a control to limit availability vulnerabilities to a system, it lowers the vulnerability score for availability, which lowers the overall vulnerability score, which impacts the risk as a whole.

Instead of using those categories, possibly consider specific issues such as directed network attacks, malicious code, or any other risk or threat you can imagine and input scores based on those issues. This will allow you a more granular approach to assessing risk metrics.



In order to implement the formula for risk indicated earlier, there are multiple frameworks and methodologies that have been developed to help organizations put some type of quantitative value or measurement to the level of risk assumed by an organization. These risk assessment frameworks in general fall into two major categories – qualitative and quantitative risk assessment methodologies.

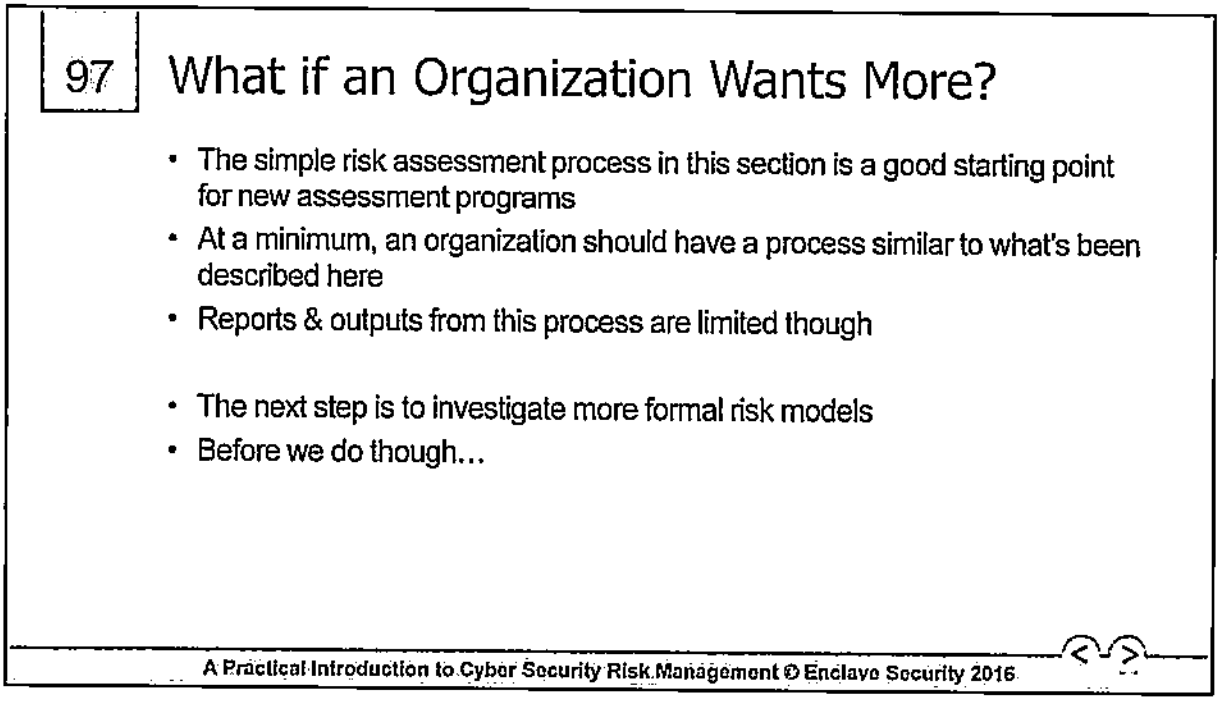
The first that we will consider in this course is the qualitative methodology. Of the two general methods, the qualitative approach is the more subjective. This is also the easier of the two methods to perform, especially for organizations with a smaller team or budget.

Rather than producing a numeric value for risk (as a quantitative approach to risk assessment would), a qualitative assessment produces a level or general category of risk as its outcome. This approach most often relies upon a matrix for determining the level of risk associated with a given information asset, and this level of risk can be used to help determine which systems are at the highest level of risk and thus addressed first.

The other methodology that could be used to assess the level of risk associated with a given information asset is the quantitative risk analysis methodology. Similar to the qualitative method of assessment in that the end product is a degree or level of risk, the major difference is with the specific output generated by this type of assessment.

Unlike the qualitative approach, the quantitative methodology utilizes a more objective approach to risk assessment. Instead of producing a general level of risk, such as high, medium, or low, this methodology actually produces a numeric dollar amount rating as the outcome for the assessment. As can be imagined, this approach to risk assessment takes more time and effort to conduct and will consume additional resources as you attempt to determine accurate numbers for the assessment.

In light of the fact that this method produces a specific dollar amount, it tends to be a more precise form of assessment and can indicate to an organization even minor differences in the associated risks between two systems, depending on how the assessment is performed.



After going through this process of performing a simple risk assessment, many organizations will likely walk away with the nagging feeling that they should be doing more to measure risk in their organizations. There will likely be a feeling that a more quantitative or metrics-based approach to risk should be taken – and there certainly is value in that determination. So what is an organization to do?

The first step should be to work through the process that we defined in this section. This simple assessment methodology will give the organization a baseline to start from as they perform more complicated assessments. By way of reminder, the process we defined here is:

1. Perform an asset inventory
2. Assign a data owner to each asset
3. Assign a data custodian to each asset
4. Assign value to each asset (criticality)
5. Determine the level of threat facing each system
6. Determine the level of vulnerability inherent in each system
7. Determine the likelihood of threats exploiting vulnerabilities
8. Document implemented compensating controls
9. Establish levels of residual risk
10. Make a business decision regarding each residual risk

The next step is to evaluate more formal risk models and tools to see if any of these tools provide automation to an organization in their assessments. But as with any other technology tool, these tools are only useful if they can be clearly linked to overall business goals (which after our discussion on the value of GRC, it is easy to identify).

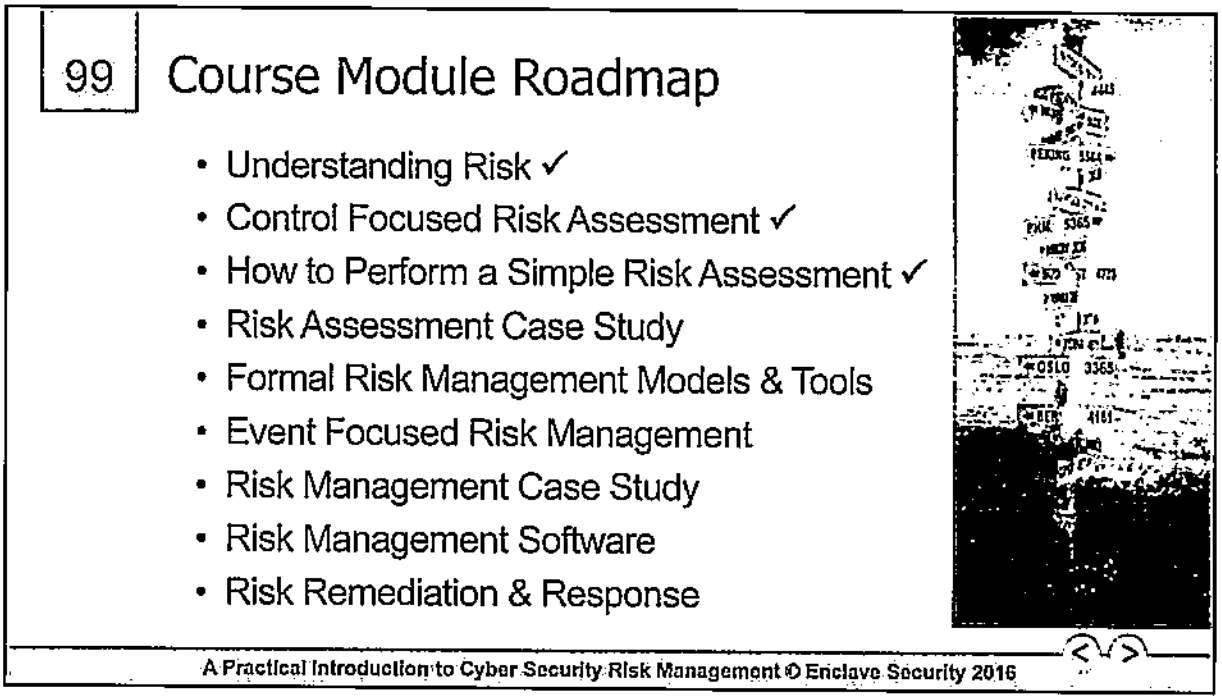
However, before we move on to more complicated methods, it is time to try a simple assessment ourselves to get a better feel for how it works.

SANS

Risk Assessment Case Study

An Instructor Led Case Study

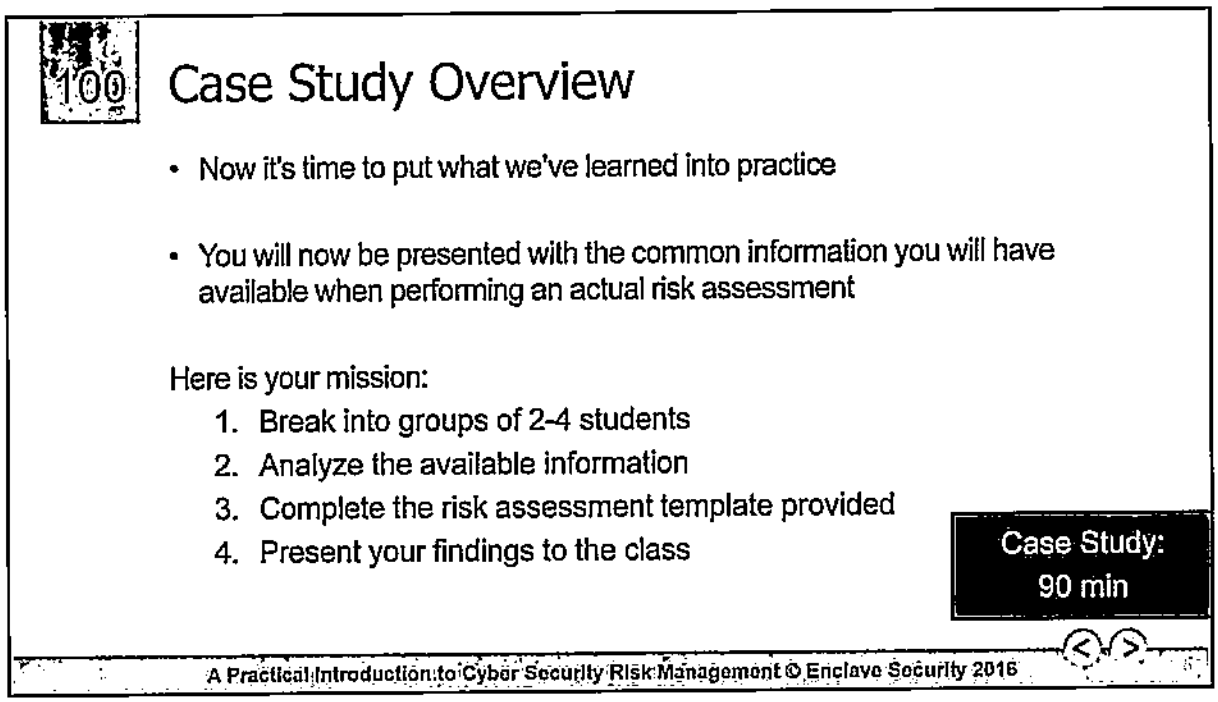
This page intentionally left blank.



In this course we will explore the concept of risk and its practical impact on an organization. Ultimately the goal of this course is to prepare students to effectively utilize risk assessment as a tool for enterprise defense. Too many times organizations think of risk assessment and risk management as academic tools with little to no practical application. These concepts are often viewed as a formal task to pursue when an organization has free time rather than as a core business activity that drives other enterprise security efforts. In today's course students will have the opportunity to learn about the proper place of risk assessment and risk management in an enterprise. They will also be given practical skills for how to perform a risk assessment on a step by step basis, from data collection to the point of presenting their findings to business leaders. Students with a desire to perform more in depth analysis will also be given tools and formal models to consider to empower them to create a long term / formal risk management program.

Specifically today we will cover the following subjects:

- Understanding Risk
- Control Focused Risk Assessment
- How to Perform a Simple Risk Assessment
- Risk Assessment Case Study
- Formal Risk Management Models & Tools
- Event Focused Risk Management
- Risk Management Case Study
- Risk Management Software
- Risk Remediation & Response



Ok, now it is your turn!

It is time to put into practice what we have just learned in the previous sections of the course. You will now be presented with the common information you will have available when performing an actual risk assessment. Detailed instructions for this section can be found in the lab materials at the end of today's material. However the basic breakdown of the lab activities are:

1. Break into groups of 2-4 students
2. Analyze the available information
3. Complete the risk assessment template provided
4. Present your findings to the class

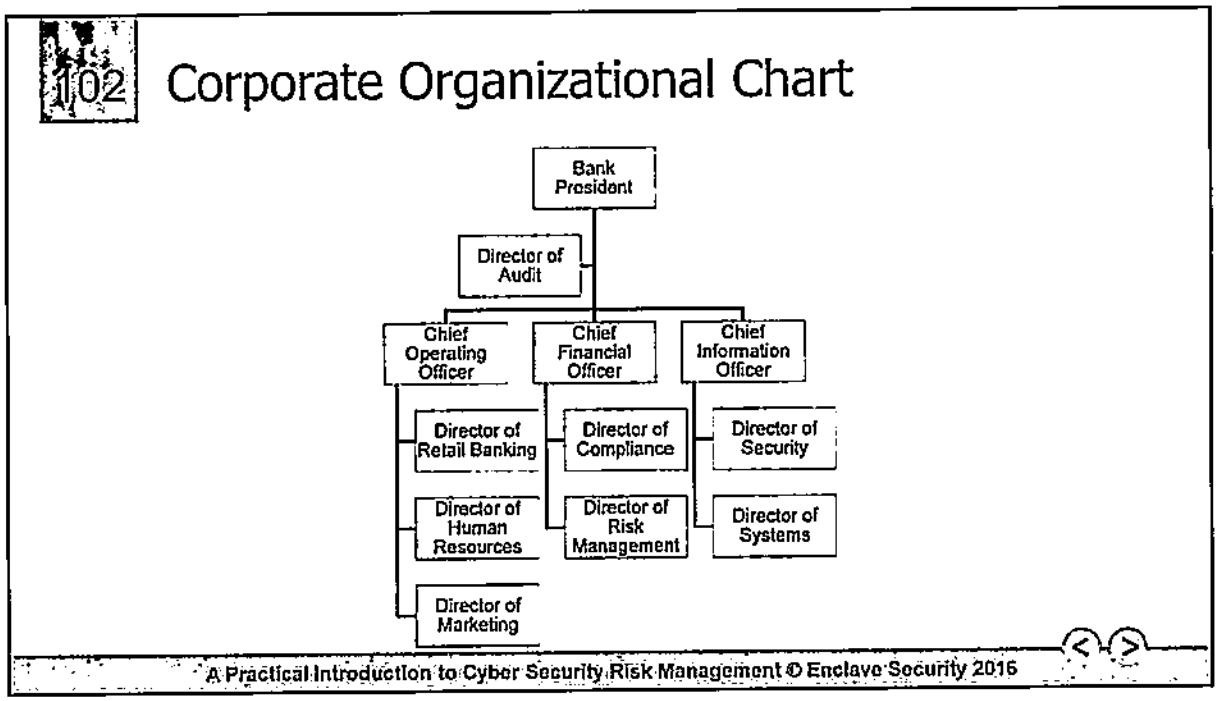
101 Company Overview

- Company Name: First Community Bank of SANS
- Established: 1982
- Physical Offices: Corporate Office (Bethesda, MD)
  12 Bank Branches
- Total Employees: 24 Corporate users
  8 Employees per branch

A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

The company you will be assessing is the First Community Bank of SANS. This bank was established in 1982 and is a small regional bank which is headquartered in the Mid-Atlantic region of the United States. Presently they have 12 branch offices, in addition to their corporate office, and there are no current plans to expand into any new markets.

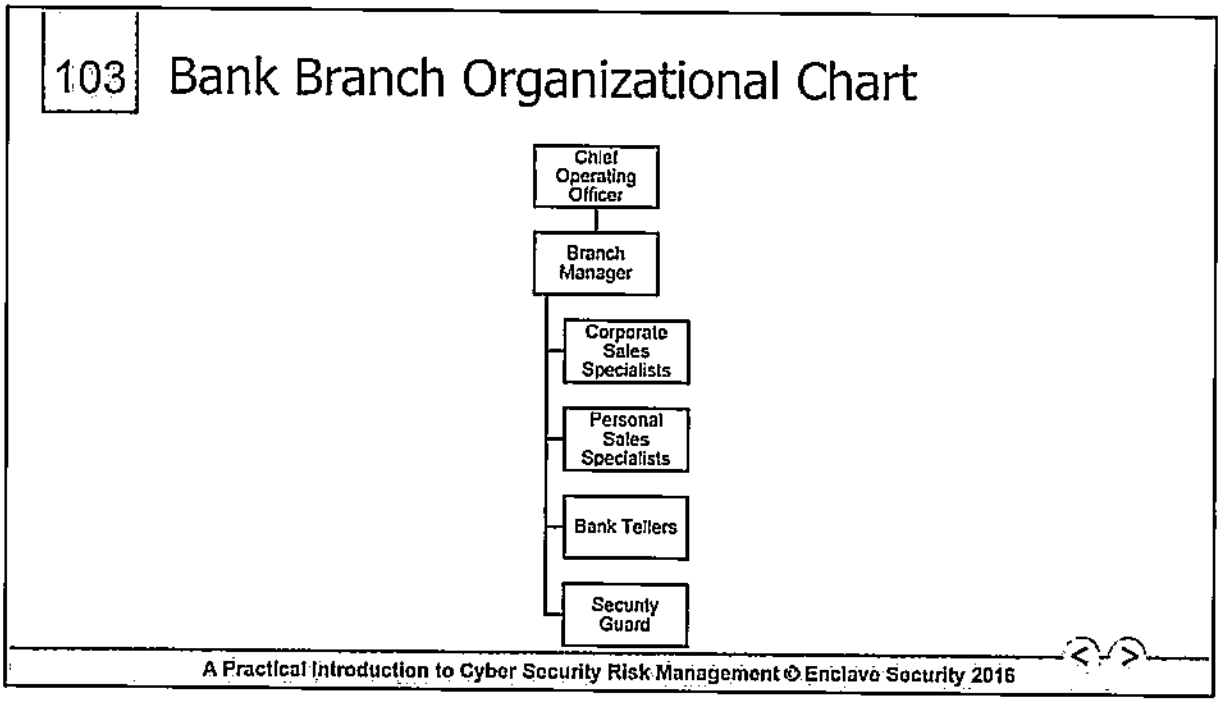
There are 24 corporate employees working out of the main corporate office and there are 8 employees at each of the branches. At the present time all positions have been filled at all of the offices.



At the corporate office there are a number of executives as well as support staff to help manage the organization as a whole. In the slide you will find a copy of the most recent organizational chart for the corporate office.

The employees and executives that are most relevant to this discussion are the following positions:

- Bank President
- Director of Audit
- Chief Operating Officer
- Chief Financial Officer
- Chief Information Officer
- Director of Retail Banking
- Director of Human Resources
- Director of Marketing
- Director of Compliance
- Director of Risk Management
- Director of Security
- Director of Systems



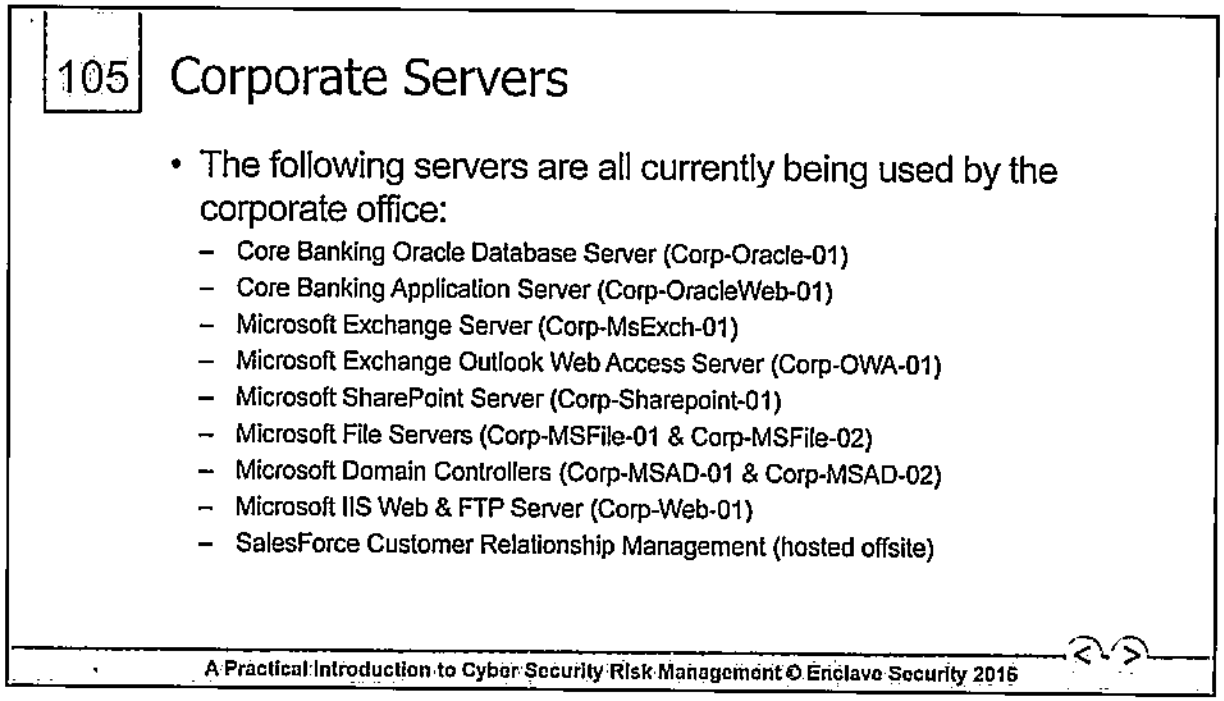
In addition to the employees at the corporate offices, each bank branch is staffed by eight employees. These employees fill the following positions at each of the branches:

- Chief Operating Officer (corporate office)
- Branch Manager
- Corporate Sales Specialists
- Personal Sales Specialists
- Bank Tellers
- Security Guard

At the present time there are twelve branch offices (in addition to the corporate office). These branch offices are located at the following locations:

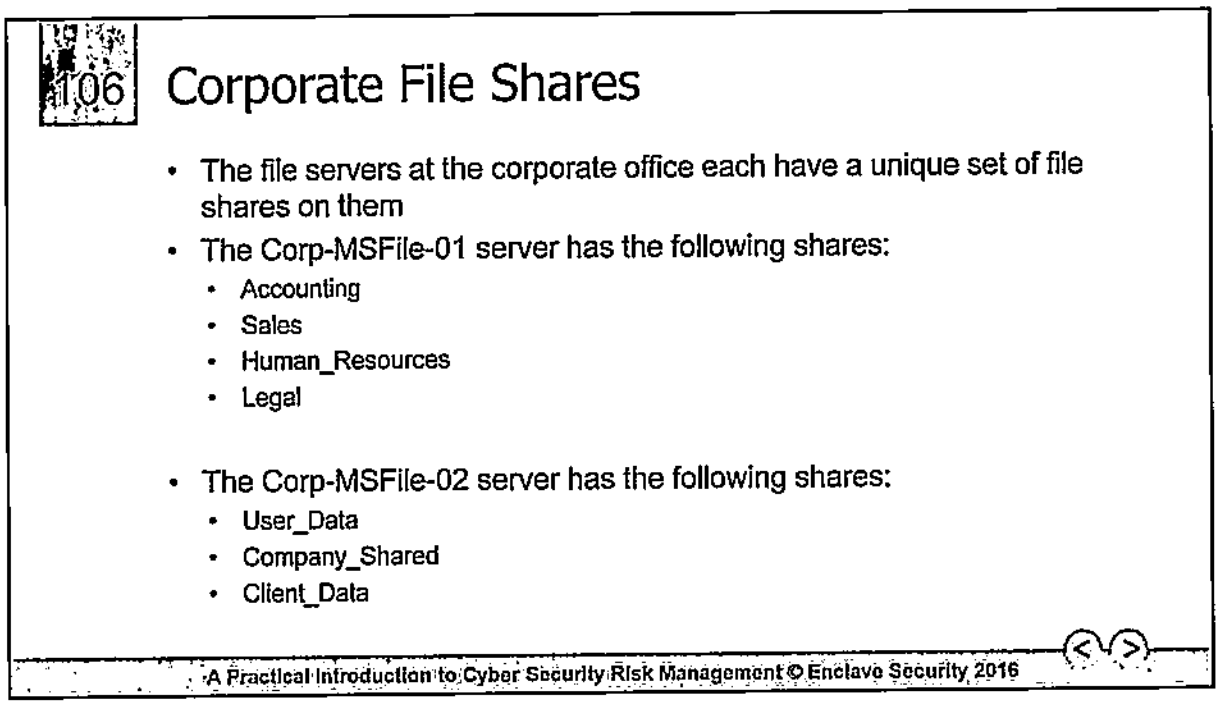
- Washington, DC (WASH)
- Bethesda, MD (BETH)
- Baltimore, MD (BALT)
- Columbia, MD (COLB)
- Rockville, MD (ROCK)
- Annapolis, MD (ANNA)
- Germantown, MD (GERM)
- Alexandria, VA (ALEX)
- Tyson's Corner, VA (TYSN)
- Herndon, VA (HERN)
- Centreville, VA (CENT)
- Springfield, VA (SPRN)

Please note, the name of each branch is followed by the branch office code for each office. Often systems have been named using this location code as a prefix for the name of the asset.



At the bank's corporate offices there are a number of computer systems used to manage the bank's operations. These systems are primarily located at the bank's main offices (Bethesda, MD). These systems include:

Core Banking Oracle® Database Server (Corp-Oracle-01)
Core Banking Application Server (Corp-OracleWeb-01)
Microsoft® Exchange Server (Corp-MsExch-01)
Microsoft® Exchange Outlook Web Access Server (Corp-OWA-01)
Microsoft® SharePoint Server (Corp-Sharepoint-01)
Microsoft® File Servers (Corp-MSFile-01 & Corp-MSFile-02)
Microsoft® Domain Controllers (Corp-MSAD-01 & Corp-MSAD-02)
Microsoft IIS® Web & FTP Server (Corp-Web-01)
SalesForce® Customer Relationship Management (hosted offsite)



A couple of the servers at the corporate office are file servers and there are a number of file shares located on these servers.

The Corp-MSFile-01 server has the following shares:

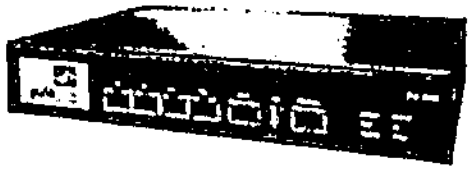
1. Accounting
2. Sales
3. Human_Resources
4. Legal

The Corp-MSFile-02 server has the following shares:

1. User_Data
2. Company_Shared
3. Client_Data

107 Corporate Network Equipment

- The following network devices are currently being used at the corporate office:
  - Cisco ASA 5510 Firewall / Router
  - Palo Alto Networks PA-500 Firewall
  - 48-port Cisco Gigabit Switch (Internal)
  - 24-port Cisco Gigabit Switch (DMZ)

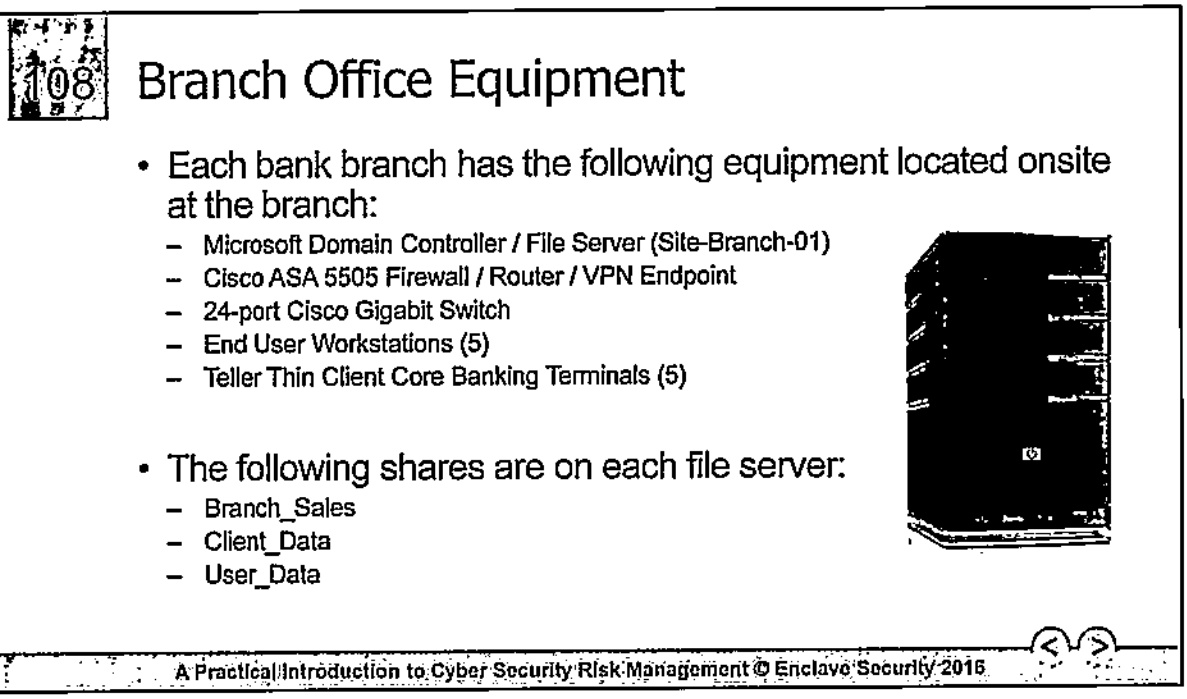


A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

In order to manage the corporate office's network and connectivity between each of the offices, the following network equipment is located at the main corporate office.

Cisco® ASA 5510 Firewall / Router
Palo Alto® Networks PA-500 Firewall
48-port Cisco® Gigabit Switch (Internal)
24-port Cisco® Gigabit Switch (DMZ)

It should be noted that the Internet connection for all of the branches is centralized through the main corporate office. Each bank branch has point to point connections back to the main corporate office and they have the ability to use the main Internet connection through this office. Also, each branch office has the ability to access network assets at the corporate office through these wide area network connections.

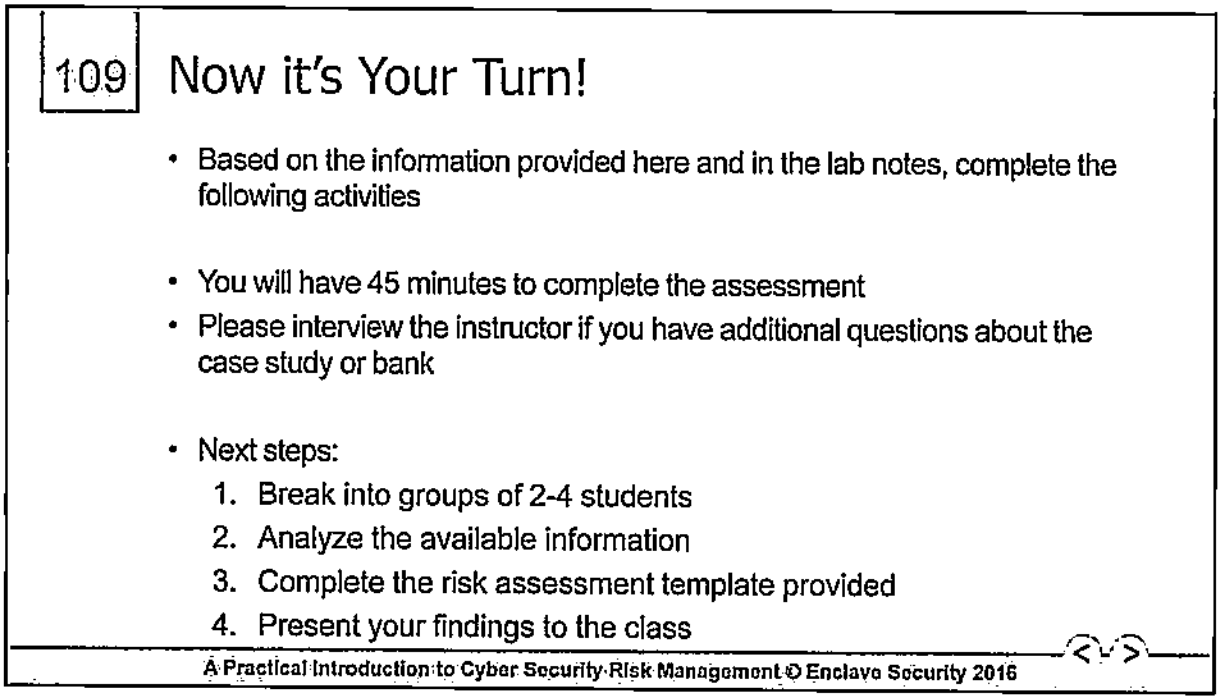


In addition to the equipment located at the corporate office, each bank branch also has equipment deployed to it as well. The network team has done a great job of standardizing each of the branch offices and each has been deployed in the same manner using similar equipment. Presently each office has the following equipment deployed to the office:

- Microsoft Domain Controller / File Server (Site-Branch-01)
- Cisco ASA 5505 Firewall / Router / VPN Endpoint
- 24-port Cisco Gigabit Switch
- End User Workstations (5)
- Teller Thin Client Core Banking Terminals (5)

On the file share for each branch, the following file shares are currently available:

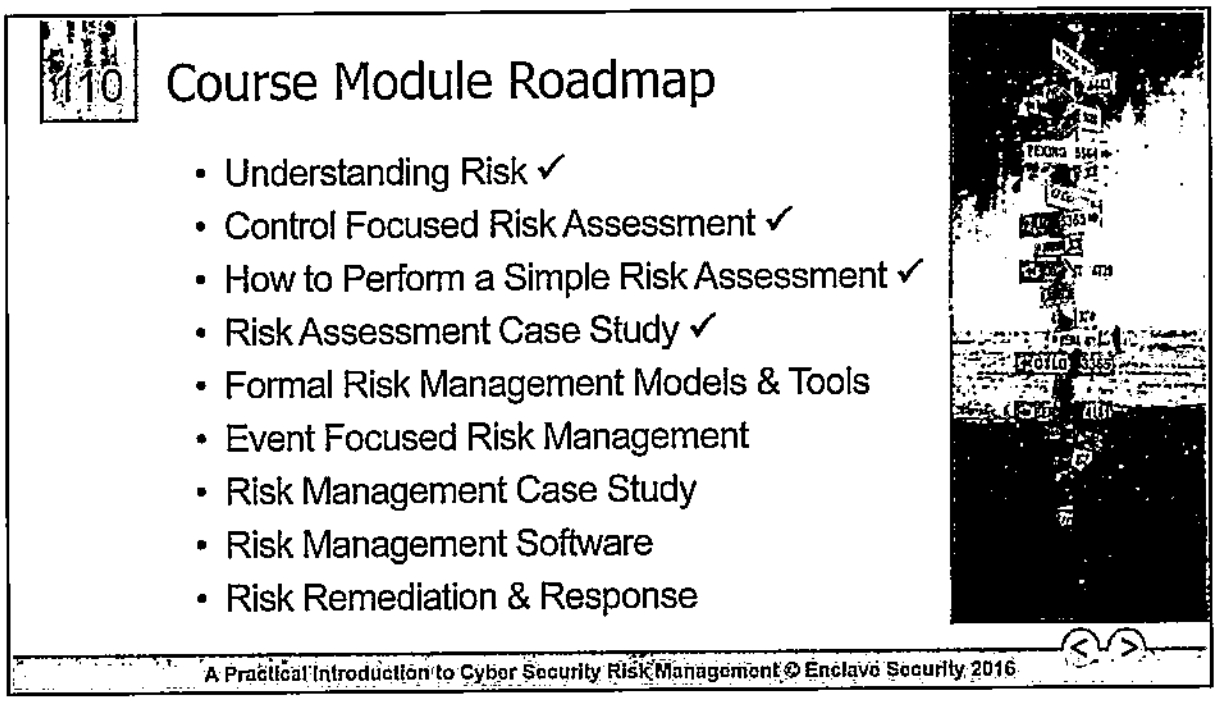
1. Branch_Sales
2. Client_Data
3. User_Data



Ok, let's get started! Based on the information that's been provided to you so far and in the lab notes, it is time to complete this case study. You will have about 45 minutes as a team to complete the assignment and be ready to present your findings to the class. It sounds like a long time, but the time will go quickly, so make sure you stay on task.

To evaluate your time, the main activities you will need to complete (with time estimates) are listed below:

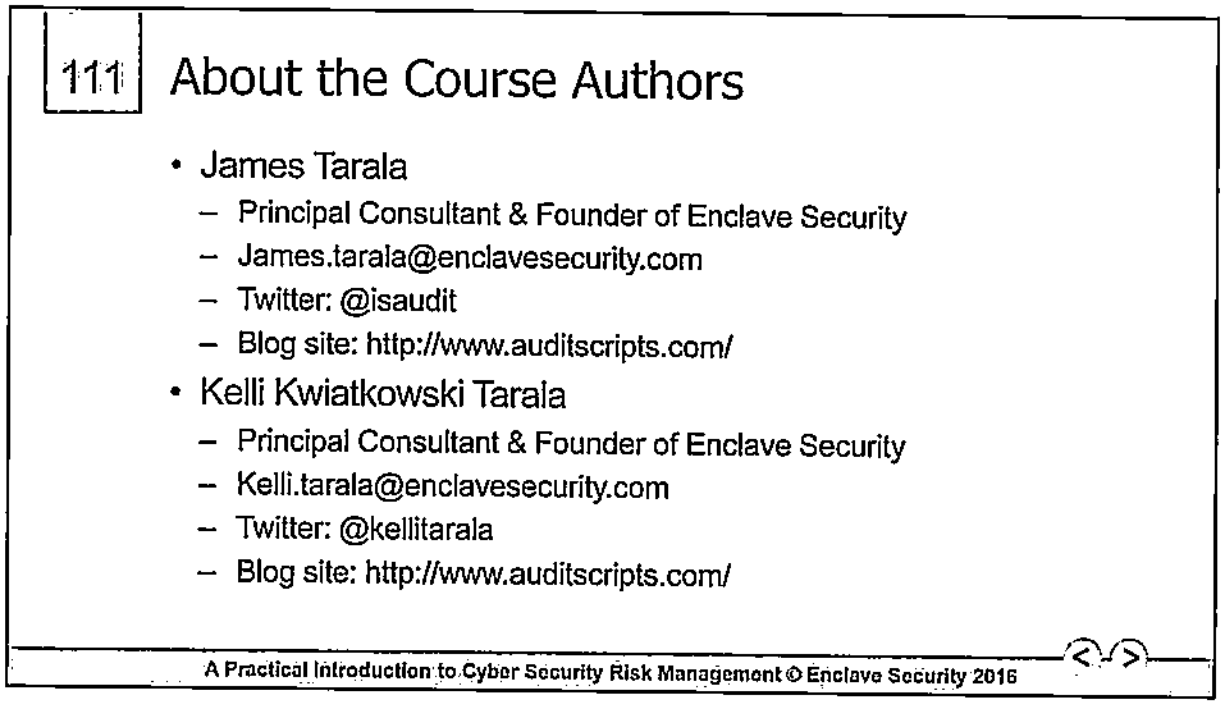
1. Break into groups of 2-4 students (5 minutes)
2. Analyze the available information (10 minutes)
3. Complete the risk assessment template provided (30 minutes)
4. Present your findings to the class (30 minutes)



In this course we will explore the concept of risk and its practical impact on an organization. Ultimately the goal of this course is to prepare students to effectively utilize risk assessment as a tool for enterprise defense. Too many times organizations think of risk assessment and risk management as academic tools with little to no practical application. These concepts are often viewed as a formal task to pursue when an organization has free time rather than as a core business activity that drives other enterprise security efforts. In today's course students will have the opportunity to learn about the proper place of risk assessment and risk management in an enterprise. They will also be given practical skills for how to perform a risk assessment on a step by step basis, from data collection to the point of presenting their findings to business leaders. Students with a desire to perform more in depth analysis will also be given tools and formal models to consider to empower them to create a long term / formal risk management program.

Specifically today we will cover the following subjects:

- Understanding Risk
- Control Focused Risk Assessment
- How to Perform a Simple Risk Assessment
- Risk Assessment Case Study
- Formal Risk Management Models & Tools
- Event Focused Risk Management
- Risk Management Case Study
- Risk Management Software
- Risk Remediation & Response



Course Lead Authors

James Tarala

James Tarala is a principal consultant with Enclave Security and is based out of Venice, FL. He is a regular speaker and senior instructor with the SANS Institute, as well as a courseware author and editor for many of their auditing and security courses. As a consultant, he has spent the past few years architecting large enterprise IT security and infrastructure architectures, specifically working with many Microsoft based directory services, e-mail, terminal services, and wireless technologies. He has also spent a large amount of time consulting with organizations to assist them in their security management, operational practices, and regulatory compliance issues, and often times performs independent security audits and assists internal audit groups to develop their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University, his graduate work at the University of Maryland, and holds numerous professional certifications.

Kelli Kwiatkowski Tarala

Kelli Tarala is a principal consultant with Enclave Security. Her career began in 1994 as a system administrator and technical editor at a pharmaceutical research organization. As a security architect and project manager, she specializes in IT security operations, information assurance strategies, and DIACAP certification & accreditation. As a consultant, she has assisted banks, DoD contractors, health insurance companies, law firms, and local, state, and tribal governments with information security initiatives. She holds numerous professional certifications including GIAC, CGEIT, and PMP. She is a courseware author editor for the CISA auditing course and regularly contributes to an information security column.

This page intentionally left blank.

Performing a Simple Risk Assessment

In this next exercise we will be performing a simple risk assessment of information assets using Microsoft Excel as the primary tool for performing the assessment. The purpose of this lab is to take the principles we have learned in class and apply them in our groups. Often times when organizations first perform risk assessments they discover that they do not have the time or the resources to use lengthy processes for performing a risk assessment. Their goal instead is simply to begin the process of risk assessment using basic tools to start prioritizing where additional controls may be necessary to protect their information systems. In addition, you may find yourself in situations where you need to recommend to organizations a simple process of performing a risk assessment if they have never performed this type of activity before. This exercise will help students to perform this type of assessment and get an initial picture of how to perform such assessments.

Part One: Break Up into Small Groups

To start this lab the first thing you will need to do is break up into groups of 4-5 people per group. For this exercise, as with a few others in the class, we will be performing the exercise as a group, so you will need to find some people sitting around you that you can work with for the course. If you have not already introduced yourself to the people around you and pick a small team to work with for the course. You will be sharing ideas and hopefully getting to know everyone quite well.

Eventually you will need to determine which roles everyone will play in the group. Each group should have a spokesperson who can report findings to the class, a timekeeper to watch the clock and keep everyone on task, and a secretary who can take notes on your group decisions. Since we will be performing multiple group exercises during the course, plan on switching these roles during each of the exercises.

Part Two: Complete the Risk Assessment Worksheet

Next, as a group it is now time to complete your risk assessment worksheet and start to discuss as a group how you would rate each of the systems in your inventory. On your course USB you will find a template for risk assessment in the Security Tools directory in a folder labeled Enclave Risk Assessment. Open the Microsoft Excel file you find in that directory and we will use it as a template for this exercise.

Please Note: Most of you will likely have Microsoft Office already installed on your system to open this file. You will have the most functionality (including conditional formatting) if you use Microsoft Excel to open the file. However, if you do not have Microsoft Office on the laptop you brought to class, there is a copy of Open Office in the Utilities directory on the course USB that you can install to open this file. If you need to, take a few moments now to install Open Office in order to read the file.

Once you've opened the Microsoft Excel file template for risk assessment, the first step will be to complete the fields identifying the Physical Data Asset and the Data Set Description. These fields will

inventory each device you have on your network (each information asset) and each data set that is present on that physical asset. Ultimately we will be providing risk scores for each data set (not each physical asset).

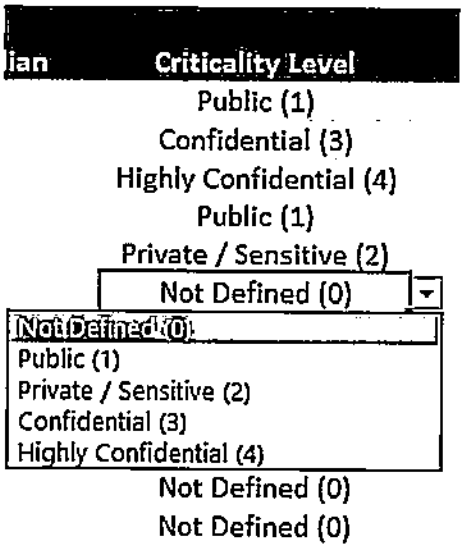
To start, enter each of the physical data assets and data sets into the worksheet using the information as you see it below:

5	Identifier	Physical Data Asset	Data Set Description
6	000001	File Server 01	Accounting File Share
7	000002	File Server 01	HR File Share
8	000003	File Server 02	Marketing File Share
9	000004	File Server 02	Sales File Share
10	000005	File Server 02	Research File Share
11	000006	File Server 02	Marketing Brochures
12	000007	File Server 03	IS Documentation
13	000008	File Server 03	IS Backup Configs
14	000009	File Server 03	IS File Share
15	000010	Accounting Server 01	Accounting Database
16	000011	HR Server 01	HR Database
17	000012	Domain Controller 01	AD Database / Config
18	000013	Web Server 01	Internet Brochure Site
19	000014	Web Server 02	Intranet Portal
20	000015	Mail Server 01	Executive Email
21	000016	Mail Server 02	Standard Email
22	000017	Core Switch 01	Configuration File
23	000018	Core Switch 02	Configuration File
24	000019	Edge Router 01	Configuration File
25	000020	Edge Firewall 01	Configuration File
26			

Once you have entered the information into these fields you will also want to assign someone in your group to be the data owner for each of the assets. As a group, assign a data owner to each of the assets that you have listed in the worksheet so far. These should be the names of people, not positions in the company – individuals should be assigned responsibility for each of the systems.

Once a data owner has been assigned to each asset the next step will be to assign a Criticality Level to each of the assets. Ultimately the data owner gets to be the one to assign the criticality asset to each of their own systems, but they will likely want to do so with input from the rest of their group.

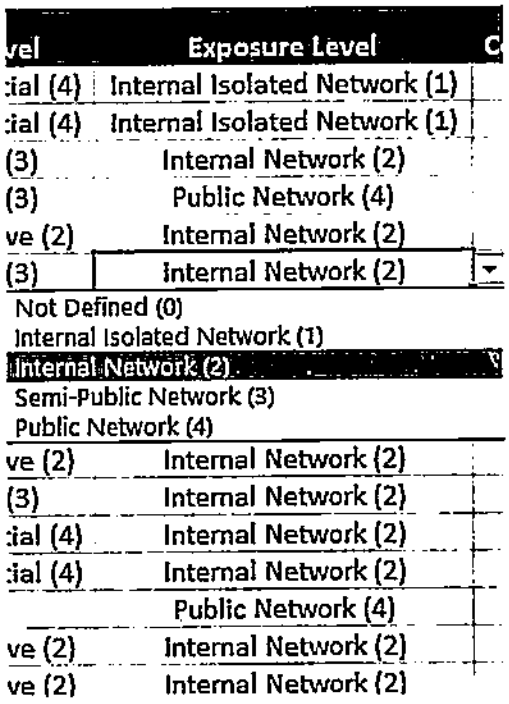
The next step is to assign a criticality level, in this case on a scale of one to four. In the blank Excel risk assessment worksheet provided you will notice that drop down menus are available for this field. It is important for the sake of the built in calculations in the worksheet to choose from a choice in the drop down menu. At this point the values are not as important as familiarizing yourself with the tool. Enter the appropriate level into the corresponding fields similar to what you see below, but ensure that every asset is assigned a value:



Please Note: Be careful in the next sections of the worksheet, some of the fields are set as formulas and are not meant to be modified. Only enter data for the fields as they are described below and be careful not to erase any of the formulas, or you will find that the calculations at the end of the worksheet are no longer accurate.

Once you have entered values for each of the criticality levels, it is now time to indicate the appropriate level of exposure for each of the assets in the risk assessment. In this case the exposure level of the system is directly tied to the location on the organization's network where the asset resides. While certainly other criteria could be used here as well, this field provides a good example of the types of choices you may want to consider when assessing the level of exposure to a given information asset.

At this point, please select an exposure level for each of the assets you have defined as seen in the following screen capture:



The next step is to assign Threat Ratings to each of the data sets assigned to the data owners. Again the data owners are the ones with the ultimate say as to what the rating will be. However again group input is always appreciated. For the sake of this exercise the way that we will be measuring threat is by determining which controls have been implemented on these systems. In this exercise we have identified four controls that we will be using as our benchmark. Those controls are:

- Whether they system has implemented application whitelisting
- Whether the system and application has been updated with patches
- Whether local administrative right have been restricted
- Whether a host-based firewall has been implemented on the system

In your group use the tool to assign ratings to each of the systems. Remember the values you choose here are not critical, it is most important that we learn how the mechanics of the tool works. When you are complete, you will see an aggregate control rating created based on the selections you choose. The results of the tool will look something similar to the following:

	Identifier	Physical Data Asset	Data Set Description	Host Based Firewall Enabled	Overall Control Rating
6	000001	Corp-Oracle-01	Core Banking Database	Policy Requires Control (1)	1.8
7	000002	Corp-OracleWeb-01	Core Banking Application	Policy Requires Control (1)	1.8
8	000003	Corp-MsExch-01	Corporate Email	Policy Requires Control (1)	1.8
9	000004	Corp-OWA-01	Corporate Email	Control Fully Implemented (3)	2.3
10	000005	Corp-Sharepoint-01	Sales & Marketing Data	Control Fully Implemented (3)	2.3
11	000006	Corp-MSFile-01	Accounting Share	Policy Requires Control (1)	2.5
12	000007	Corp-MSFile-01	Sales Share	Policy Requires Control (1)	2.5
13	000008	Corp-MSFile-01	Human Resources Share	Policy Requires Control (1)	2.5
14	000009	Corp-MSFile-01	Legal Share	Policy Requires Control (1)	2.5
15	000010	Corp-MSFile-02	User File Share	Policy Requires Control (1)	2.5
16	000011	Corp-MSFile-02	Company File Share	Policy Requires Control (1)	2.5
17	000012	Corp-MSFile-02	Client Data Share	Policy Requires Control (1)	2.5
18	000013	Corp-MSAD-01	AD Domain Credentials	Policy Requires Control (1)	2.5
19	000014	Corp-MSAD-02	AD Domain Credentials	Policy Requires Control (1)	2.5
20	000015	Corp-Web-01	Web Application	Control Fully Implemented (3)	2.3
21	000016	Corp Cisco ASA	Configuration File	Policy Requires Control (1)	2.3
22	000017	Corp Palo Alto	Configuration File	Policy Requires Control (1)	2.3
23	000018	Corp Internal Switch	Configuration File	Policy Requires Control (1)	2.3
24	000019	Corp DMZ Switch	Configuration File	Policy Requires Control (1)	2.3

The next step is to perform the same process, this time for what the data owner considers to be the Vulnerability Ratings for each of their systems. Please complete the section of the worksheet now and assign values (on a scale of one to four) for each of the assets you have identified. Once again, make sure you select from the available options in the drop down menus provided.

The worksheet should appear similar to the following screen capture:

5	Identifier	Physical Data Asset	Data Set Description	Vulnerability Rating
6	000001	Corp-Oracle-01	Core Banking Database	Critical (3)
7	000002	Corp-OracleWeb-01	Core Banking Application	Critical (3)
8	000003	Corp-MsExch-01	Corporate Email	Urgent (4)
9	000004	Corp-OWA-01	Corporate Email	Urgent (4)
10	000005	Corp-Sharepoint-01	Sales & Marketing Data	Urgent (4)
11	000006	Corp-MSFile-01	Accounting Share	Serious (2)
12	000007	Corp-MSFile-01	Sales Share	Serious (2)
13	000008	Corp-MSFile-01	Human Resources Share	Serious (2)
14	000009	Corp-MSFile-01	Legal Share	Serious (2)
15	000010	Corp-MSFile-02	User File Share	Serious (2)
16	000011	Corp-MSFile-02	Company File Share	Serious (2)
17	000012	Corp-MSFile-02	Client Data Share	Serious (2)
18	000013	Corp-MSAD-01	AD Domain Credentials	Serious (2)
19	000014	Corp-MSAD-02	AD Domain Credentials	Serious (2)
20	000015	Corp-Web-01	Web Application	Urgent (4)
21	000016	Corp Cisco ASA	Configuration File	Critical (3)
22	000017	Corp Palo Alto	Configuration File	Critical (3)
23	000018	Corp Internal Switch	Configuration File	Critical (3)
24	000019	Corp DMZ Switch	Configuration File	Critical (3)

Finally, now that we have completed the remainder of the risk assessment template, we can see automated risk scores created as a result of our calculations. Please understand that the formulas that are used will create odd numbers as overall risk ratings. These are meant to be relative ratings that can be used to understand where our greatest areas of risk exist. The remediation priority field is an automatic field that will be completed in light of the risk scores and give the user a relative expression of priorities for remediating risk. Hopefully these scores will help reflect the information you have already entered into the system and help you to prioritize where you need to concentrate your efforts to implement additional compensating controls.

5	Identifier	Physical Data Asset	Data Set Description	Overall Risk Rating	Remediation Priority
6	000001	Corp-Oracle-01	Core Banking Database	2.1	Very High
7	000002	Corp-OracleWeb-01	Core Banking Application	2.1	Very High
8	000003	Corp-MsExch-01	Corporate Email	2.4	Very High
9	000004	Corp-OWA-01	Corporate Email	2.9	Very High
10	000005	Corp-Sharepoint-01	Sales & Marketing Data	1.9	High
11	000006	Corp-MSFile-01	Accounting Share	1.5	Medium
12	000007	Corp-MSFile-01	Sales Share	1.2	Medium
13	000008	Corp-MSFile-01	Human Resources Share	1.5	Medium
14	000009	Corp-MSFile-01	Legal Share	1.5	Medium
15	000010	Corp-MSFile-02	User File Share	1.2	Medium
16	000011	Corp-MSFile-02	Company File Share	1.2	Medium
17	000012	Corp-MSFile-02	Client Data Share	1.5	Medium
18	000013	Corp-MSAD-01	AD Domain Credentials	1.8	High
19	000014	Corp-MSAD-02	AD Domain Credentials	1.8	High
20	000015	Corp-Web-01	Web Application	2.3	Very High
21	000016	Corp Cisco ASA	Configuration File	1.6	Medium
22	000017	Corp Palo Alto	Configuration File	1.6	Medium
23	000018	Corp Internal Switch	Configuration File	1.6	Medium
24	000019	Corp DMZ Switch	Configuration File	1.6	Medium

PART THREE: ANALYZE YOUR RISK CALCULATIONS

In light of the scores that were calculated for you in the previous section, it is now time to make sure we understand how these scores were calculated and what our response to these numbers should be. In light of the individual findings that your group determined, please answer the following questions regarding your findings:

In your organization, and in light of your findings in this exercise, which of the scores you completed (threat, vulnerability, impact, or compensating controls) are under your control to change? Explain to your group why you believe this to be true.

In light of your answer to the previous question, what can you do as an organization that will most effectively lower your risk scores?

For your individual risk assessment calculations that your group determined, which assets should be the focus of your risk remediation efforts? Can you give examples of what you think might best lower the scores in your assessment to acceptable levels?

Part Four: Reporting Group Consensus

Now that your group has answered the questions, be prepared to share your decisions with the rest of the class. Remember we need to be able to be good information security analysts that can analyze complex data sets on behalf of the business, but we also have to be effective communicators who have the ability to share our ideas with others and be persuasive in the process. So for the final portion of this exercise, and for a few exercises that we are going to complete during this course, be prepared to share your ideas with the class.

We will be performing multiple small group exercises during class, so as you break into small groups, make sure you pick a spokesperson for your group, but make sure it is a different spokesperson for each exercise we perform. That will give everyone a chance to practice their skills of oral persuasion. For this exercise though, pick one person who will be the primary reporter for these results.

After each of the groups has had enough time to come up with appropriate answers to the earlier questions we will reconvene as a class to discuss the results. The instructor will announce when it is time to get back together as a class to report the findings.

This page intentionally left blank.

Risk Assessment Case Study

In this next exercise we will be performing a simple risk assessment of information assets using Microsoft Excel as the primary tool for performing the assessment. The purpose of this case study is to take the principles we have learned in class and apply them in our groups. Whereas in the previous exercise the instructor guided your groups through this exercise, in this case study you will be provided the necessary data to perform a simple risk assessment, and you will perform that assessment on your own (with your group) and report your findings to the class.

As we discussed in the previous lab exercise today, often times when organizations first perform risk assessments they discover that they do not have the time or the resources to use lengthy processes for performing a risk assessment. Their goal instead is simply to begin the process of risk assessment using basic tools to start prioritizing where additional controls may be necessary to protect their information systems. In addition, you may find yourself in situations where you need to recommend to organizations a simple process of performing a risk assessment if they have never performed this type of activity before. This exercise will help students to perform this type of assessment and get an initial picture of how to perform such assessments.

Part One: Break Up into Small Groups

To start this lab the first thing you will need to do is break up into groups of 4-5 people per group. For this exercise, as with a few others in the class, we will be performing the exercise as a group, so you will need to find some people sitting around you that you can work with for the course. If you have not already introduced yourself to the people around you and pick a small team to work with for the course. You will be sharing ideas and hopefully getting to know everyone quite well.

Eventually you will need to determine which roles everyone will play in the group. Each group should have a spokesperson who can report findings to the class, a timekeeper to watch the clock and keep everyone on task, and a secretary who can take notes on your group decisions. Since we will be performing multiple group exercises during the course, plan on switching these roles during each of the exercises.

PART TWO: COMPLETE THE RISK ASSESSMENT WORKSHEET

Next, as a group it is now time to complete your risk assessment worksheet and start to discuss as a group how you would rate each of the systems in your inventory. On your course USB you will find a template for risk assessment in the Security Tools directory in a folder labeled Enclave Risk Assessment. Open the Microsoft Excel file (Day 1 - Enclave_Risk_Assessment_Template_Blank) you find in that directory and we will use it as a template for this exercise.

Please Note: As we indicated in the course laptop setup requirements, you should have a copy of Microsoft Office 2010 or later already installed on your system to open this file. You will have the most functionality (including conditional formatting) if you use Microsoft Excel to open the file. However if you have an earlier version of Microsoft Office installed on your computer, many of the drop down choices in the tool will not work properly. You may need to work with a partner to complete the exercises.

Although we have performed a similar lab exercise already in class under the direction of the instructor, this is your opportunity to perform the assessment on your own (as a group). Your primary goal for this portion of the case study is to:

1. Complete the risk assessment spreadsheet from your course USB.
2. Answer the follow up questions from Part Three of this assignment.

All of the information you need to complete the assignment can be found in the case study section of the course from today's materials. This includes a full background on the company you will be analyzing as a part of this assessment. If you have any questions about the background or assumptions going into this assessment, please feel free to ask your instructor for feedback and clarification.

To keep your group on task, consider completing the following tasks in order in order to complete this exercise:

1. Perform an asset inventory
2. Assign a data owner to each asset (job title)
3. Assign a data custodian to each asset (job title)
4. Assign value to each asset (criticality)
5. Define the level of exposure for each asset
6. Determine the level of threat (implemented controls) facing each system
7. Determine the level of vulnerability inherent in each system
8. Establish levels of residual risk
9. Make a business decision regarding each residual risk (complete part 3)

Case Study Assumptions:

In order to complete this case study there are certain assumptions you will need to make about the controls that have been implemented on the organization's information systems. Unfortunately budgets have been limited in recent years at the organization so you are unable to take the time to technically audit each of these information systems. This leaves the organization with ambiguity regarding the implementation of certain controls. However there are some things you know about the organization, having worked for them, but many of these items are your best understandings of the issue.

- The organization has documented policies which state that every system should have application whitelisting enabled, should be up to date with all system and application patches, and that every system should have a host based firewall enabled.
- The organization also believes in the principle of least privilege and that only necessary individuals should be local administrators / super users of systems or applications.
- The organization does not always follow their own policies, but they try their best.
- Sysadmins have enabled application whitelisting on most file servers and domain controllers, but are struggling completing the process for all workstations and other servers. It's a work in progress that still has some work that needs to be completed. No documentation is available for which systems are complete on this project, it is being done in the data custodians' free time.
- The organization uses Microsoft Windows Software Update Services (WSUS) to push out Microsoft patches to systems. All other application patches are done on an ad hoc basis by data custodians and system owners.
- Most everyone is a local administrator of their own system. There are a limited number of server administrators though, and only server administrators have local administrator rights on those systems. But most every system administrator is a domain administrator. Everyone has also been given full administrator rights in SalesForce to make it easier for users to work with the system.
- The Microsoft Windows Firewall is enabled on all workstations via Group Policy. Servers and network devices sometimes have firewalls enabled, but not enforced by policy. Because sysadmins change these settings regularly it is unclear where it is enabled or not on servers.

You and your group will feel uncertain and have ambiguity regarding many of these issues. That makes a risk assessment more difficult to complete. Unfortunately it is the reality of most assessments. Ideally we would have clear answers to all of our questions, but rarely do we get the level of detail we would like when performing a high level assessment such as this.

Try your best as a group to complete the spreadsheet, even with your limited knowledge. If you are really struggling, don't be afraid to ask your instructor for help – although be aware you may not always get the clear answer you are hoping for ☺

Part Three: Analyze Your Risk Calculations

In light of the scores that were calculated for you in the previous section, it is now time to make sure we understand how these scores were calculated and what our response to these numbers should be. In light of the individual findings that your group determined, please answer the following questions regarding your findings:

In your organization, and in light of your findings in this exercise, which of the scores you completed (threat, vulnerability, impact, or compensating controls) are under your control to change? Explain to your group why you believe this to be true.

In light of your answer to the previous question, what can you do as an organization that will most effectively lower your risk scores?

For your individual risk assessment calculations that your group determined, which assets should be the focus of your risk remediation efforts? Can you give examples of what you think might best lower the scores in your assessment to acceptable levels?

Part Four: Reporting Group Consensus

Now that your group has answered the questions, be prepared to share your decisions with the rest of the class. Remember we need to be able to be good information security analysts that can analyze complex data sets on behalf of the business, but we also have to be effective communicators who have the ability to share our ideas with others and be persuasive in the process. So for the final portion of this exercise, and for a few exercises that we are going to complete during this course, be prepared to share your ideas with the class.

We will be performing multiple small group exercises during class, so as you break into small groups, make sure you pick a spokesperson for your group, but make sure it is a different spokesperson for each exercise we perform. That will give everyone a chance to practice their skills of oral persuasion. For this exercise though, pick one person who will be the primary reporter for these results.

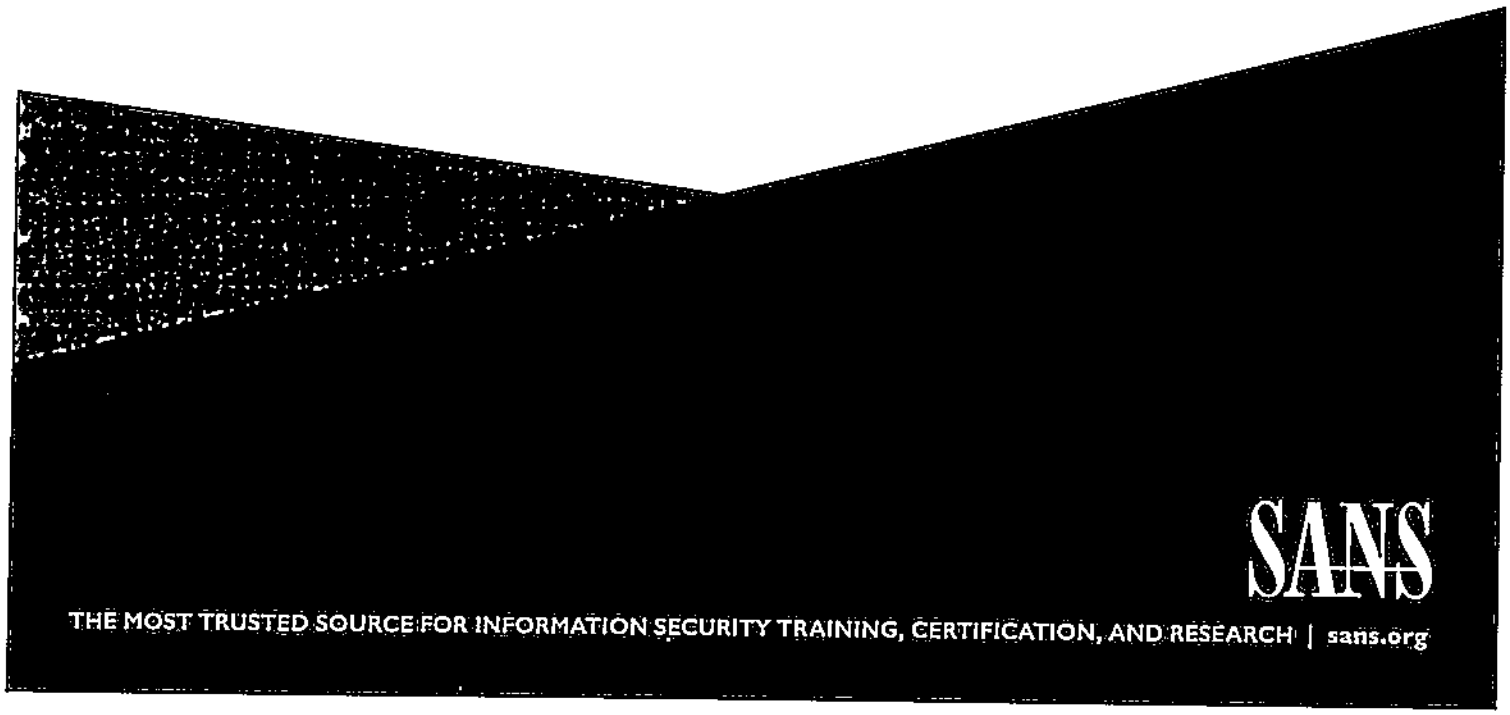
After each of the groups has had enough time to come up with appropriate answers to the earlier questions we will reconvene as a class to discuss the results. The instructor will announce when it is time to get back together as a class to report the findings.

MGT415 | A PRACTICAL INTRODUCTION TO CYBER SECURITY RISK MANAGEMENT

415.2

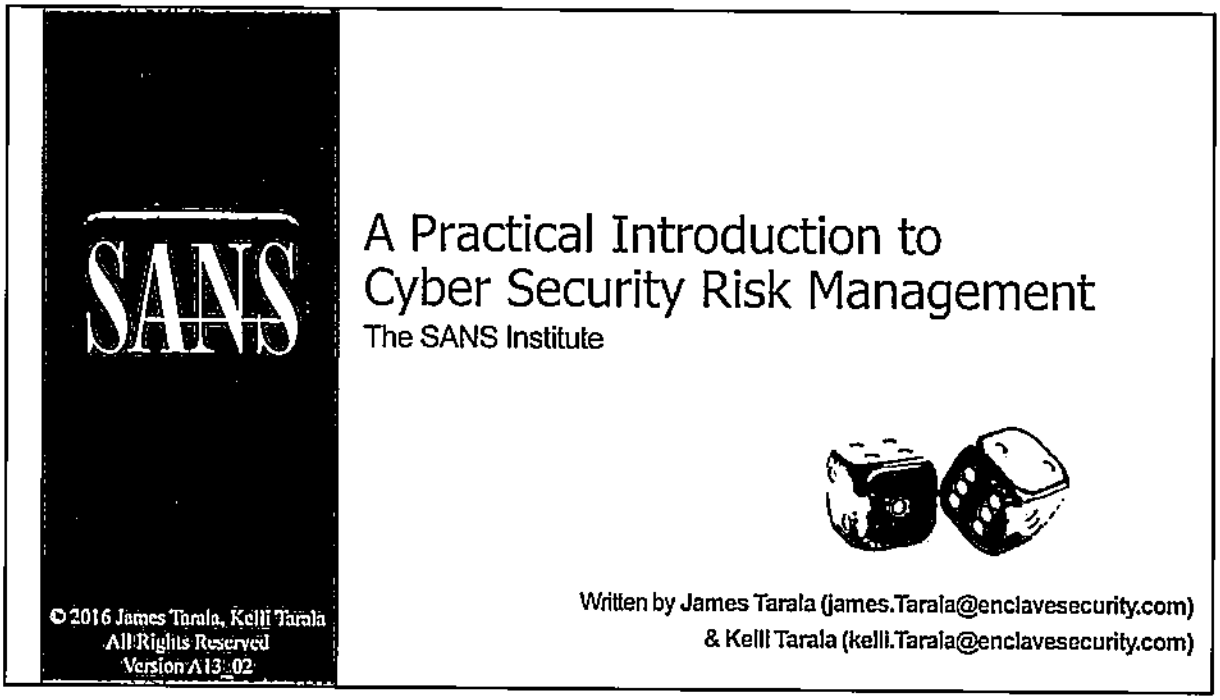
A Practical Introduction to Managing Cyber Security Risk

jepurcell@gmail.com

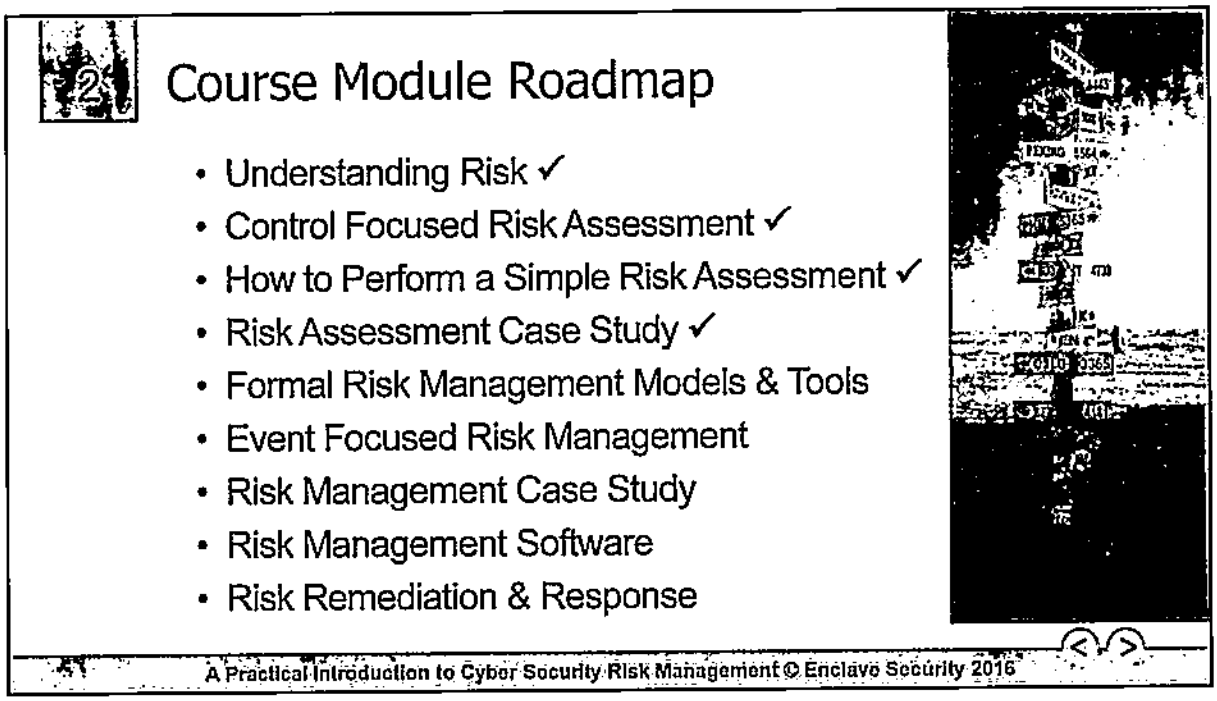


SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org



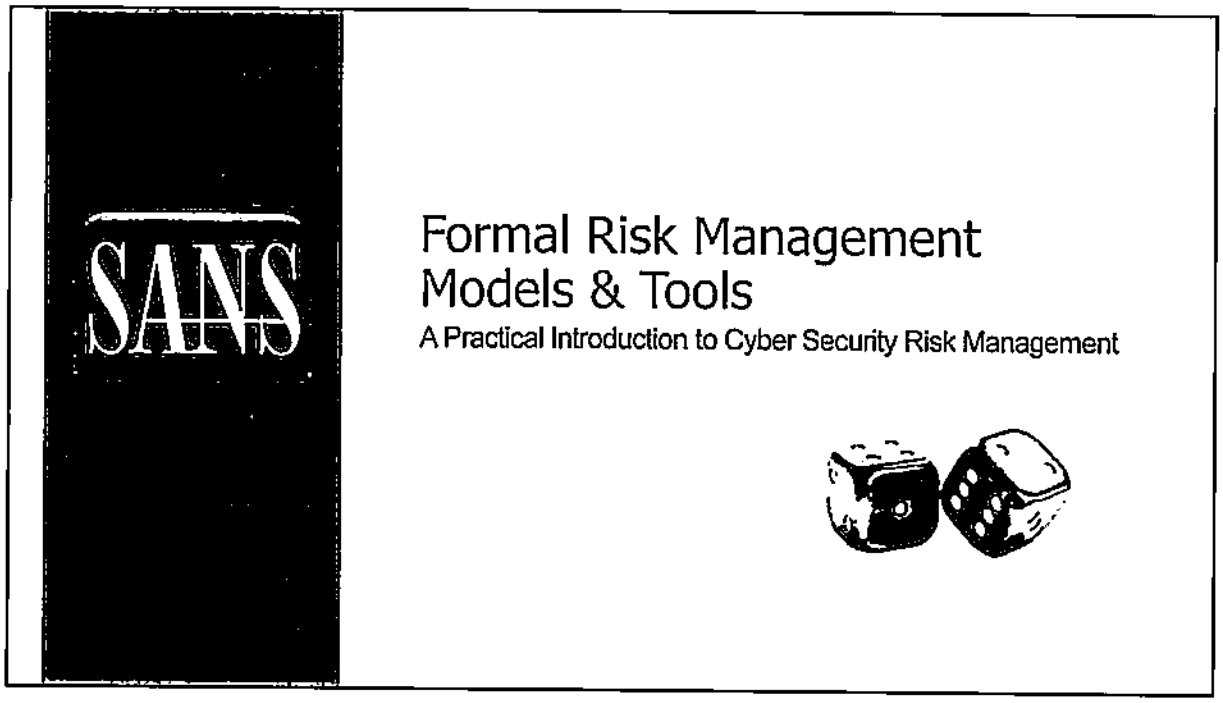
This page intentionally left blank.



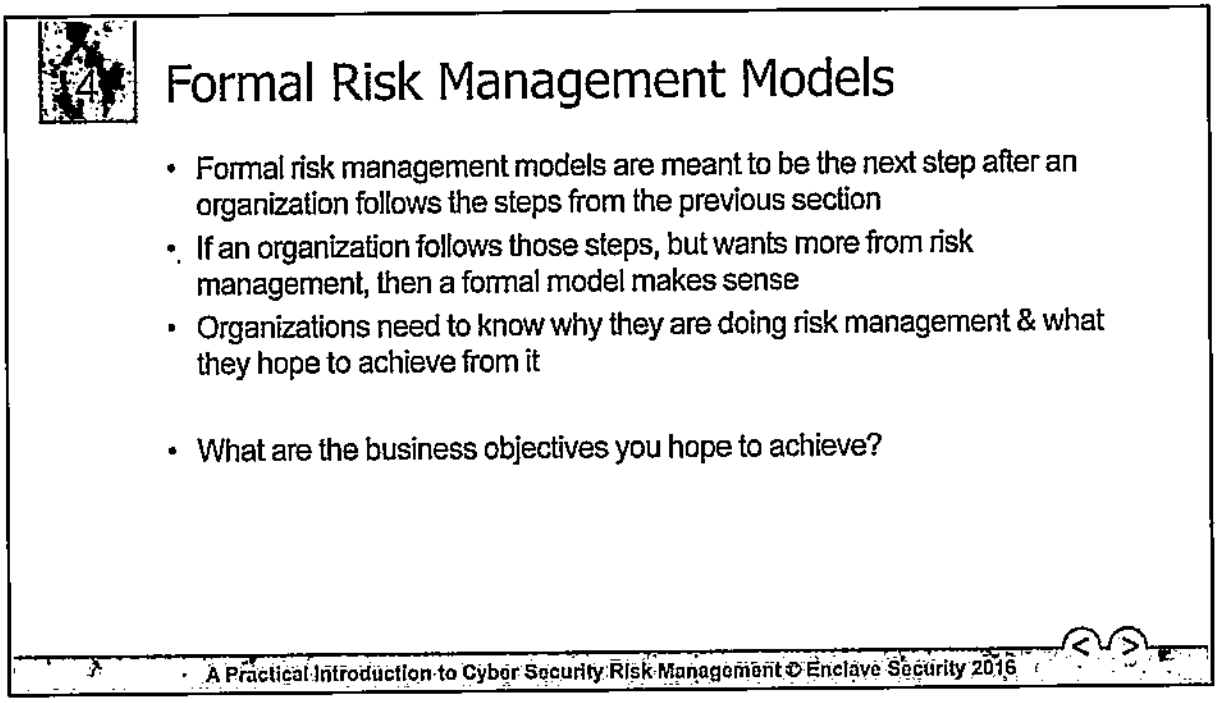
In this course we will explore the concept of risk and its practical impact on an organization. Ultimately the goal of this course is to prepare students to effectively utilize risk assessment as a tool for enterprise defense. Too many times organizations think of risk assessment and risk management as academic tools with little to no practical application. These concepts are often viewed as a formal task to pursue when an organization has free time rather than as a core business activity that drives other enterprise security efforts. In today's course students will have the opportunity to learn about the proper place of risk assessment and risk management in an enterprise. They will also be given practical skills for how to perform a risk assessment on a step by step basis, from data collection to the point of presenting their findings to business leaders. Students with a desire to perform more in depth analysis will also be given tools and formal models to consider to empower them to create a long term / formal risk management program.

Specifically today we will cover the following subjects:

- Understanding Risk
- Control Focused Risk Assessment
- How to Perform a Simple Risk Assessment
- Risk Assessment Case Study
- Formal Risk Management Models & Tools
- Event Focused Risk Management
- Risk Management Case Study
- Risk Management Software
- Risk Remediation & Response



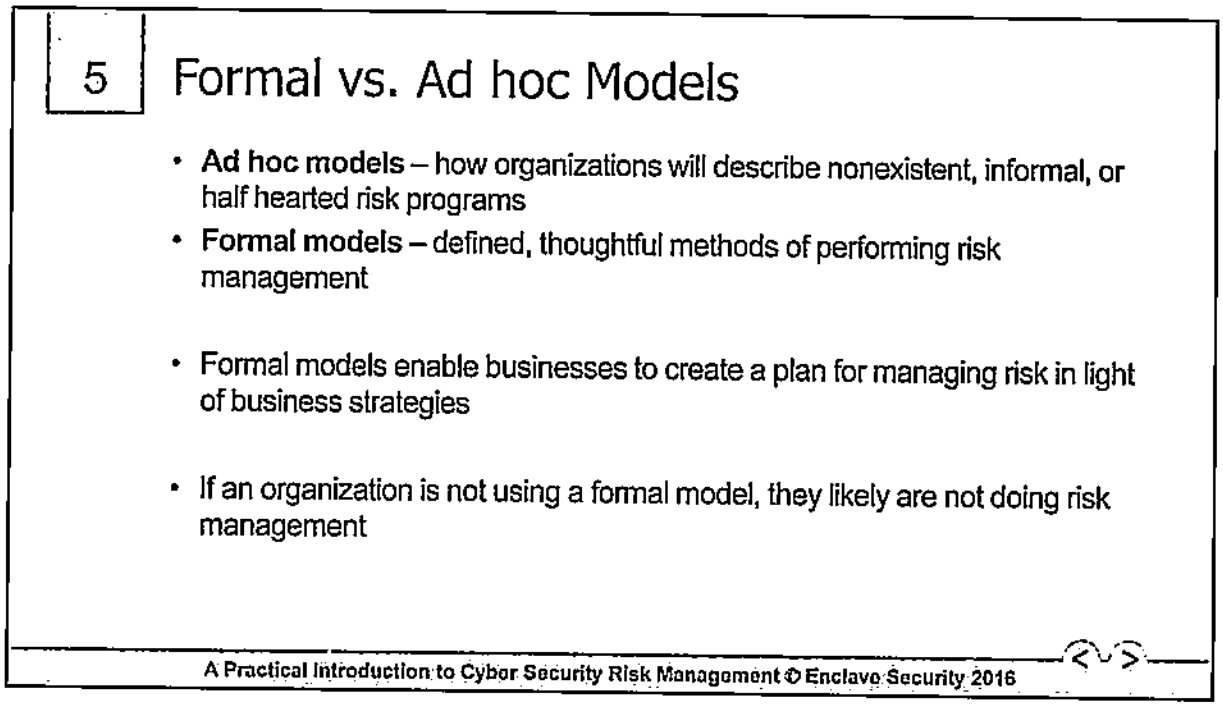
This page intentionally left blank.



In this course we have covered certain key processes that logically work together to bring us to the point where we are now, and each of the steps in this prepares us to evaluate formal risk management models. Up to this point, we have defined governance, we have identified how policies help to practically define governance strategies, and we have evaluated simple methods of performing risk assessment. The next logical step for an organization to take is to evaluate potential risk management models, which are more formalized and can bring additional value.

However, before you proceed, recognize that this step, like those before, requires resources and dedicated system personnel. Resources are not inexpensive and, therefore, should only be allocated if there is strong business support for the plan and clear business objectives can be achieved by taking these steps.

Make sure you know what those business goals are before you continue down this path.



What we are about to describe falls into the category of formal risk management models, or as we discussed them earlier, Enterprise Risk Management (ERM) capabilities. These models enable businesses to create a plan for managing risk in light of business strategies. Risk management is strategic thinking and disciplined thinking about controls, not simply random controls meshed together as a response to threats.

One option would be for organizations to follow an ad hoc model. Many times when we evaluate organizations we ask them what risk assessment or risk management model they follow, and they indicate to us that they are following an ad hoc model for risk management. But now is the time to speak honestly and directly about this topic. If an organization is not using a formal model, they likely are not doing risk management. In fact it is not uncommon that an organization will declare that they are using ad hoc risk assessment, and what they really mean is that they have nonexistent, informal, or half-hearted risk programs.

Risk management may not be for everyone. Even though most compliance programs require it, many people will create a document, call it a "risk assessment" and print a copy to laminate for their wall, but that document will never be used to manage the business. This is why compliance often times fails: we do things to check off a box rather than actually attempt to treat a risk.

Variety & Scope of Available Models

- There are many, many formal models to choose from
- Remember, not all risk management models were created to support information assurance
- Many risk models were created to manage:
  - The insurance industry
  - Financial services
  - Healthcare
  - Legal liability
- IA risk management focuses on creating metrics & priorities for managing appropriate risk levels

A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

Let us assume for the remainder of the class that you have decided to adopt a formal risk management model. You say, ok, I'll bite, let's see what options are out there. Well the first thing you will realize is that there are many, many risk management models to choose from. One of the first things you have to be aware of is that not all of the models out there were specifically written with information assurance in mind. In fact, many of them specifically were *not* written with information assurance in mind.

There are risk management models for what seems like every industry. Specifically we have seen risk management models at least for the following industry- specific issues:

- The insurance industry
- Financial services
- Healthcare
- Legal liability

Just because a program is called a risk management program it does not mean that it will be helpful when it comes to managing assurance risk. Some of these plans are written to address issues such as liability or financial loss much more so than information assurance risks. Information assurance risk management focuses on creating metrics and priorities for managing appropriate risk level. We will present risk models to you, which will assist you in meeting these goals.

7

Choosing the Right Risk Model

- One of the more important risk management decisions an organization will make is which model to follow

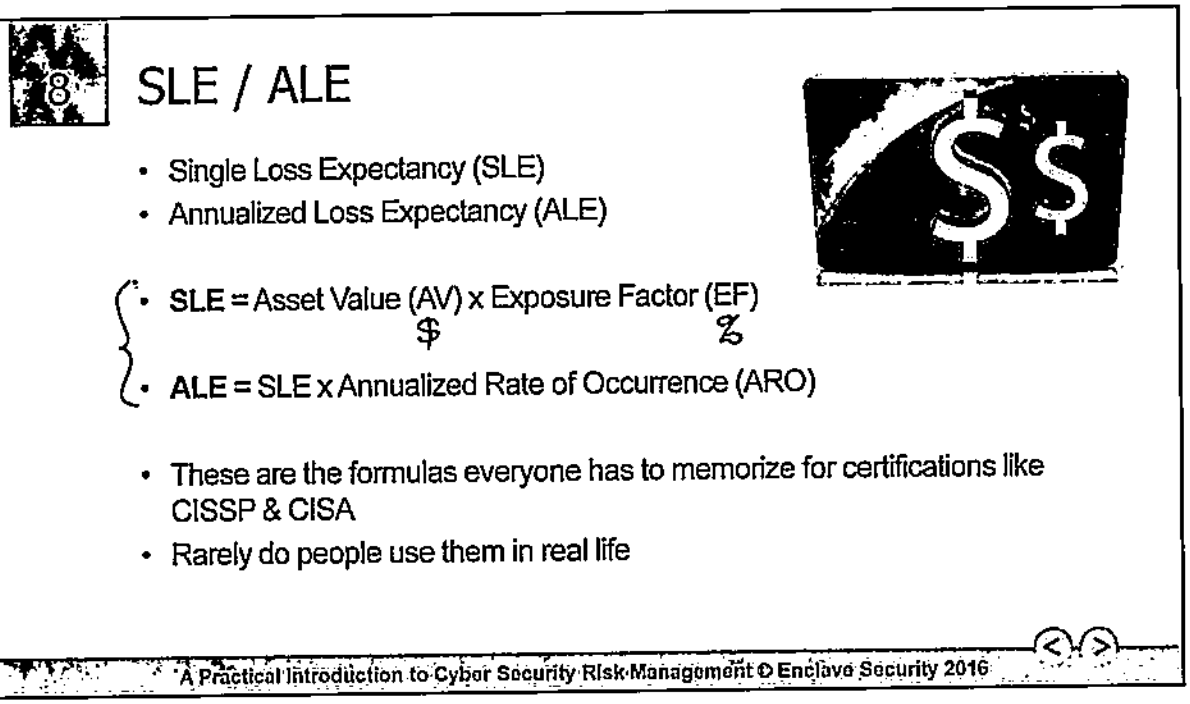
- The model an organization chooses:
  - Has to fit the culture of the organization
  - Has to be supported by executive management
  - Has to be consistent across all business units
  - Has to be used comprehensively
  - Has to be useable and produce valuable outputs

A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

how does an organization choose what the right model for their organization truly is? This decision, which model to follow, will be one of the more important decisions regarding risk management overall. If the organization chooses the wrong model, it may likely lead to ineffective use of the program and, thus, the implementation of ineffective controls, or more likely, and even worse, the risk management program being thrown out altogether or ignored.

There are many ways to choose a risk management model. Most of the time organizations will simply choose a model that is known by the personnel that work at the organization (similarly to how development languages are chosen by developers – what everyone already know how to do). That is not completely a bad idea. However some other things to consider when choosing a model is that the model:

- Has to fit the culture of the organization
- Has to be supported by executive management
- Has to be consistent across all business units
- Has to be used comprehensively
- Has to be useable and produce valuable outputs



The Single Loss Expectancy (SLE) calculation is one calculation that can be performed using a quantitative approach to risk assessment. This risk assessment method is a quantitative method for determining the financial impact of an incident occurring to a given information asset. The end goal of this type of assessment is to determine what it would cost an organization if a potential risk to the system was realized. The number that is generated as a result of this assessment can then be compared to the SLE of other systems in order to determine a general level of risk associated with an asset.

In order to calculate the SLE of an information asset, multiply the Exposure Factor (EF) by the Asset Value (AV) of the resource. The EF is a percentage value, which represents the likelihood of a given threat/vulnerability being realized. The AV is a dollar amount, which represents the total value of an asset (hardware, software, resources to rebuild, public exposure, downtime, etc). By multiplying these two values together you are able to determine the SLE. In other words, the calculation is as follows:

EF x AV = SLE

Another similar risk calculation that follows the quantitative methodology for analyzing risk is the Annualized Loss Expectancy (ALE) method. Similar to SLE in that the end product of this type of assessment is a dollar amount based on the probability of threats/vulnerabilities and the degree of impact to the organization, ALE tends to provide a bigger picture view of risk than the SLE method. The major difference between the two is that ALE builds on SLE by determining not only the cost associated with a single incident, but the cost of a single incident factored by the likelihood of the incident occurring in a given year time period.

In order to calculate the ALE of an asset, you needs to multiply the SLE of a given asset by the Annualized Rate of Occurrence (ARO). The ARO is a value indicating the potential of a given incident occurring in the course of a year. When the product of these two numbers is calculated, a big picture view of a risk occurring materializes and can then be better compared to the values of other assets.

NIST Special Publications (800 Series)

- "Documents of general interest to the computer security community."
  – NIST (http://csrc.nist.gov)

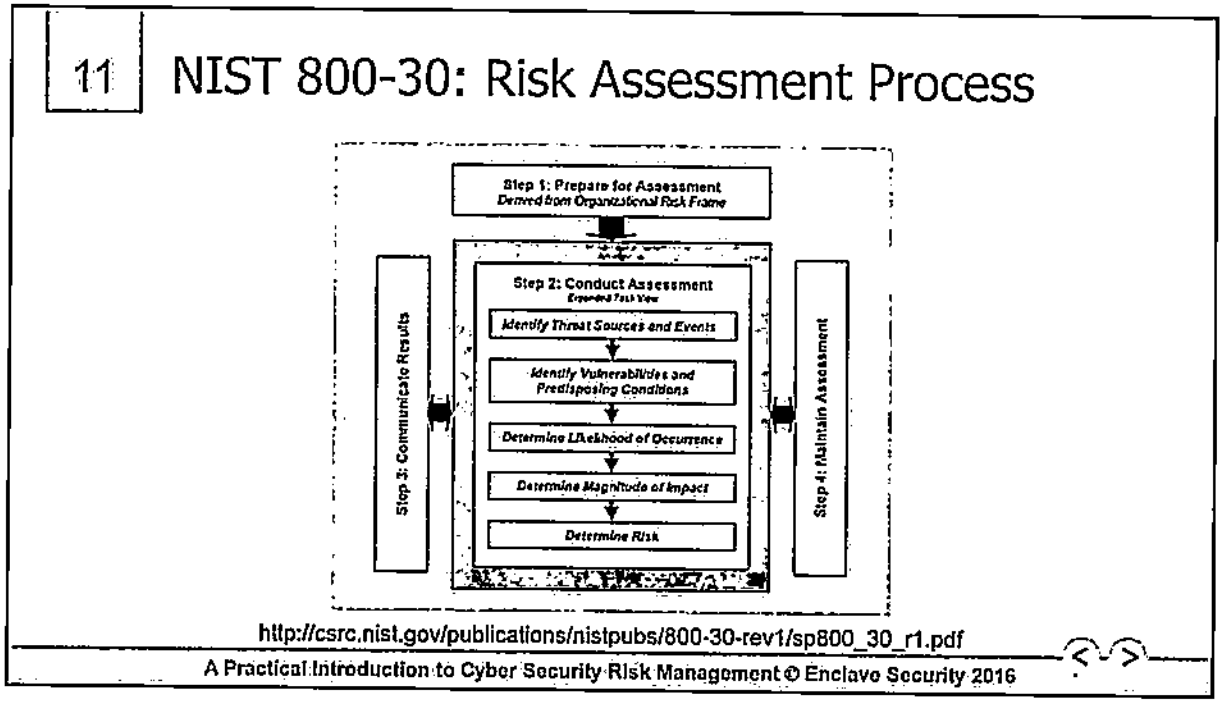
- Some of the more relevant documents to risk assessment / management are:
  – 800-30: Guide for Conducting Risk Assessments
  – 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
  – 800-39: Managing Information Security Risk: Organization, Mission, and Information System View

One popular method of risk assessment is the process described by the US National Institute of Standards & Technology (NIST). NIST has been given the charter by the US government to establish standards and resources, many of which are directly related to the study of information assurance and risk assessment specifically. In NIST's 800 series of special publications NIST publishes "documents of general interest to the computer security community' at http://csrc.nist.gov" These resources are often relied upon by US agencies and those in the private sector as definitive guides in the practice of information assurance.

Specifically in the area of risk assessment, NIST has published a number of guides which can be useful to organizations both inside and outside of the US government. Many of these guides relate to governance principles in general, while others directly describe the process of performing risk assessments or engaging in a risk management program. The three most popular guides in this series are:

- 800-30: Guide for Conducting Risk Assessments
- 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- 800-39: Managing Information Security Risk: Organization, Mission, and Information System View

NIST 800-30: guide to management
↳ NIST Ways.



In the above diagram one can see the process NIST describes for risk assessment in their 800-30 special publication. This is described in more detail in the NIST 800-30 document itself which can be found at http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf. While this process is a good overview, it is vague enough to allow organizations to customize the process and make it specific to their own organization's needs.

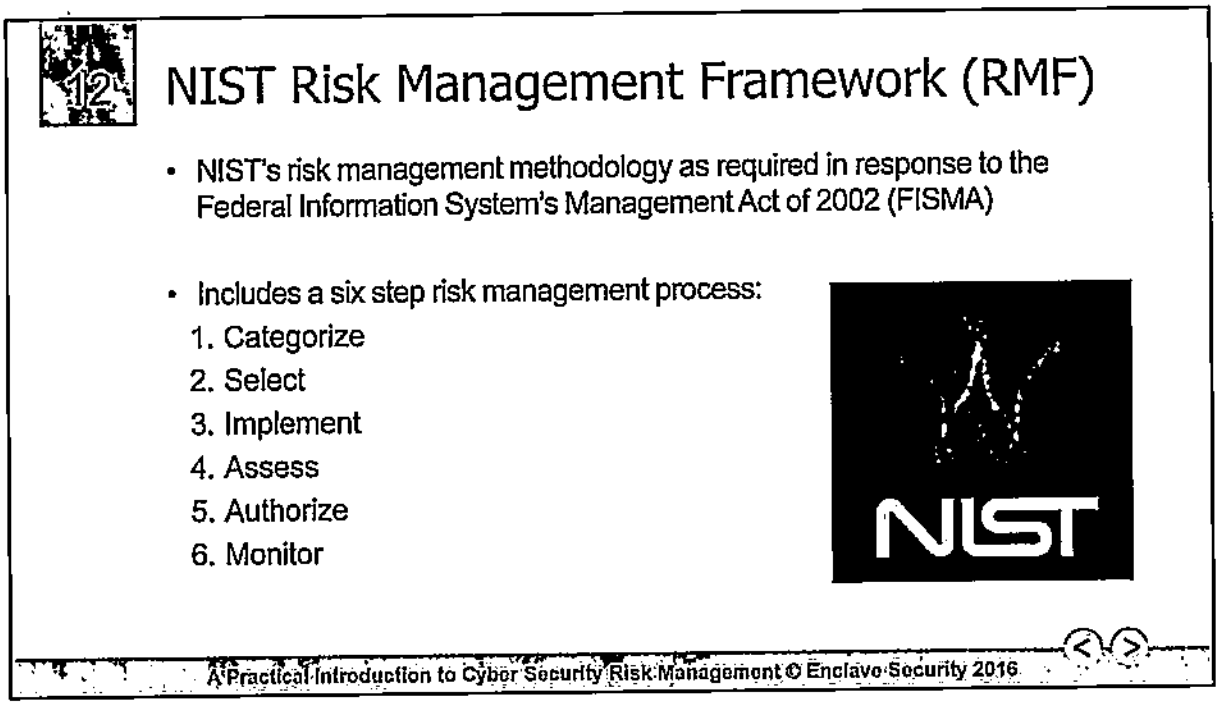
The four main steps in the risk assessment process defined by NIST 800-30 are:

Step One:	Prepare for Assessment
Step Two:	Conduct Assessment
Step Three:	Communicate Results
Step Four:	Maintain Assessment

In the process of actually performing the assessment itself (Step Two), NIST recommends the following steps as components to the overall assessment process:

1. Identify threat sources and events.
2. Identify vulnerabilities and predisposing conditions
3. Determine likelihood of occurrence
4. Determine magnitude of impact
5. Determine risk

So as we have see with many other approaches, the components of threat, vulnerability, likelihood, and impact are all mentioned in NIST's guidance as well.

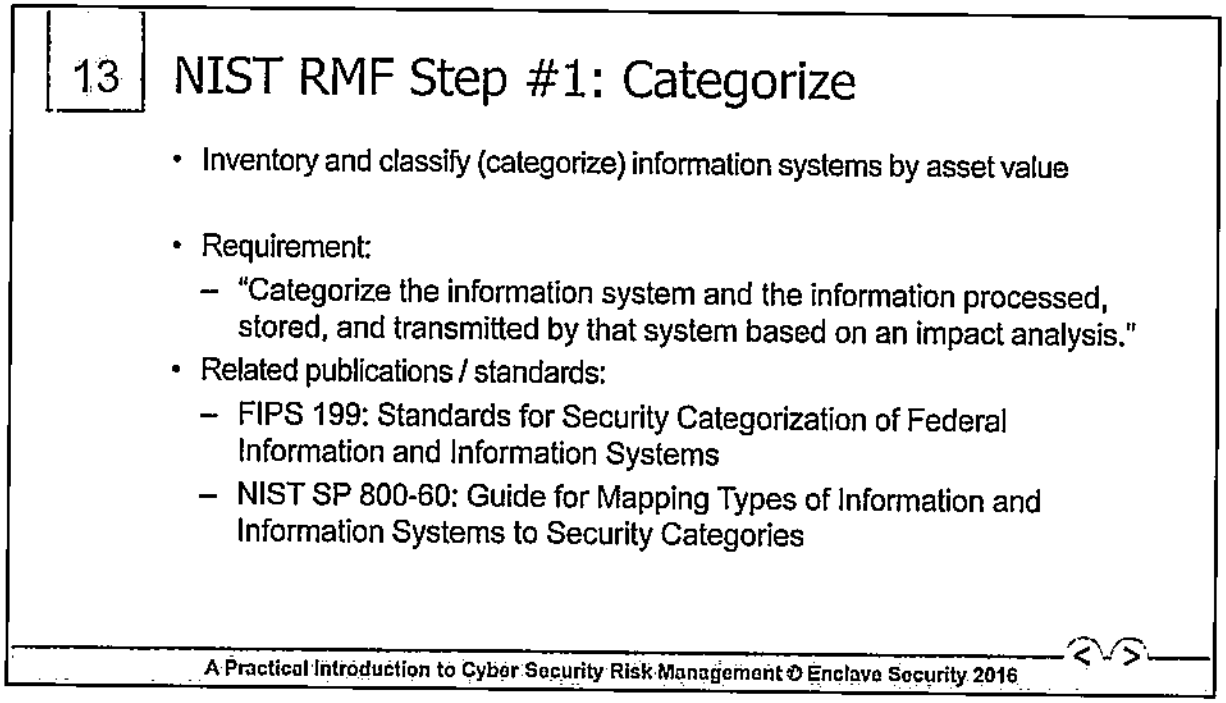


The US Government has also defined a formal risk management model that they have recommended to each of their government agencies to follow as a part of compliance with the Federal Information Systems Management Act (FISMA). The National Institute for Standards in Technology (NIST) has been chartered with the responsibility of maintaining a risk management framework that US federal agencies could utilize in order to defend their information systems. This Risk Management Framework (RMF) is comprised of multiple documents, mostly from their 800 series special publications, which describe the individual components of the RMF.

Specifically in this model there are six steps which federal agencies are expected to follow. Those six steps are:

1. Categorize
2. Select
3. Implement
4. Assess
5. Authorize
6. Monitor

More information on the RMF as a whole can be found at NIST's website at http://csrc.nist.gov/groups/SMA/fisma/framework.html.



The first phase of the model is Categorize, and organizations to meet the goals of this phase are expected to inventory and classify (or categorize) information system by asset value. This is the data classification and inventory phase of the risk assessment.

NIST's requirement for this phase of the Risk Management Framework (RMF) is the following (quoted from http://csrc.nist.gov/groups/SMA/fisma/framework.html):

"Categorize the information system and the information processed, stored, and transmitted by that system based on an impact analysis."

In order to achieve the goals of this requirement, NIST has defined additional FIPS standards and 800 series special publications to clarify specifically instructions. For this phase of the RMF, the following publications are required:

- FIPS 199: Standards for Security Categorization of Federal Information and Information Systems
- NIST SP 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories

NIST RMF Step #2: Select

- Select information assurance defensive controls
- Requirement:
  - "Select an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on organization assessment of risk and local conditions."
- Related publications / standards:
  - FIPS 200: Minimum Security Requirements for Federal Information and Information Systems
  - NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations

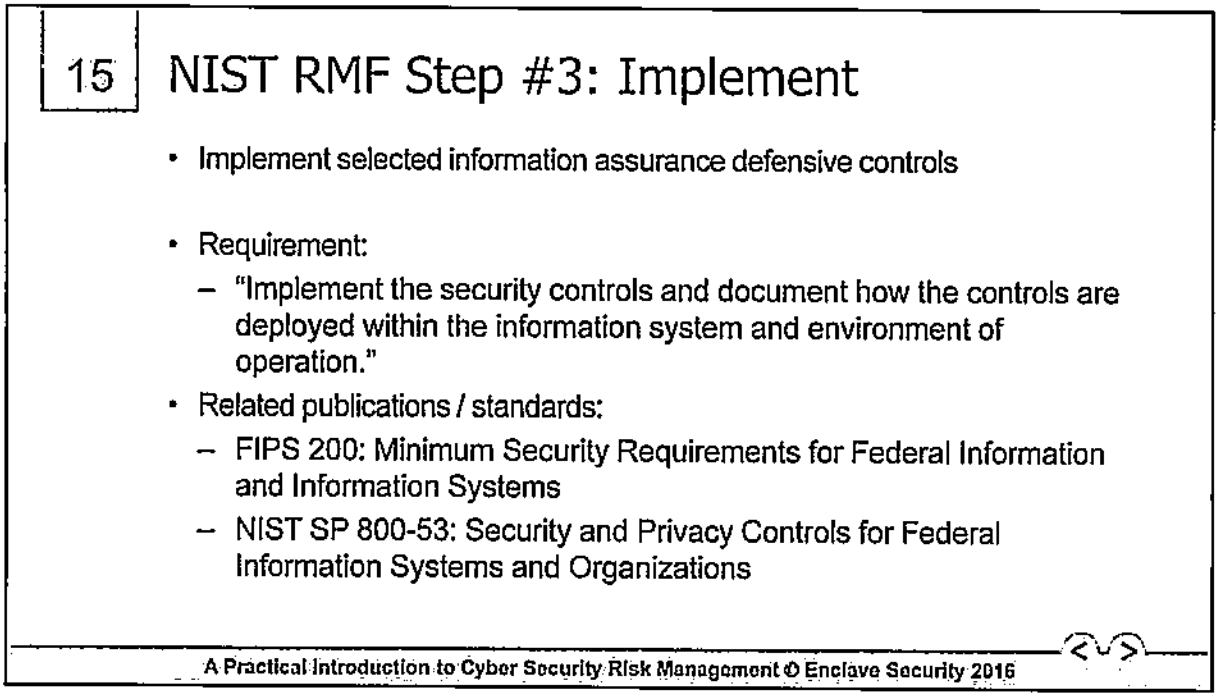
The next phase is the Select phase where organizations are expected to select which controls are best suited to defend the organization's information assets. NIST provides recommendations on how to accomplish this phase through other 800 series special publications.

NIST's requirement for this phase of the Risk Management Framework (RMF) is the following (quoted from http://csrc.nist.gov/groups/SMA/fisma/framework.html):

"Select an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on organization assessment of risk and local conditions."

In order to achieve the goals of this requirement, NIST has defined additional FIPS standards and 800 series special publications to clarify specifically instructions. For this phase of the RMF, the following publications are required:

- FIPS 200: Minimum Security Requirements for Federal Information and Information Systems
- NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations



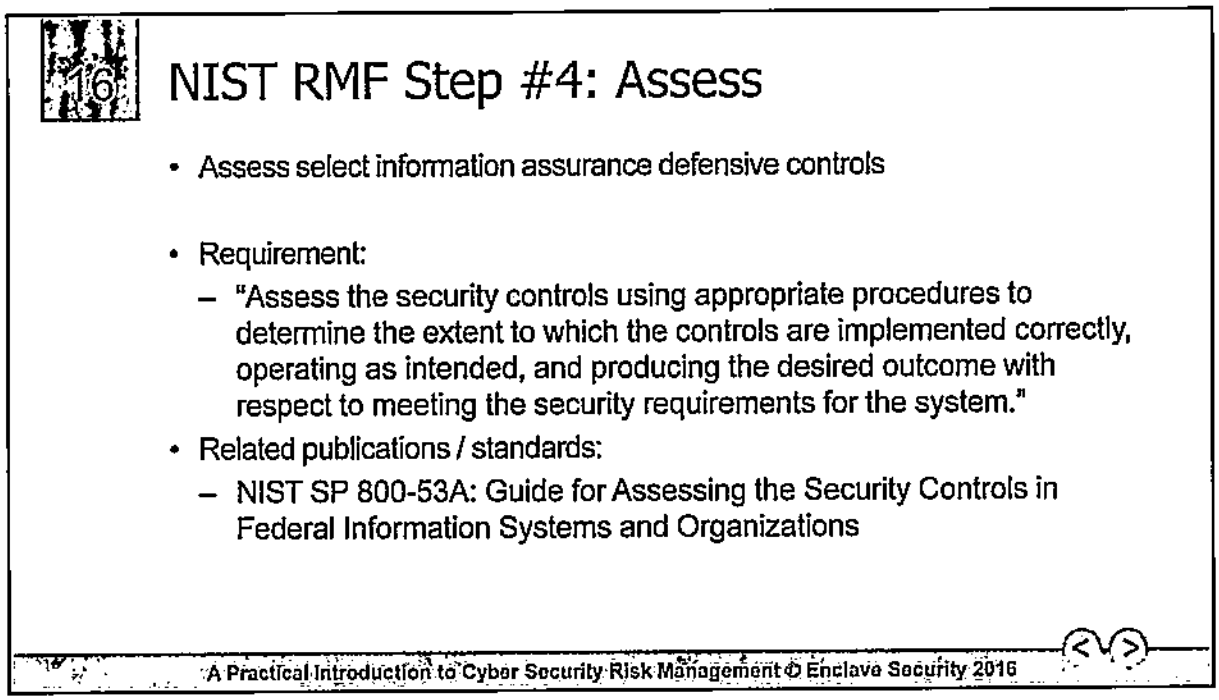
Next, organizations are to Implement the controls that are defined in the previous stage of the methodology. Their responsibility here is to actually do the things that they indicated they would do in the previous stage of the process.

NIST's requirement for this phase of the Risk Management Framework (RMF) is the following (quoted from http://csrc.nist.gov/groups/SMA/fisma/framework.html):

"Implement the security controls and document how the controls are deployed within the information system and environment of operation."

In order to achieve the goals of this requirement, NIST has defined additional FIPS standards and 800 series special publications to clarify specifically instructions. For this phase of the RMF, the following publications are required:

- FIPS 200: Minimum Security Requirements for Federal Information and Information Systems
- NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations



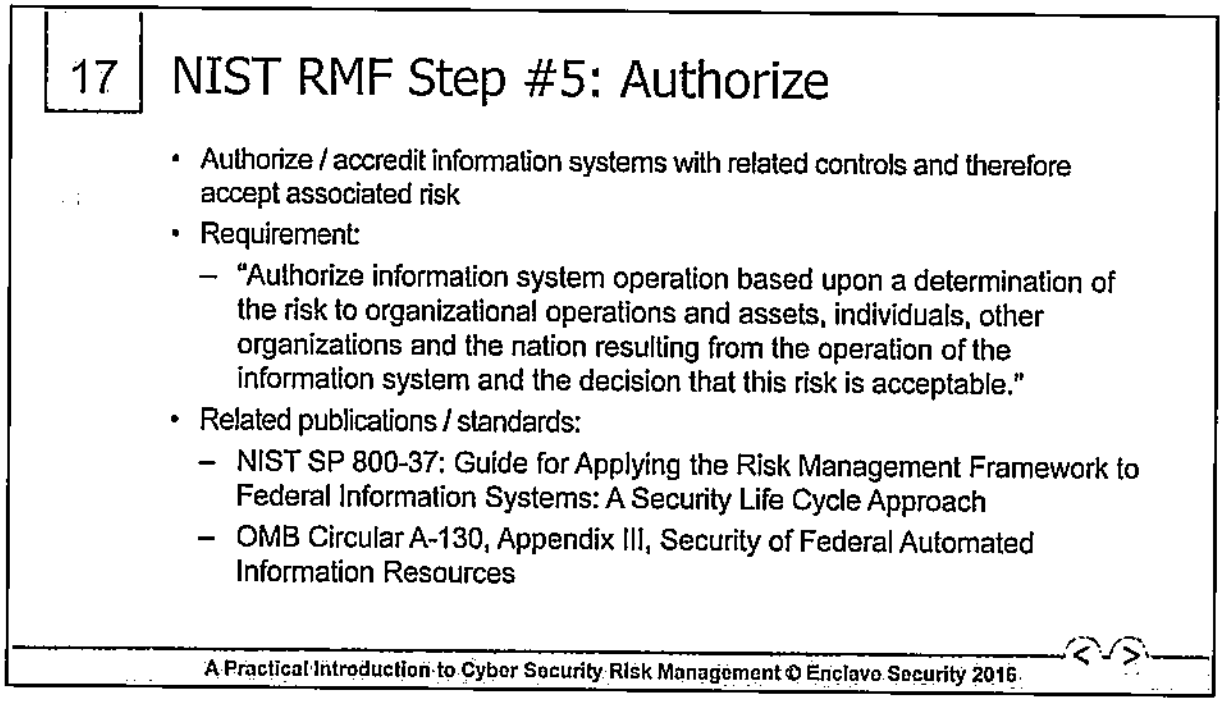
The fourth stage of the process is to Assess the controls that were previously implemented. This phase is the audit and monitoring stage of the framework. The goal is to assess the implementation of the appropriate controls to ensure that they meet the goals defined in previous stages.

NIST's requirement for this phase of the Risk Management Framework (RMF) is the following (quoted from http://csrc.nist.gov/groups/SMA/fisma/framework.html):

"Assess the security controls using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system."

In order to achieve the goals of this requirement, NIST has defined additional FIPS standards and 800 series special publications to clarify specifically instructions. For this phase of the RMF, the following publications are required:

- NIST SP 800-53A: Guide for Assessing the Security Controls in Federal Information Systems and Organizations



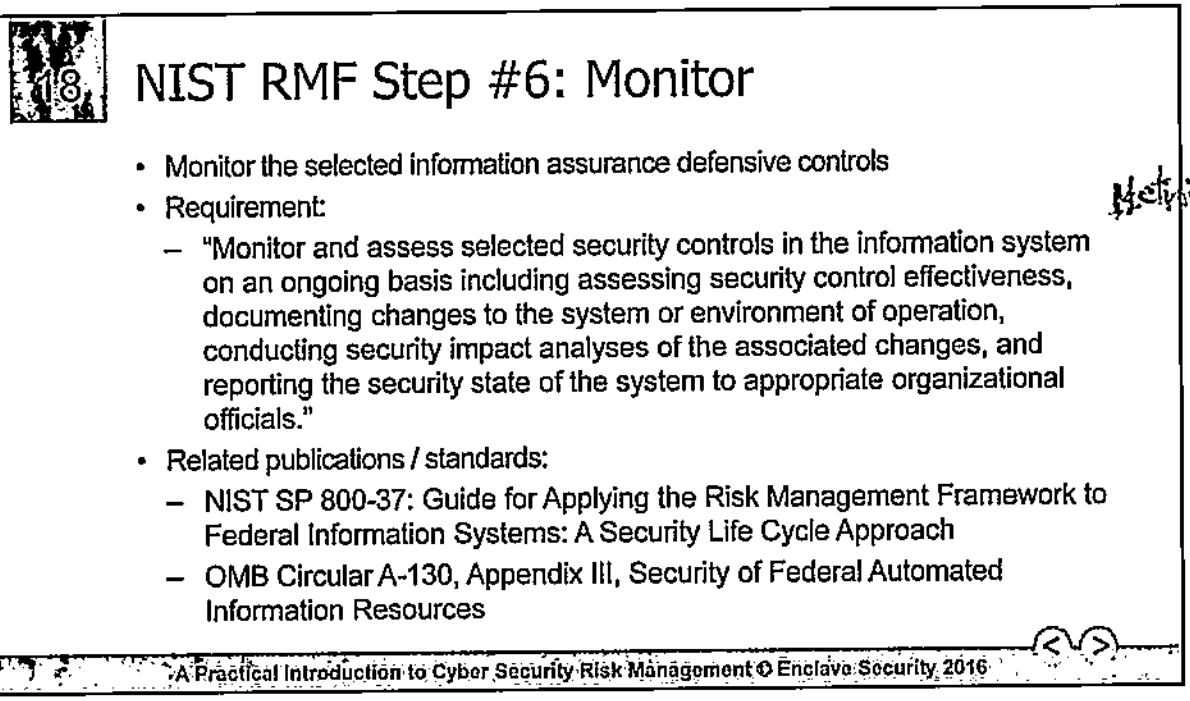
The next stage is the authorization phase where data owners and decision makers authorize / accredit information systems with related controls and therefore accept associated risk. There will be times when sufficient controls are not implemented or resources are not available to completely implement all controls. This phase authorizes those defined exceptions and accepts residual risk levels.

NIST's requirement for this phase of the Risk Management Framework (RMF) is the following (quoted from http://csrc.nist.gov/groups/SMA/fisma/framework.html):

"Authorize information system operation based upon a determination of the risk to organizational operations and assets, individuals, other organizations and the nation resulting from the operation of the information system and the decision that this risk is acceptable."

In order to achieve the goals of this requirement, NIST has defined additional FIPS standards and 800 series special publications to clarify specifically instructions. For this phase of the RMF, the following publications are required:

- NIST SP 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources



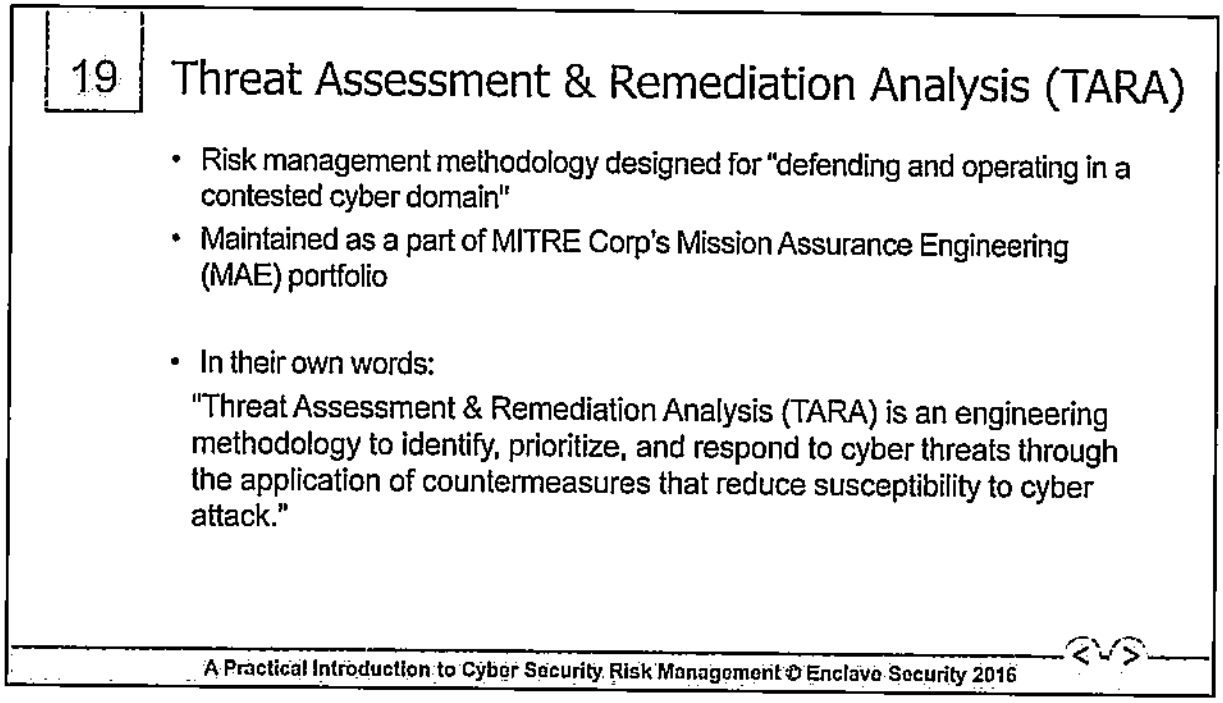
The final stage of the framework is the Monitor stage where organization continue to monitor the controls that were implemented and assessed in previous stages to ensure continued compliance with the controls defined for the organization.

NIST's requirement for this phase of the Risk Management Framework (RMF) is the following (quoted from http://csrc.nist.gov/groups/SMA/fisma/framework.html):

"Monitor and assess selected security controls in the information system on an ongoing basis including assessing security control effectiveness, documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to appropriate organizational officials."

In order to achieve the goals of this requirement, NIST has defined additional FIPS standards and 800 series special publications to clarify specifically instructions. For this phase of the RMF, the following publications are required:

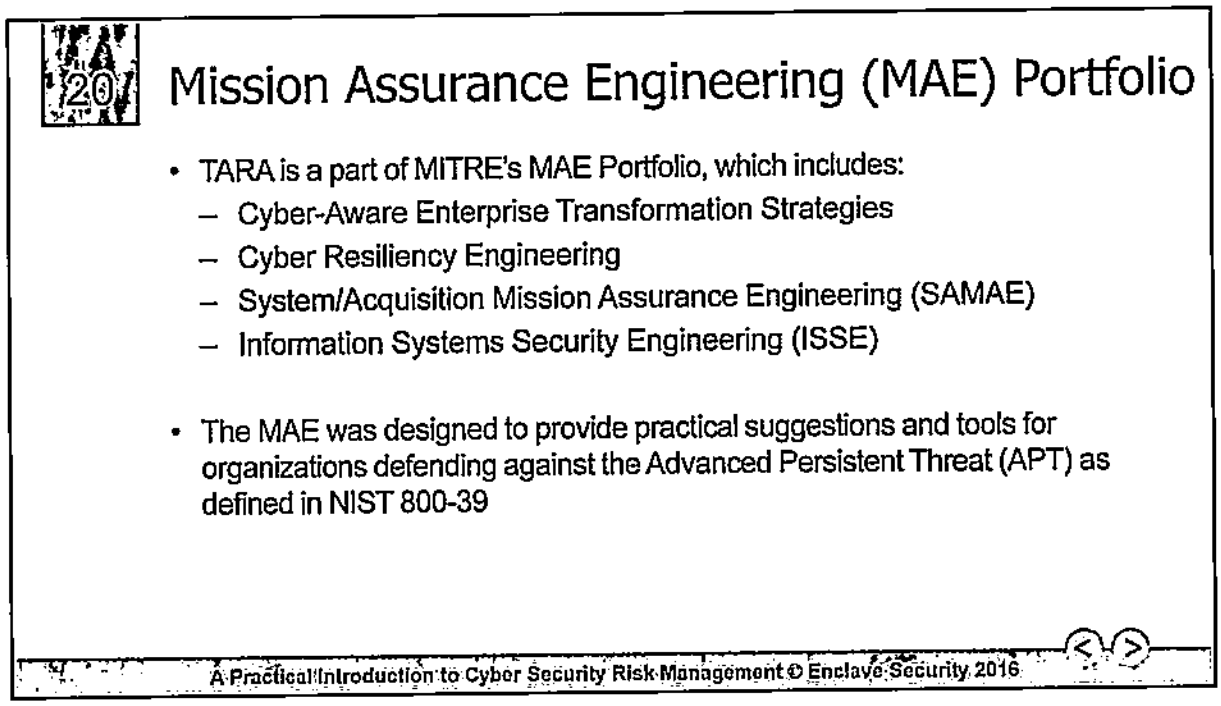
- NIST SP 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources



The Threat Assessment and Remediation Analysis (TARA) risk management model is another methodology that organizations may want to consider as a way to manage risk. TARA was designed as a part of MITRE Corporation's Mission Assurance Engineering (MAE) portfolio for the specific purpose of system defense. Many risk management methodologies were designed generically and later applied to the idea of cyber defense. However this model was designed from the beginning with that in mind.

In their own words, MITRE describes the TARA model as, "Threat Assessment & Remediation Analysis (TARA) is an engineering methodology to identify, prioritize, and respond to cyber threats through the application of countermeasures that reduce susceptibility to cyber attack (http://www.mitre.org/sites/default/files/pdf/11_4982.pdf)."

More information on this risk management model can be found at:
http://www.mitre.org/sites/default/files/pdf/11_4982.pdf



MITRE Corporation's Mission Assurance Engineering (MAE) Portfolio is comprised of a number of elements, including:

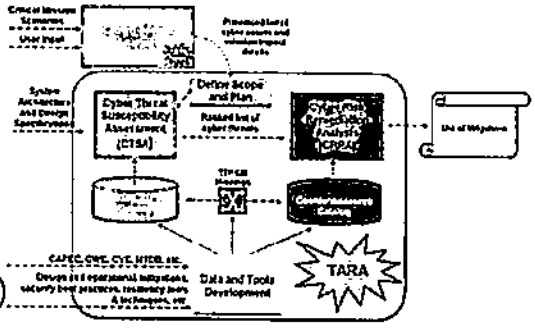
- Cyber-Aware Enterprise Transformation Strategies
- Cyber Resiliency Engineering
- System/Acquisition Mission Assurance Engineering (SAMAE)
- Information Systems Security Engineering (ISSE)

The original idea behind this model was that MITRE wanted to provide specific, actionable steps that an organization could follow in an effort to combat the Advanced Persistent Threat (APT). MITRE observed organizations attempting to defend themselves and created this model and engineering portfolio as a tool that could be practically used for defense. MITRE as a part of this study has references NIST 800-39 repeatedly as their definition of APT and has designed it's methodology with that definition in mind.

21 MITRE's TARA Visualized

- The TARA methodology is composed of:
  1. Crown Jewels Analysis
  2. TARA Assessment
  3. Mitigation Strategies & Activities

- Each TARA Assessment is composed of:
  - Cyber Threat Susceptibility Analysis (CTSA)
  - Cyber Risk Remediation Analysis (CRRA)
  - Data and tools development

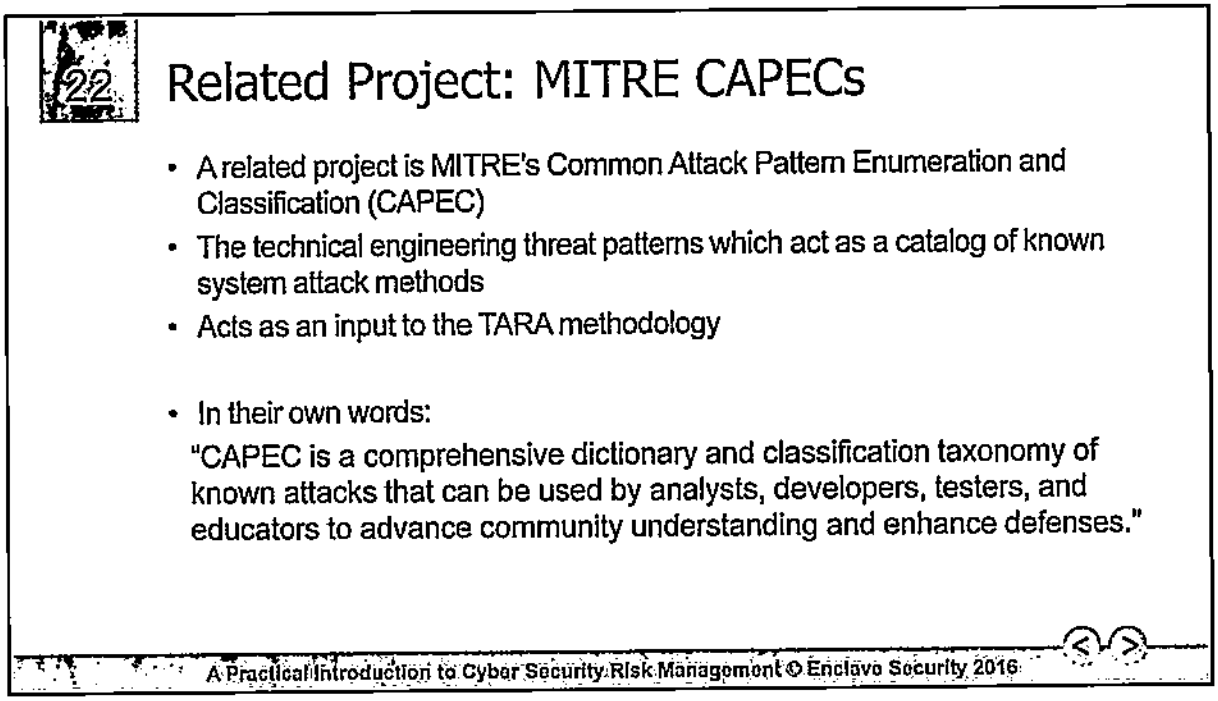


http://www.mitre.org/sites/default/files/pdf/11_4982.pdf

The above screen capture illustrates the various components of the MITRE methodology. The grey box in the center of the diagram outline the components of TARA itself. Those components interact to create the overall process. At a high level that process includes:

- The development of data and tools for the purpose of risk management.
- That development process leads to the creation of an attack catalog (threats) and a countermeasures catalog (controls).
- The attack catalog can then be used to perform a Cyber Threat Susceptibility Assessment (CTSA).
- The countermeasures catalog, with the CTSA, can then be used to perform a Cyber Risk Remediation Analysis (CRRA).
- The CRRA then leads to the definition of a list of practical mitigations that an organization can perform in light of the risk assessment.

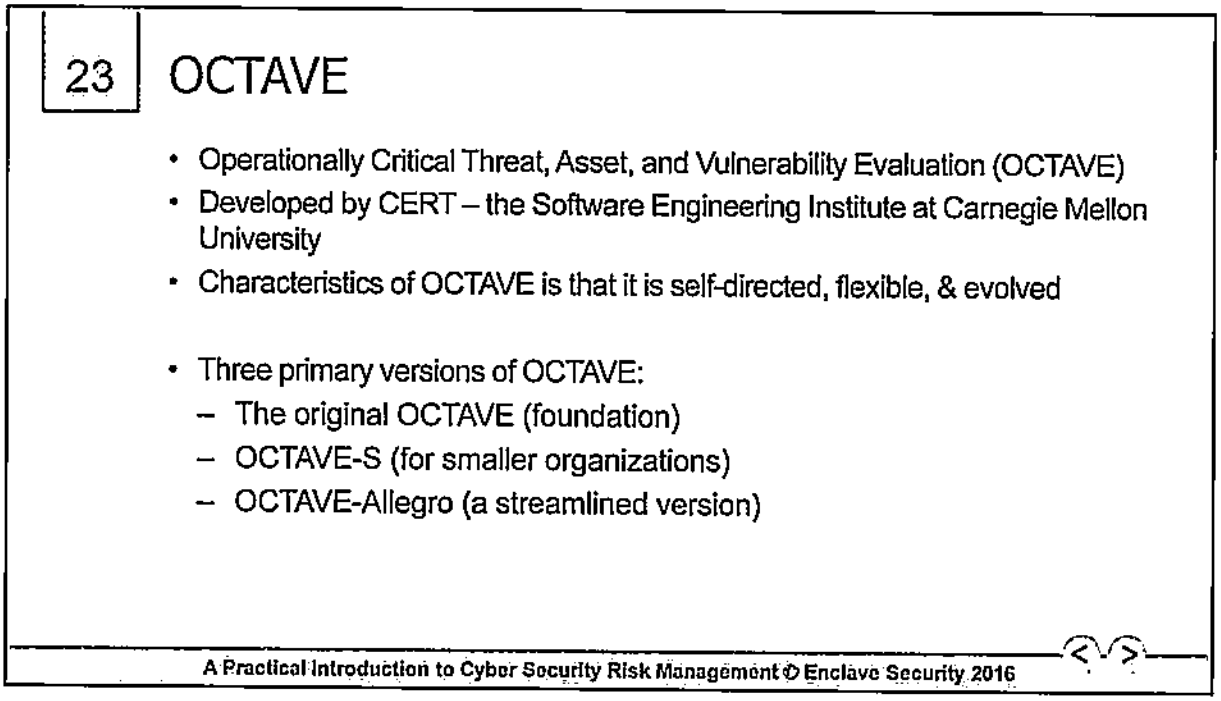
The above graphic / model was taken from MITRE's documentation which can be found at http://www.mitre.org/sites/default/files/pdf/11_4982.pdf



As an input to the TARA risk management methodology, MITRE has also developed a related project known as their Common Attack Pattern Enumeration and Classification (CAPEC) project. These CAPECs is an example of what an organization could utilize as an attack catalog as part of the TARA methodology described earlier. These CAPECs are engineering focused (technical) attack patterns which could be used against an organization's information systems.

In their own words, MITRE describes these CAPECs as:

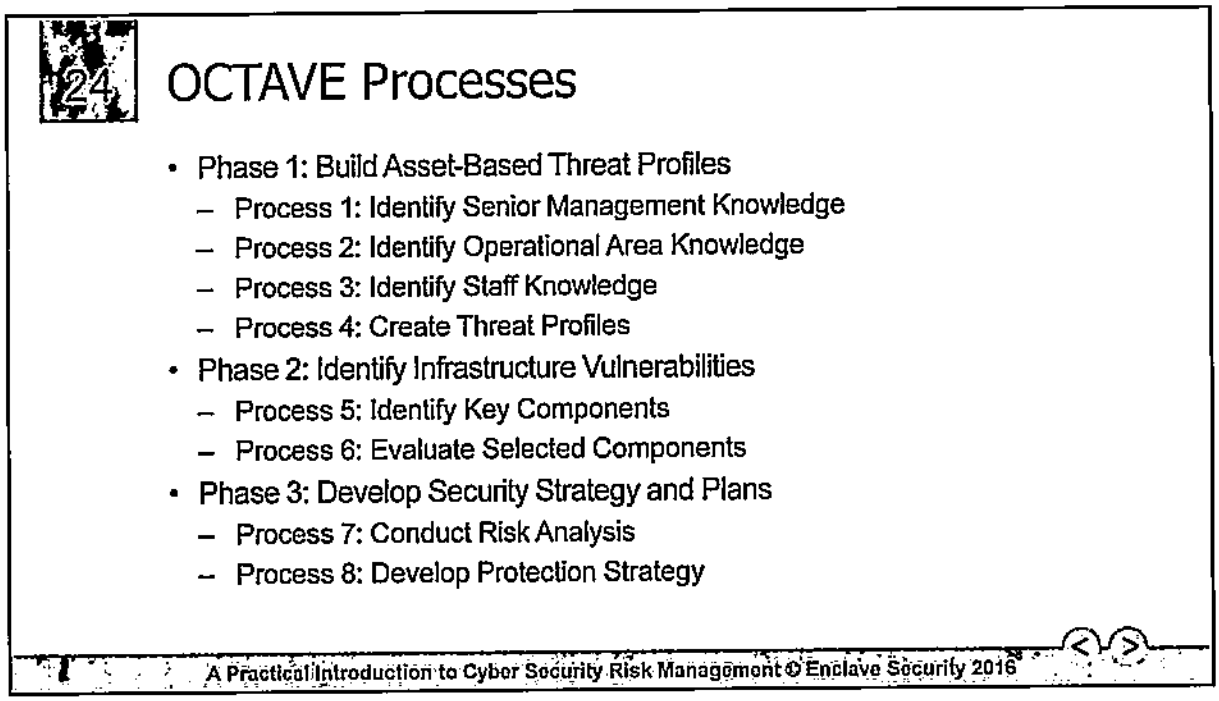
"CAPEC is a comprehensive dictionary and classification taxonomy of known attacks that can be used by analysts, developers, testers, and educators to advance community understanding and enhance defenses (http://capec.mitre.org/)."



One of the more popular risk management approaches comes from CERT and the Software Engineering Institute at Carnegie Mellon University, known as Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE). OCTAVE as a risk framework has been around for quite some time and is used as a formal process by many organizations looking for a more academic, formal approach to risk management. OCTAVE is known as a self-directed, flexible, and evolved framework that can fit itself into multiple organizational information assurance programs – thus a big part of its popularity.

There are different versions of OCTAVE too. The original OCTAVE version is what is known as the OCTAVE foundation. From this model other OCTAVE models have been developed that complement the original and help to apply the standard in specific situations. The two most common branches are OCTAVE-S and OCTAVE-Allegro. OCTAVE-S is meant to be an implementation of the original framework, specifically designed for small businesses looking for a risk framework. OCTAVE-Allegro on the other hand was written as a streamlined version of the original standard in order to make it easier for organizations to take advantage of the tools provided. [1]

[1] OCTAVE® Information Security Risk Evaluation. (n.d.). Welcome to CERT. Retrieved February 1, 2011, from http://www.cert.org/octave



The above outline documents the three phases and eight processes that go into the OCTAVE framework. These are the processes that an organization is expected to follow in order to work through the risk management plan. This framework is very similar to many of the approaches we have discussed in class so far, and certainly the discussions that we have had were influenced by OCTAVE and other standards.

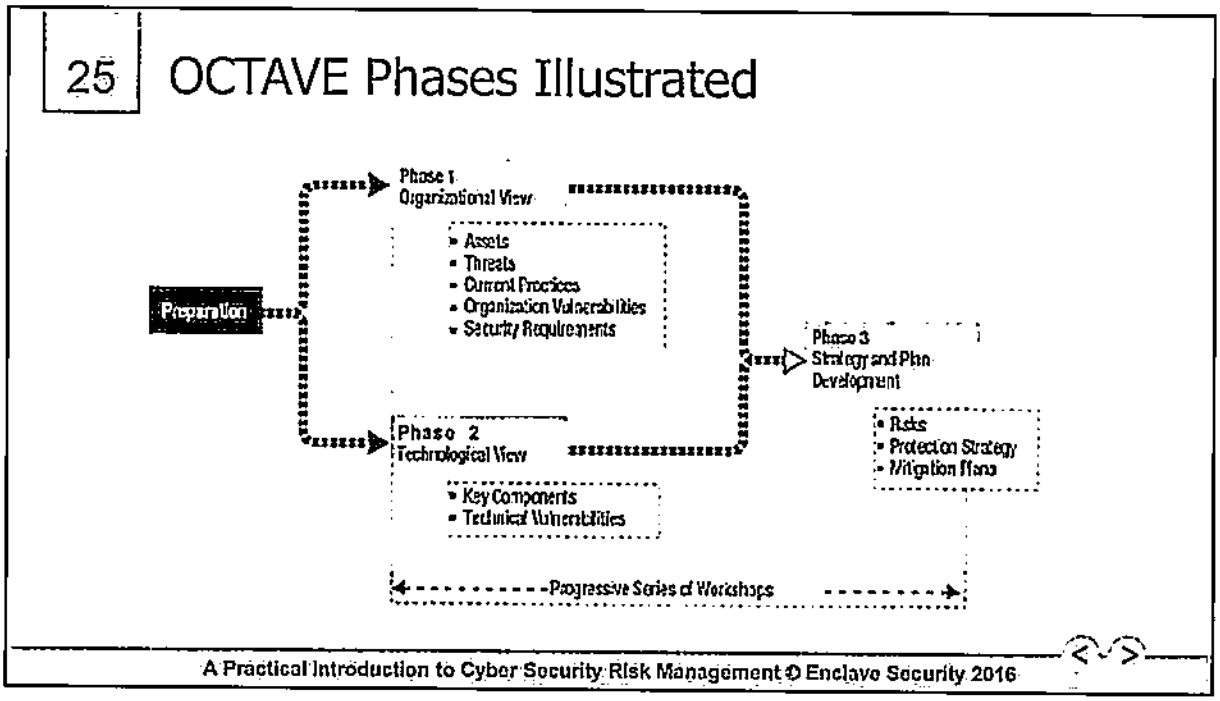
At this point we do not want to address much commentary on the phases and processes of OCTAVE, but we do want students to be exposed to them and start to consider what is included in this approach to risk. Specifically the following phases and processes make up the OCTAVE framework:

Phase 1: Build Asset-Based Threat Profiles
- Process 1: Identify Senior Management Knowledge
- Process 2: Identify Operational Area Knowledge
- Process 3: Identify Staff Knowledge
- Process 4: Create Threat Profiles

Phase 2: Identify Infrastructure Vulnerabilities
- Process 5: Identify Key Components
- Process 6: Evaluate Selected Components

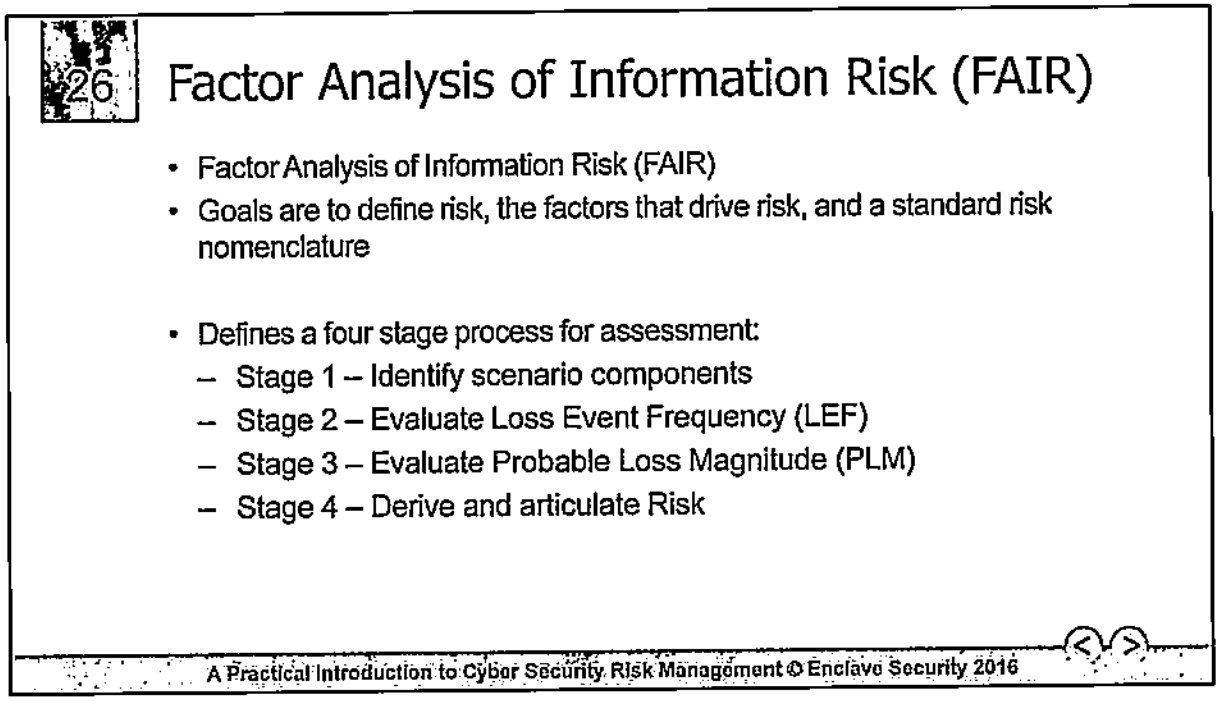
Phase 3: Develop Security Strategy and Plans
- Process 7: Conduct Risk Analysis
- Process 8: Develop Protection Strategy

For more complete information on OCTAVE, the phases, and its processes, please visit http://www.cert.org/octave/methodintro.html



Shown a different way, the above diagram illustrates the phases and processes included in OCTAVE and how they tend to work together to perform risk management. By combining these phases, an organization is able to progress through the process of identifying and remediating risks that are discovered.

This diagram was taken from the OCTAVE website at http://www.cert.org/archive/pdf/07tr012.pdf.



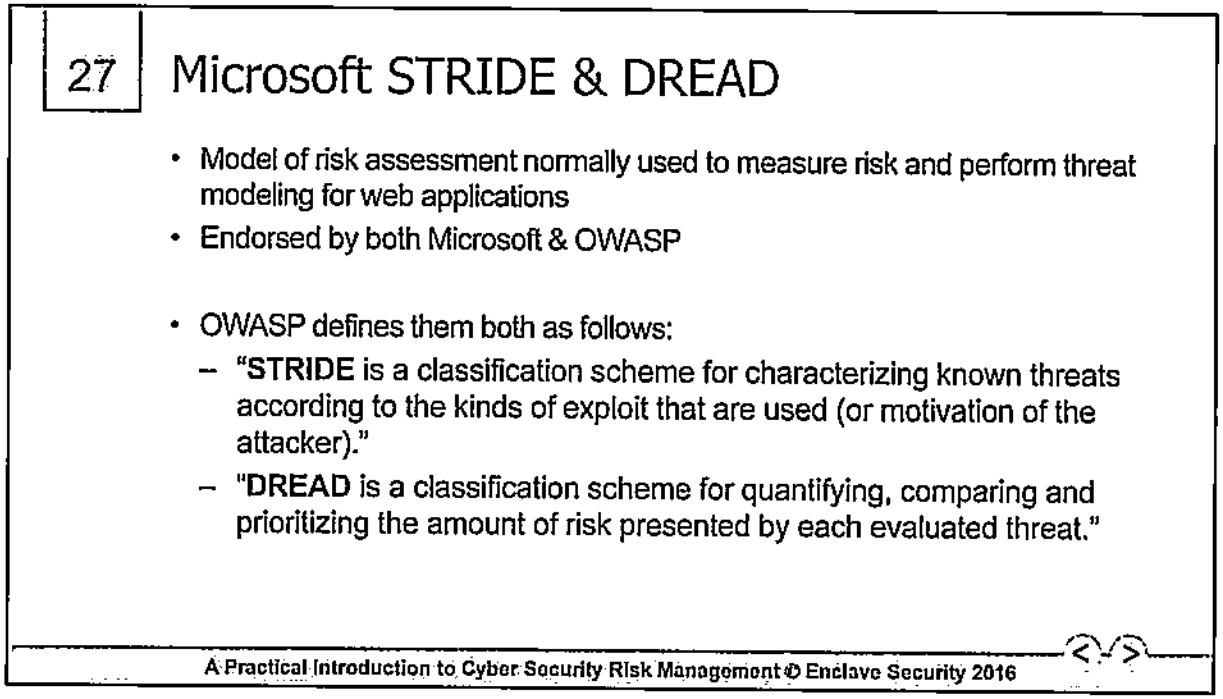
Another risk analysis technique that an organization may consider is what is known as the Factor Analysis of Information Risk (FAIR) model of risk management. In this standard the idea is that goals are to define risk, the factors that drive risk, and standard risk nomenclature. This is meant to make it easier for organizations to apply a consistent method of risk assessment to the different aspects of an organization.

Within the FAIR model there exists a four-stage process for risk assessment. These stages are meant to provide a process for the identification and reporting of risk on an enterprise level. The four stages of risk assessment are:

- Stage 1 – Identify scenario components
- Stage 2 – Evaluate Loss Event Frequency (LEF)
- Stage 3 – Evaluate Probable Loss Magnitude (PLM)
- Stage 4 – Derive and articulate Risk

The hope for students in this class is that by looking at the aspects of various risk assessment and risk management models, the student will be able to be exposed to multiple models and be in a better position to be able to decide which model best suits their organization.

More information on the FAIR model can be reviewed in the model's main document that can be found from the following location:
http://en.wikipedia.org/wiki/Factor_analysis_of_information_risk

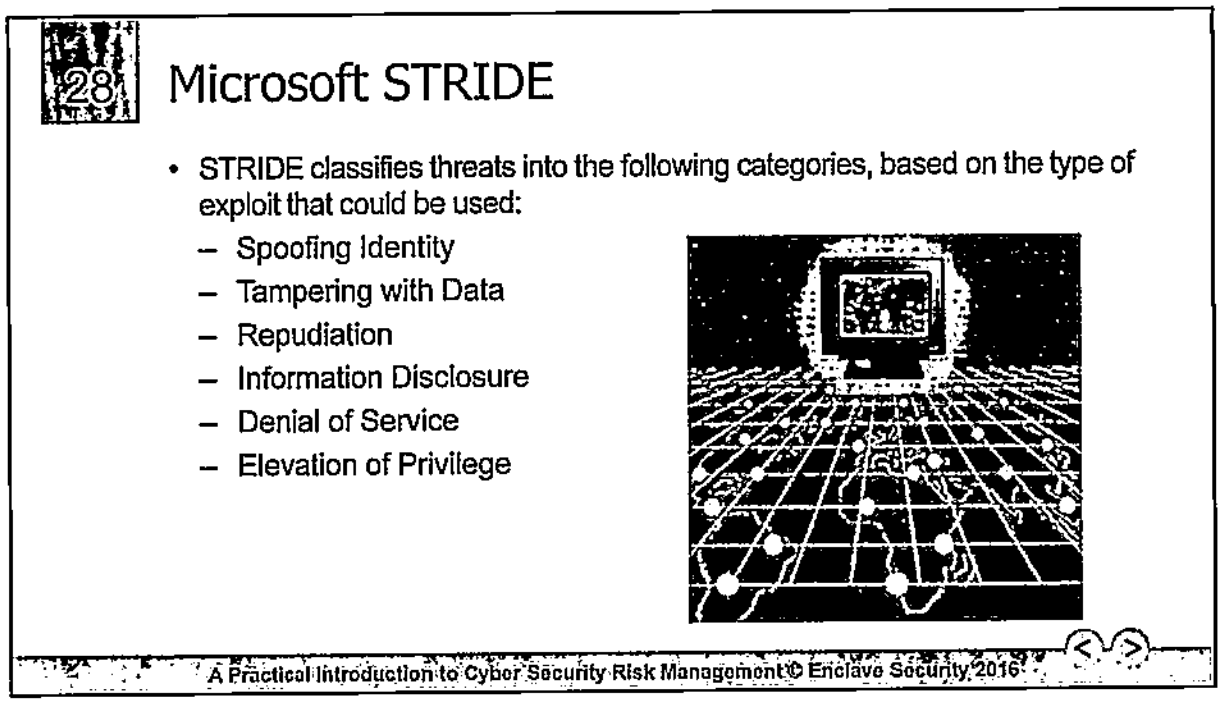


Another form of risk assessment that an organization may consider is what is known as Microsoft's STRIDE and DREAD approach to risk assessment. This model is most often used by developers, web developers specifically, as a model of risk assessment for measuring risk and performing threat modeling for web applications. Both Microsoft and the Open Web Application Security Project (OWASP) have endorsed this approach as a way to address potential threats to applications.

OWASP has given some clear definitions for both of these models. They define them as:

> "**STRIDE** is a classification scheme for characterizing known threats according to the kinds of exploit that are used (or motivation of the attacker)."
> "**DREAD** is a classification scheme for quantifying, comparing and prioritizing the amount of risk presented by each evaluated threat." [1]

[1] Threat Risk Modeling - OWASP. (n.d.). Main Page - OWASP. Retrieved February 1, 2011, from http://www.owasp.org/index.php/Threat_Risk_Modeling



First let us look at STRIDE. STRIDE classifies threats into categories, based on the type of exploit that could be used against the application. As a result it becomes a very threat-centric approach to dealing with risk. Rather than focusing on vulnerabilities which may exist in the system, they focus on the threats that potentially could impact the system and then respond accordingly.

The thought here is that if developers understand the threats facing an application system, then they will be better prepared to write code, introducing fewer vulnerabilities, to make sure those threats are never realized.

Specifically STRIDE is an acronym for the six different threat areas that are the focus of the model. Those six areas are:

- Spoofing Identity
- Tampering with Data
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege [1]

[1] The STRIDE Threat Model. (n.d.). MSDN | Microsoft Development, Subscriptions, Resources, and More. Retrieved February 1, 2011, from http://msdn.microsoft.com/en-us/library/ee823878(CS.20).aspx

29

Microsoft DREAD

- The DREAD Formula is:

Risk_DREAD = (DAMAGE + REPRODUCIBILITY + EXPLOITABILITY + AFFECTED USERS + DISCOVERABILITY) / 5

- Each of the following are given a score between 0-10:
  - Damage Potential
  - Reproducibility
  - Exploitability
  - Affected Users
  - Discoverability

A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

The other piece of the Microsoft & OWASP model is DREAD. This model is more focused on providing metrics for risk values than on determining which threats might be facing a system.

The specific formula for this method is:

(DAMAGE + REPRODUCIBILITY + EXPLOITABILITY + AFFECTED USERS + DISCOVERABILITY) / 5

Damage Potential

If a threat exploit occurs, how much damage will be caused?

0 = Nothing

5 = Individual user data is compromised or affected.

10 = Complete system or data destruction

Reproducibility

How easy is it to reproduce the threat exploit?

0 = Very hard or impossible, even for administrators of the application.

5 = One or two steps required, may need to be an authorized user.

10 = Just a web browser and the address bar is sufficient, without authentication.

Exploitability

What is needed to exploit this threat?

0 = Advanced programming and networking knowledge, with custom or advanced attack tools.

5 = Malware exists on the Internet, or an exploit is easily performed, using available attack tools.

10 = Just a web browser

Affected Users

How many users will be affected?

0 = None

5 = Some users, but not all

10 = All users

Discoverability

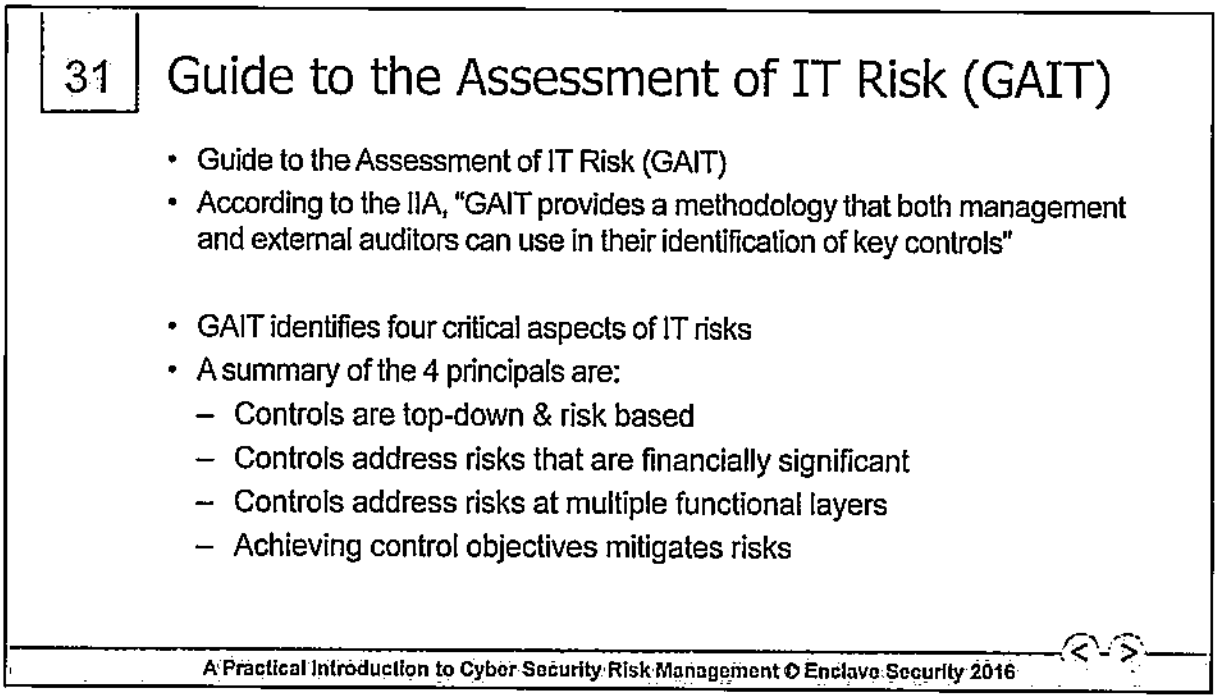
How easy is it to discover this threat?

0 = Very hard to impossible; requires source code or administrative access.

5 = Can figure it out by guessing or by monitoring network traces.

9 = Details of faults like this are already in the public domain and can be easily discovered using a search engine.

10 = The information is visible in the web browser address bar or in a form.



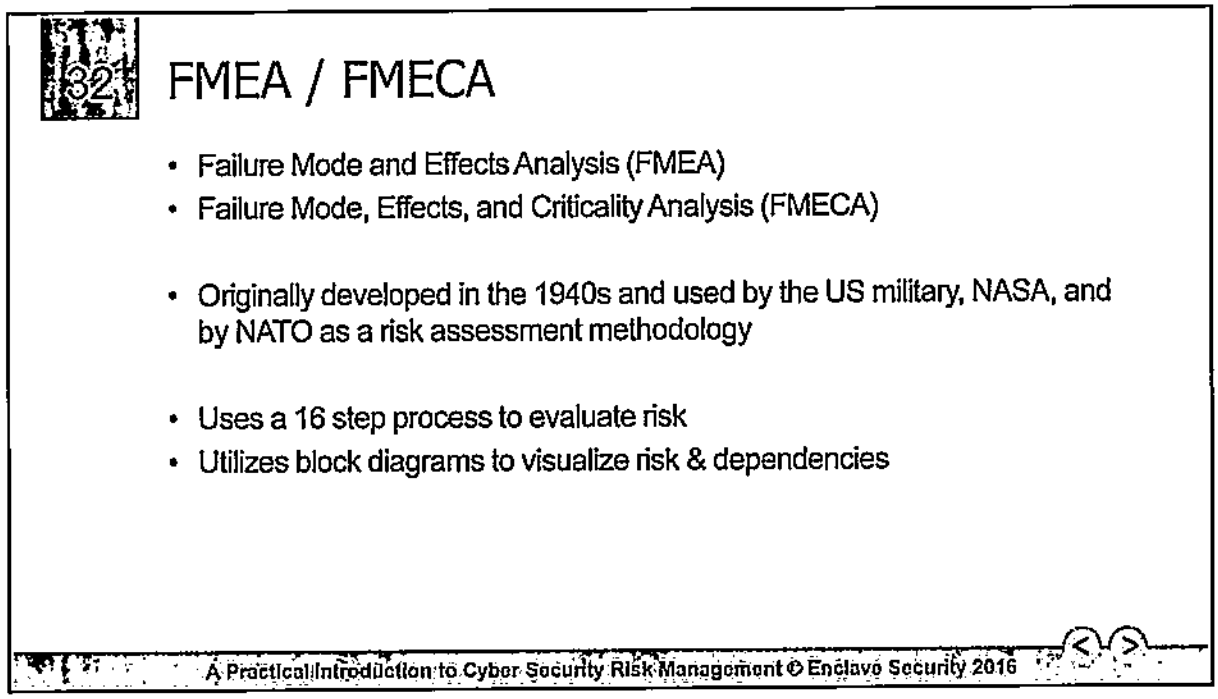
Another model to consider, especially in light of the GTAG standards we discussed earlier in the class is the Guide to the Assessment of IT Risk (GAIT) which is published as a resource by the Institute of Internal Auditors (IIA). According to the IIA,

"GAIT provides a methodology that both management and external auditors can use in their identification of key controls" [1]

The four principles GAIT identifies as the four critical aspects of IT risks are the following:

1. The identification of risks and related controls in IT general control processes (e.g., in change management, deployment, access security, operations) should be a continuation of the top-down and risk based approach used to identify significant accounts, risks to those accounts, and key controls in the business processes.
2. The IT general control process risks that need to be identified are those that affect critical IT functionality in financially significant applications and related data.
3. The IT general control process risks that need to be identified exist in processes and at various IT layers: application program code, databases, operating systems, and network.
4. Risks in IT general control processes are mitigated by the achievement of IT control objectives, not individual controls.

[1] Institute of Internal Auditors Australia - Practice Guides. (n.d.). Voice of the profession: Institute of Internal Auditors - Australia. Retrieved February 1, 2011, from http://www.iia.org.au/Default.aspx?PageID=1953454&A=WebApp&CCID=5016&Page=2&Items=10



Another pair of methods for performing risk management is Failure Mode and Effects Analysis (FMEA) and Failure Mode, Effects, and Criticality Analysis (FMECA). These two management models were originally developed in the 1940s and used by the US military, NASA, and NATO as a risk assessment methodology. In fact these methods were most commonly used for both military and aerospace programs primarily (more than an information assurance model). [1]

These models generally use block diagrams, including both AND and OR visuals to diagram risks and risk dependencies. In that regard this model is very similar in execution to DCCA and event tree methodologies.

"The sixteen steps usually performed in this model are:

1. Define the system
2. Define ground rules and assumptions in order to help drive the design
3. Construct system block diagrams
4. Identify failure modes (piece part level or functional)
5. Analyze failure effects/causes
6. Feed results back into design process
7. Classify the failure effects by severity
8. Perform criticality calculations
9. Rank failure mode criticality
10. Determine critical items
11. Feed results back into design process

12. Identify the means of failure detection, isolation and compensation
13. Perform maintainability analysis
14. Document the analysis, summarize uncorrectable design areas, identify special controls necessary to reduce failure risk
15. Make recommendations
16. Follow up on corrective action implementation/effectiveness"

[1] Failure mode, effects, and criticality analysis - Wikipedia, the free encyclopedia. (n.d.). Wikipedia, the free encyclopedia. Retrieved February 1, 2011, from http://en.wikipedia.org/wiki/Failure_Mode,_Effects,_and_Criticality_Analysis

FMEA / FMECA Severity & Criticality

- They define the following severity levels:
  - Category 1 – Catastrophic
  - Category 2 – Critical
  - Category 3 – Marginal
  - Category 4 – Negligible
- They also define the following criticality levels:
  - Level A – Frequent
  - Level B – Probable
  - Level C – Occasional
  - Level D – Remote
  - Level E – Improbable

FMEA and FMECA specifically define severity levels and criticality levels, which can be used to further define risks. Although many of you in this class may not choose to implement these models whole heartedly, many of you may find the severity and criticality levels useful as you determine what levels you may employ in your organizations.

Specifically the following severity levels are defined within the model:

- Category 1 – Catastrophic
- Category 2 – Critical
- Category 3 – Marginal
- Category 4 – Negligible

In addition, specifically the following criticality levels are defined within the model:

- Level A – Frequent
- Level B – Probable
- Level C – Occasional
- Level D – Remote
- Level E – Improbable

More information on the model, including these severity levels and criticality levels can be found best summarized by Wikipedia at
http://en.wikipedia.org/wiki/Failure_Mode,_Effects,_and_Criticality_Analysis

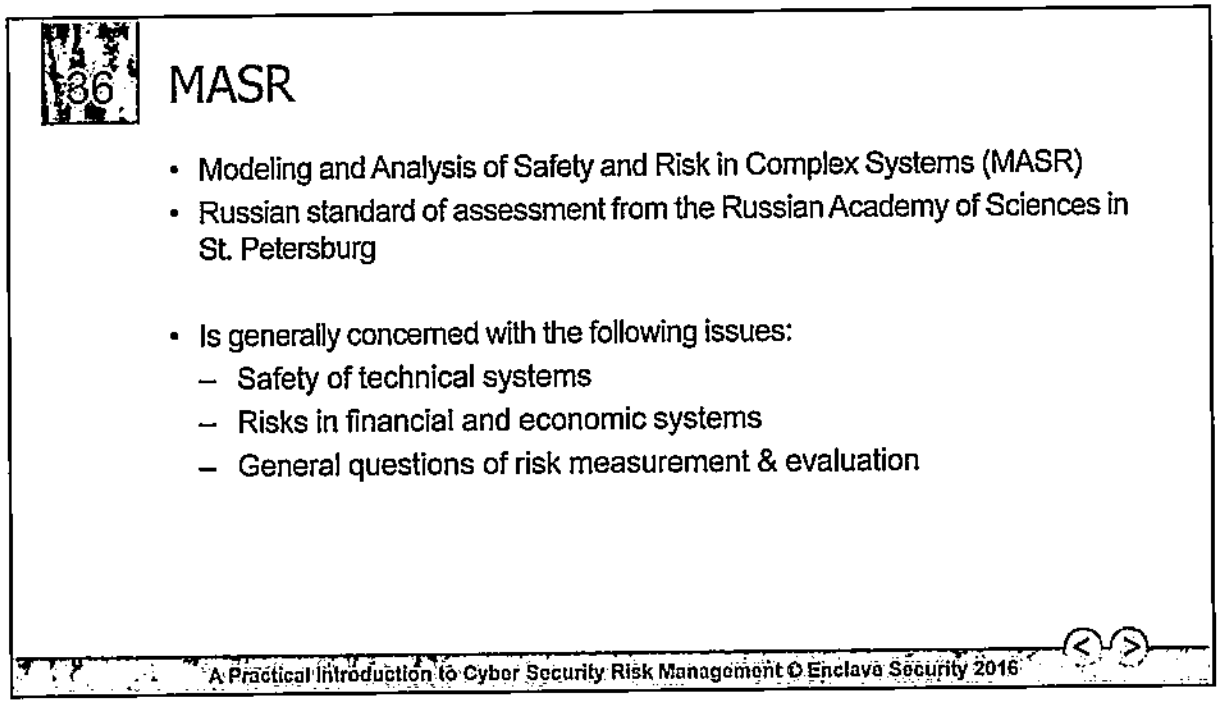
35 Deductive Cause-Consequence Analysis (DCCA)

- A generalization of other risk assessment methods – mostly FMEA & FMECA
- Used to measure safety & control safeguards in critical systems
- Used often in the transportation, aerospace, & similar industries for safety analysis
- Uses AND gates & OR gates to illustrate issues
- Combines the ideas of the following analysis techniques:
  - Fault tree analysis (FTA)
  - Computational tree logic (CTL)

Another model, which to a large degree is based on the principles of FMEA and FMECA, is what is known as Deductive Cause-Consequence Analysis (DCCA). This is a more generalized version of FMEA & FMECA and is used for safety and control safeguards, although not necessarily in a military or aerospace application. It does have a wider view than the original FMEA and FMECA.

Just like the other model, it also uses AND gates and OR gates to illustrate issues in more of a tree like model. It does this by combining the principles of both Fault Tree Analysis (FTA) and Computational Tree Logic (CTL), also known as event tree logic. [1]

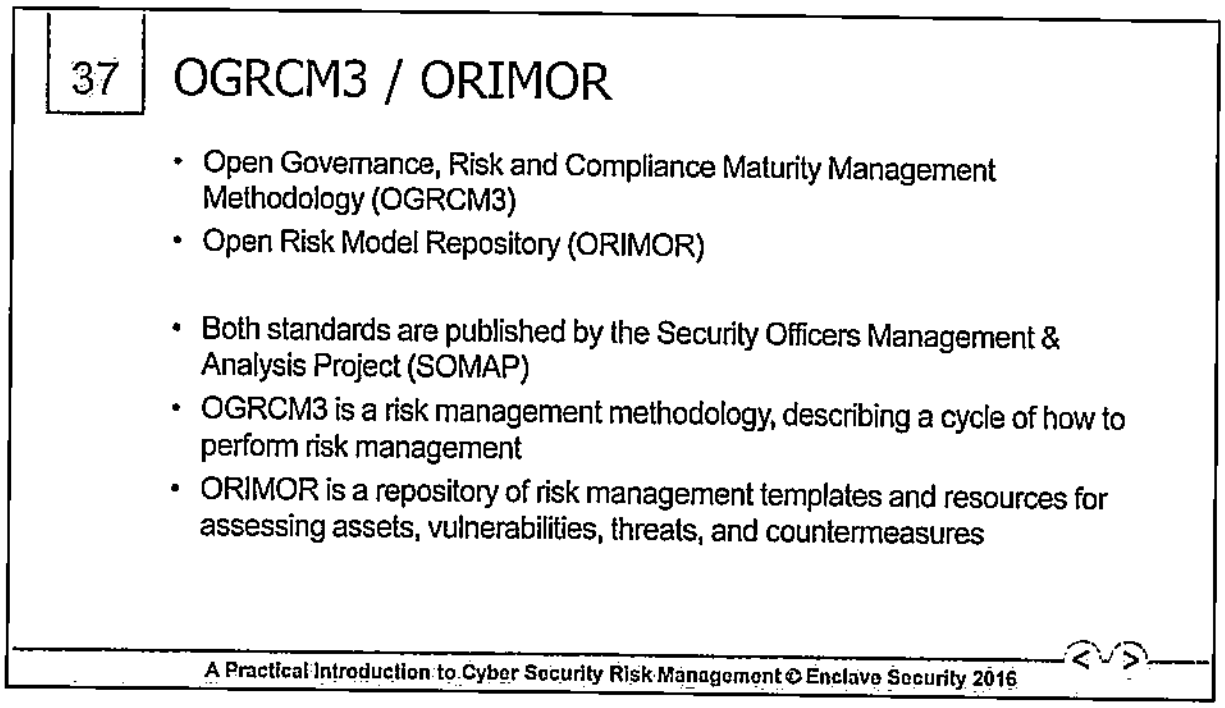
[1] CiteSeerX — Formal safety analysis of a radio based railroad crossing using deductive cause-consequence analysis (DCCA. (n.d.). CiteSeerX. Retrieved February 1, 2011, from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.147.2193



Another standard that might be worth considering is what is known as the Modeling and Analysis of Safety and Risk in Complex Systems (MASR) standard for risk management. This is a Russian standard of assessment from the Russian Academy of Sciences in St. Petersburg. As a result not as many resources currently exist for this standard in English. Most of the available references are available primarily in Russian. [1]

Like DCCA, MASR is also generally concerned with the issue of safety in technical systems. In addition, this model is concerned with risks found in financial systems, economic systems, and general questions of risk measurement and evaluation.

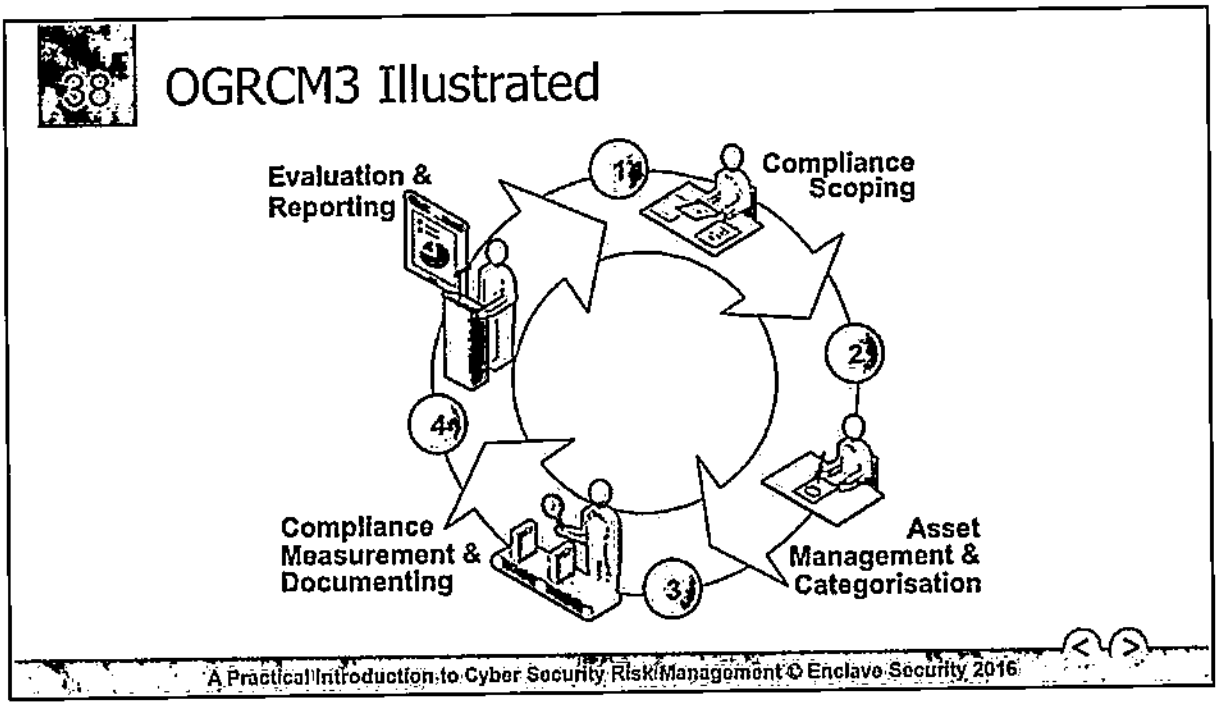
[1] Modeling and Analysis of Safety and Risk in Complex Systems / Proceedings of the Tenth International Scientific School MA SR - 2010 . (2010). Saint-Petersburg, Russia: Russian Academy of Sciences



According to their website, "One of the main goals of the Security Officers Management and Analysis Project (SOMAP.org) is to develop and maintain Open Source Information Security Risk Management documents, tools and utilities." (www.somap.org) Two of the resources provided by this group are the Open Governance, Risk and Compliance Maturity Management Methodology (OGRCM3) and the Open Risk Model Repository (ORIMOR). Both of these resources, along with their ORICO tool, are meant to be free tools to help enterprises manage risk effectively. [1]

OGRCM3 is a risk management methodology, describing a cycle of how to perform risk management. On the next slide we will see this four step methodology and how their cyclical approach functions. ORIMOR is a repository of risk management templates and resources for assessing assets, vulnerabilities, threats, and countermeasures. The ORIMOR templates are meant to serve as templates that organizations can collaborate on in order to create consistent methods for scoring risk across an enterprise.

1 SOMAP.org - Security Officers Management and Analysis Project. (n.d.). SOMAP.org - Security Officers Management and Analysis Project. Retrieved February 1, 2011, from http://SOMAP.org



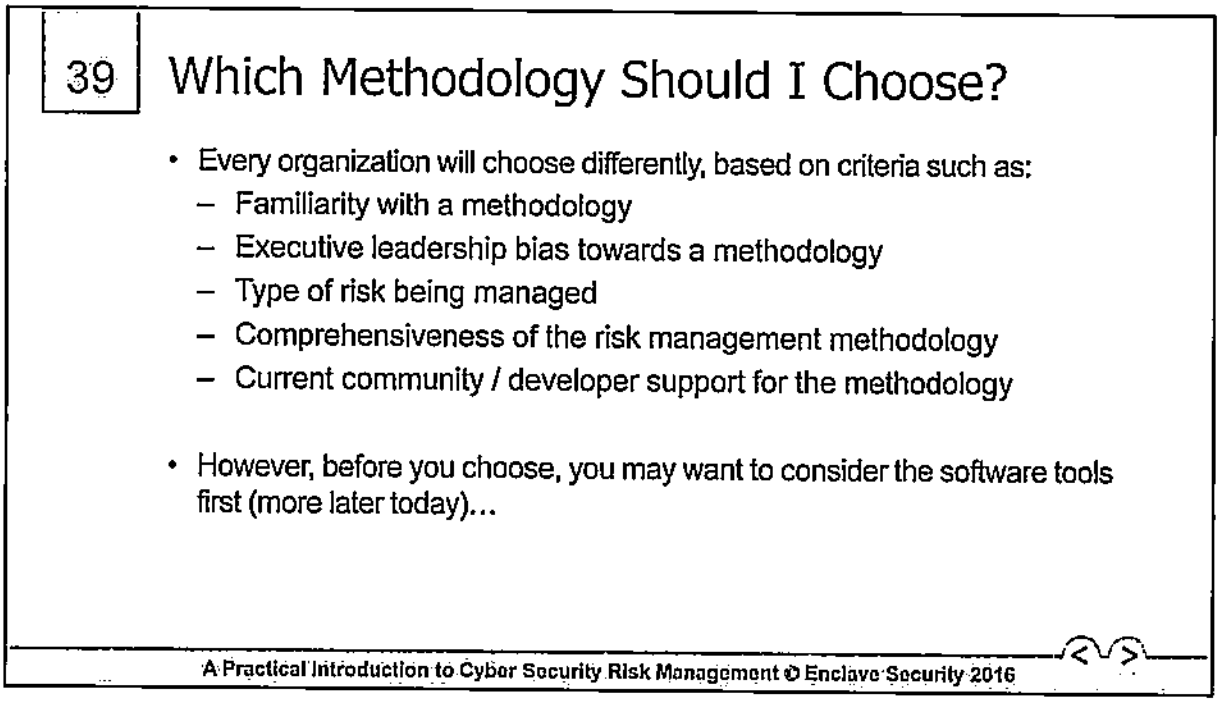
The OGRCM3 framework views risk assessment as a four- step cycle that continuously repeats itself in the organization. The cycle seen above is an illustration from the SOMAP group, which illustrates this cycle. [1]

The four phases of the cycle are:

- Compliance Scoping
- Asset Management & Categorization
- Compliance Measurement & Documentation
- Evaluation & Reporting

The goal is that by consistently working its way through the cycle, an organization will be able to identify and treat risks that are discovered. At the same time, the cycle shows itself to be a continuous monitoring cycle, where continuous process improvement is still the goal.

[1] SOMAP.org - Security Officers Management and Analysis Project. (n.d.). SOMAP.org - Security Officers Management and Analysis Project. Retrieved February 1, 2011, from http://SOMAP.org

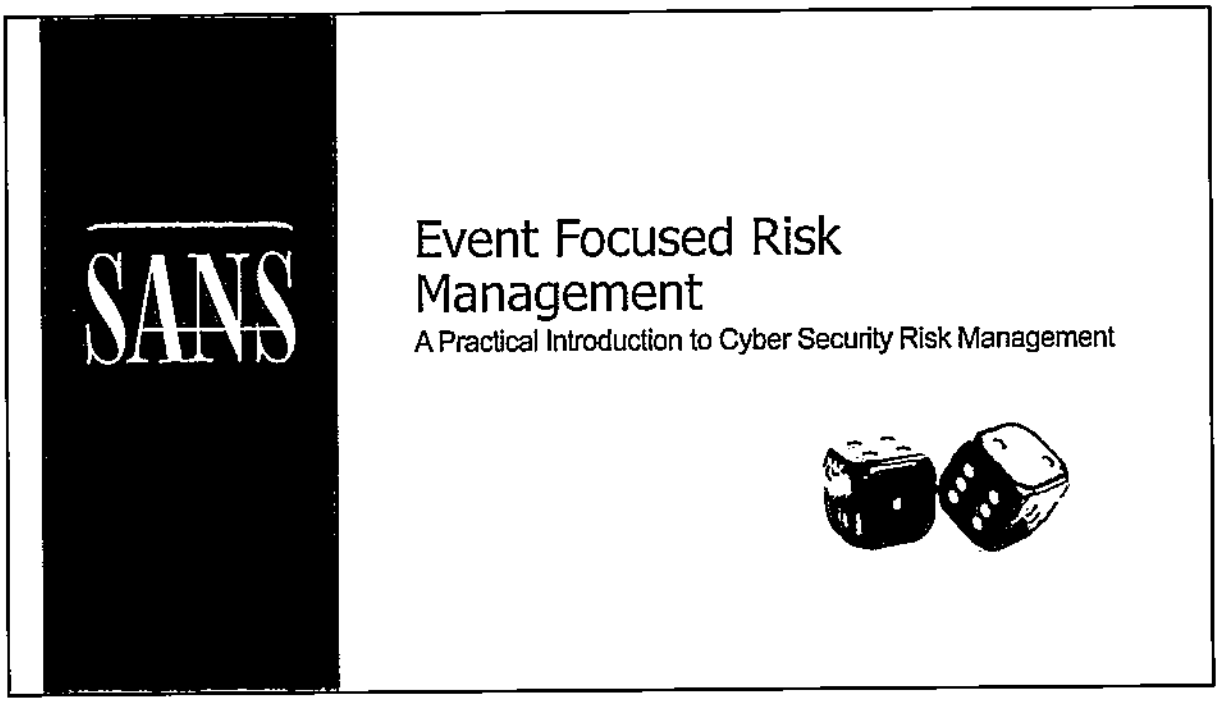


Based on the methodologies we've just seen an organization will want to make a decision which of these models makes the most sense for their business purposes. Every organization will have different business needs and may necessitate the use of one model or another. Sometimes organizations may even be mandated, as in the case of US Government agencies, to use one model over another.

Some of the criteria that an organization might want to consider when making this decision includes:

- Familiarity with a methodology
- Executive leadership bias towards a methodology
- Type of risk being manage
- Comprehensiveness of the risk management methodology
- Current community / developer support for the methodology

Before an organization chooses just one specific risk management methodology, another consideration they should evaluate is how they plan to maintain the data that they gather when using these risk management models. Most likely the organization will want to use a software product to measure this information over time. That being said, next let's take a look at some of the software tools an organization might want to consider as a part of this effort.



This page intentionally left blank.

41

Course Module Roadmap

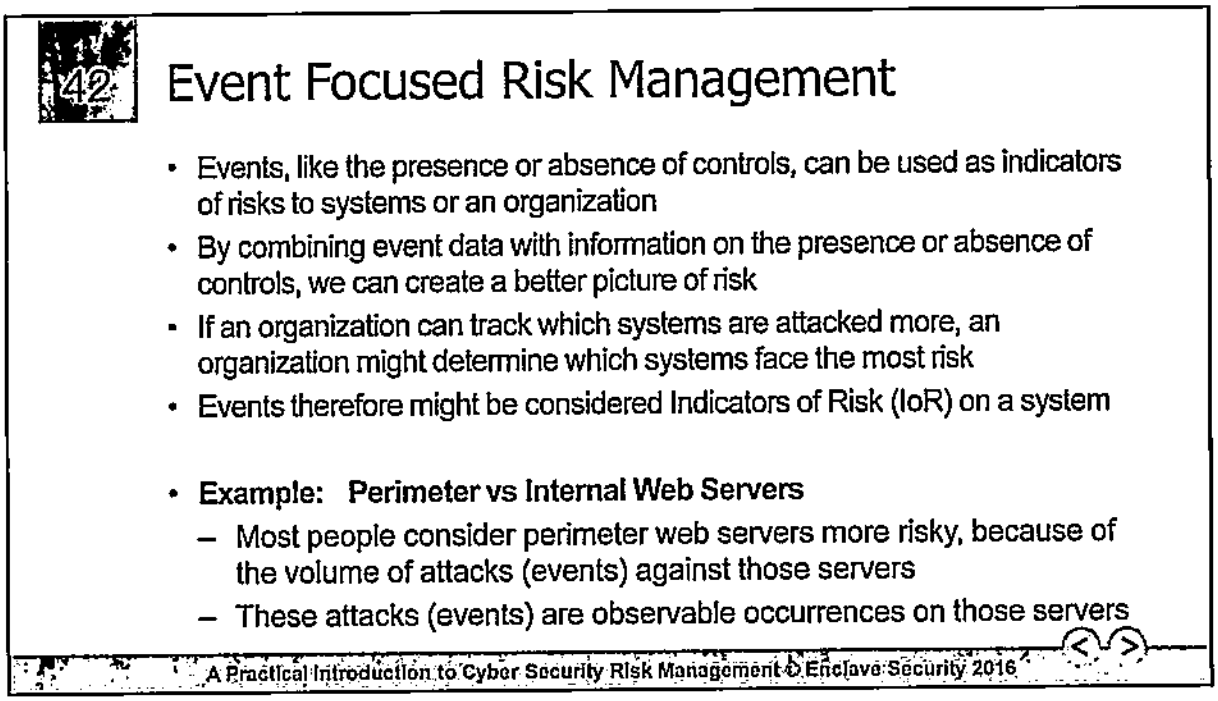
- Understanding Risk ✓
- Control Focused Risk Assessment ✓
- How to Perform a Simple Risk Assessment ✓
- Risk Assessment Case Study ✓
- Formal Risk Management Models & Tools ✓
- Event Focused Risk Management
- Risk Management Case Study
- Risk Management Software
- Risk Remediation & Response

A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

In this course we will explore the concept of risk and its practical impact on an organization. Ultimately the goal of this course is to prepare students to effectively utilize risk assessment as a tool for enterprise defense. Too many times organizations think of risk assessment and risk management as academic tools with little to no practical application. These concepts are often viewed as a formal task to pursue when an organization has free time rather than as a core business activity that drives other enterprise security efforts. In today's course students will have the opportunity to learn about the proper place of risk assessment and risk management in an enterprise. They will also be given practical skills for how to perform a risk assessment on a step by step basis, from data collection to the point of presenting their findings to business leaders. Students with a desire to perform more in depth analysis will also be given tools and formal models to consider to empower them to create a long term / formal risk management program.

Specifically today we will cover the following subjects:

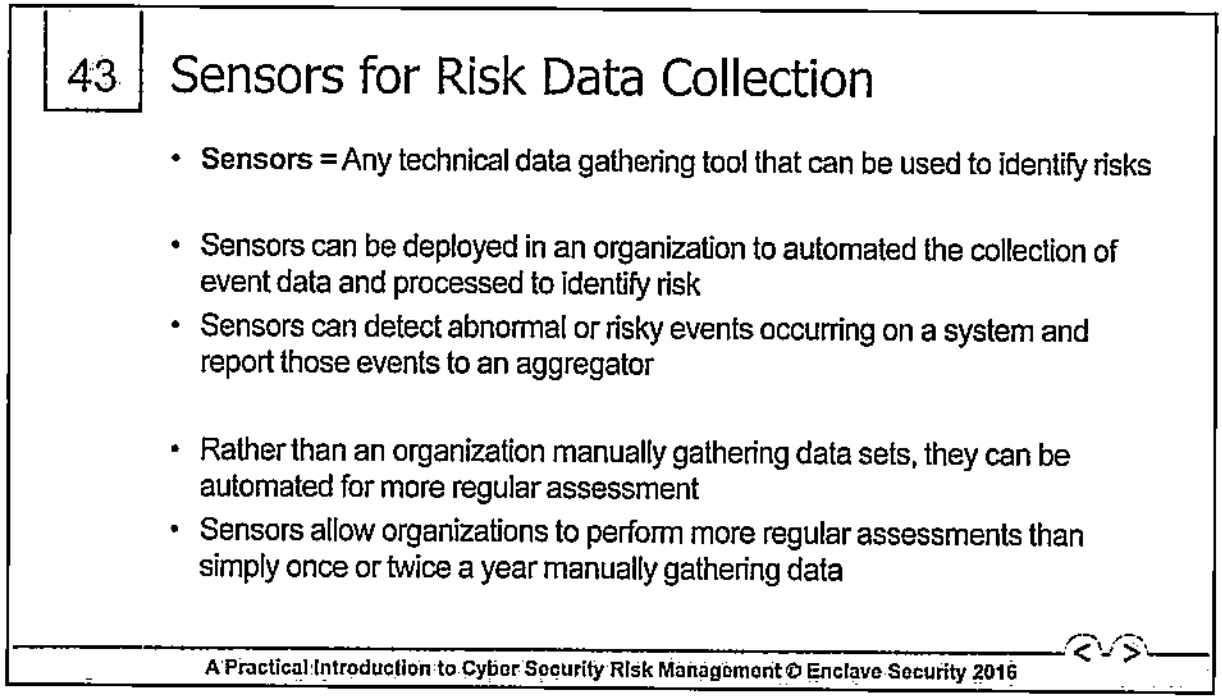
- Understanding Risk
- Control Focused Risk Assessment
- How to Perform a Simple Risk Assessment
- Risk Assessment Case Study
- Formal Risk Management Models & Tools
- Event Focused Risk Management
- Risk Management Case Study
- Risk Management Software
- Risk Remediation & Response



The presence or absence of controls is not the only thing that can quantify risk for an organization. Events occurring on systems can also be used as indicators of risk in an environment. If an organization can combine data points on the presence or absence of controls with the volume of events that occur on a system, it may help the organization to better prioritize responses to risks.

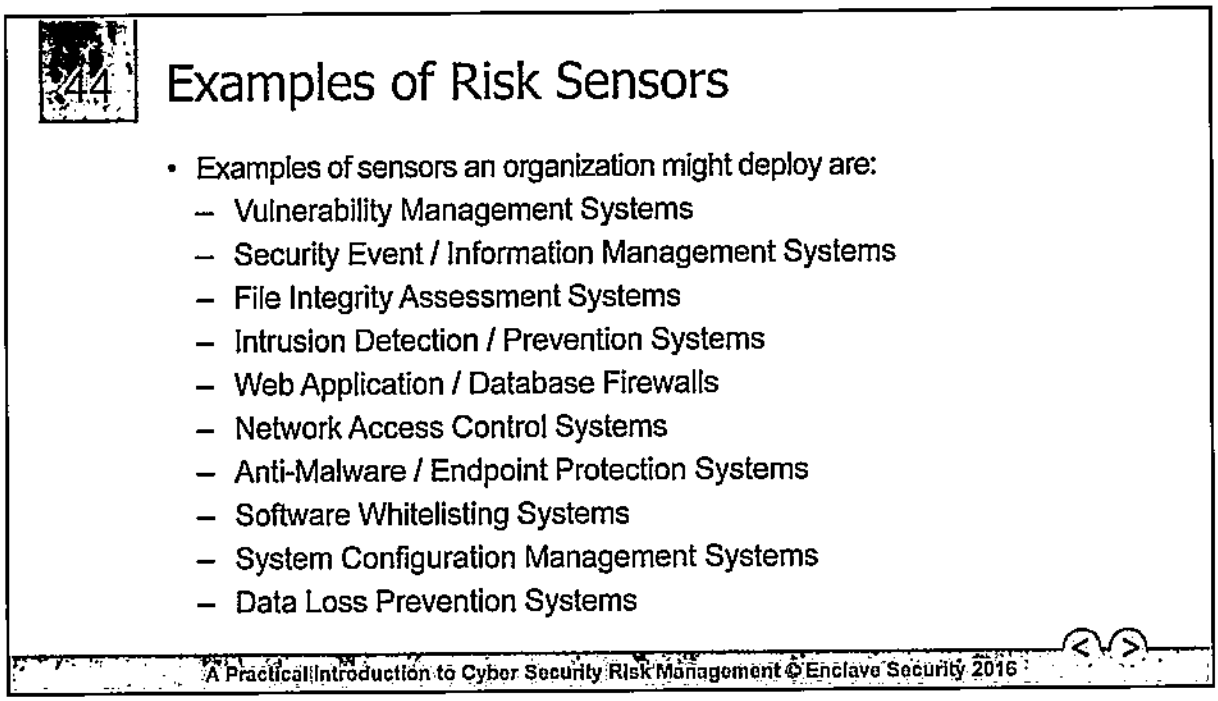
Anecdotally organizations may know that publically facing web servers are more vulnerable to attack than internally facing web servers. But this is based on logic, common sense, and architectural principles rather than on hard data. If instead of relying on these softer data points we could measure the volume of attacks against both types of servers, then organizations would not only be able to quantify the difference, but they could also measure the impact of additional controls to the attack surface of the system.

In addition, if there are ten web servers, for example, in a public facing system how would an organization know which of those ten servers needed the most priority? The same would be true for internally facing systems. The more data points an organization is able to collect, the more precise their response becomes.



One of the primary methods organization have for collecting event based data sets is to deploy technical security sensors that can be used to measure and identify potential risks. Sensors can be deployed to process events, consolidate data sets, and even detect anomalies against a standard baseline. This information can then be used to alert an organization to potential risks they may face. These sensors also move an organization into a more quantifiable mode of risk analysis.

By deploying technical sensors, the organization can automate the process of data collection and create an architecture to consolidate and analyze event data in business terms. This is also the first step towards creating the security dashboards that are the vision of many executive security sponsors. This process allows organizations to continuously monitor their organizations for potential risks rather than limiting them to sporadic assessments throughout a one or five year period, thus giving the organization access to actionable intelligence on a more frequent basis.



There are a number of sensors that an organization might deploy in order to gather this type of data from their systems. Each organization will use different vendors and software solutions, but ideally they could document the data sets they're hoping to collect and then match that with a sensor that they have deployed to collect the information. Examples of a few sensors that an organization may want to consider are:

- Vulnerability Management Systems
- Security Event / Information Management Systems
- File Integrity Assessment Systems
- Intrusion Detection / Prevention Systems
- Web Application / Database Firewalls
- Network Access Control Systems
- Anti-Malware / Endpoint Protection Systems
- Software Whitelisting Systems
- System Configuration Management Systems
- Data Loss Prevention Systems

Organizations may also want to consider interoperability when selecting vendors in these spaces. Ideally each would have the ability to output data in a standardized or parsable format such as XML in order to facilitate the exchange of information between systems.

45 Sample Sensor – Microsoft LogParser (1)

- One sample sensor that can be used to process event data for risk assessment is Microsoft's free LogParser tool
- Data from this tool can be added to control based data for enhanced risk analysis and reporting

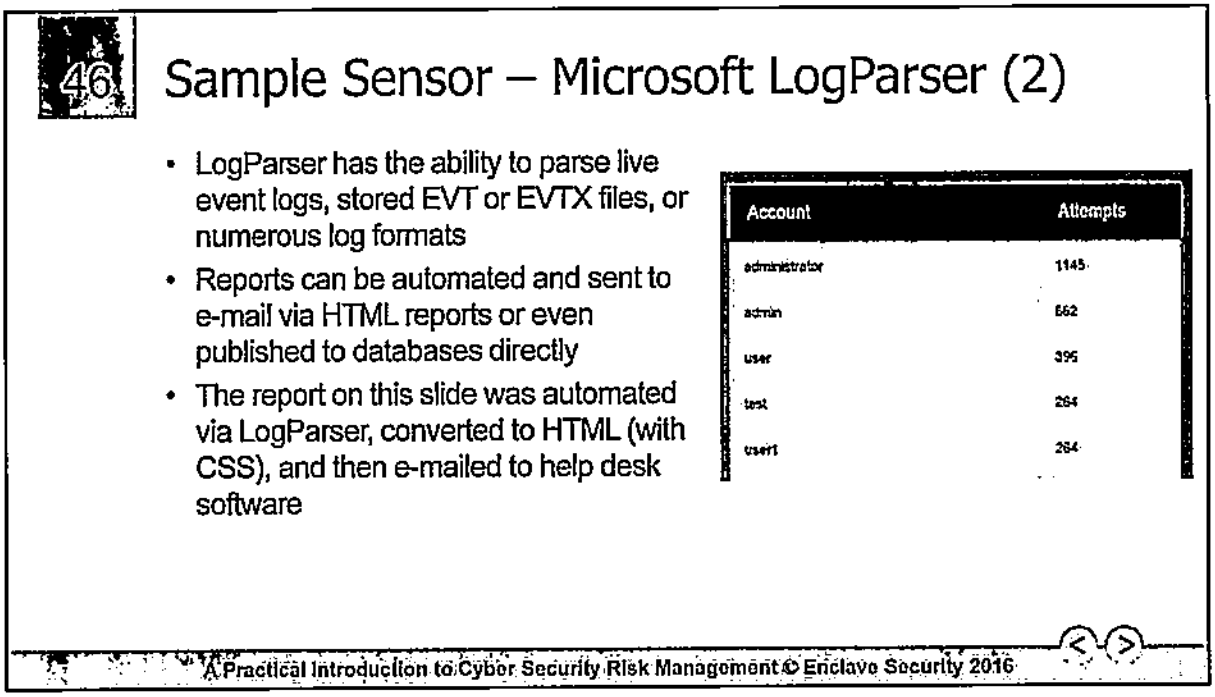
- Command line tool for parsing and reporting on data from various log formats (Microsoft, Unix, network devices, etc.)
- Graphical wrapper also available, LogParser Lizard

- Free download from Microsoft's website at:
  - http://www.microsoft.com/en-us/download/details.aspx?id=24659

One software tool that is a simple, free example of a sensor that an organization might consider is Microsoft's LogParser utility. This utility is a free utility that is distributed by Microsoft to help organizations to automate the process of log analysis. This tool is not an log aggregator. Any organization deploying this tool will need to first determine which logs they want to collect and although it is not a necessity, it is certainly easier to use if the logs are aggregated or at least easy to reach. Once the utility has access to the logs, then it can be used to automate analysis of the logs in order to identify specific Indicators of Risk.

This is also a command line utility that has the ability to parse logs in a number of different formats. The log formats are not simply limited to Microsoft systems, but instead can analyze Unix, network device, or logs from any other standard system. There is even a graphical tool that an organization can use to parse logs on the fly, called LogParser Lizard – which has both a free and commercial version available.

More information on the tool, including the download, can be found at http://www.microsoft.com/en-us/download/details.aspx?id=24659.



As noted previously, LogParser has the ability to parse logs from a number of different formats. For example, for Microsoft Windows servers it has the ability to parse live Event Logs or stored event logs in EVT or EVTX formats. In addition to these formats, it has the ability to parse the following formats (and many more):

- IIS Log File Input Formats
  - IISW3C: parses IIS log files in the W3C Extended Log File Format.
  - IIS: parses IIS log files in the Microsoft IIS Log File Format.
  - BIN: parses IIS log files in the Centralized Binary Log File Format.
  - IISODBC: returns database records from the tables logged to by IIS when configured to log in the ODBC Log Format.
  - HTTPERR: parses HTTP error log files generated by Http.sys.
  - URLSCAN: parses log files generated by the URLScan IIS filter.

- Generic Text File Input Formats ◦CSV: parses comma-separated values text files.
  - TSV: parses tab-separated and space-separated values text files.
  - XML: parses XML text files.
  - W3C: parses text files in the W3C Extended Log File Format.
  - NCSA: parses web server log files in the NCSA Common, Combined, and Extended Log File Formats.
  - TEXTLINE: returns lines from generic text files.
  - TEXTWORD: returns words from generic text files.

- System Information Input Formats •EVT: returns events from the Windows Event Log and from Event Log backup files (.evt files).
  - FS: returns information on files and directories.
  - REG: returns information on registry values.
  - ADS: returns information on Active Directory objects.

- Special-purpose Input Formats •NETMON: parses network capture files created by NetMon.
  - ETW: parses Enterprise Tracing for Windows trace log files and live sessions.
  - COM: provides an interface to Custom Input Format COM plug-ins."

(List taken from http://blogs.msdn.com/b/robert_mcmurray/archive/2012/05/25/advanced-log-parser-charts-part-4-adding-custom-input-formats.aspx).

The graphic on the screen represents an automated e-mail generated by LogParser after analyzing a set of stored EVTX files. This report illustrates the tool analyzing a Security Log for failed logon attempts – which then sorts the number of unsuccessful logons by attempts and alerts the system administrators.

Risk Management / Continuous Monitoring

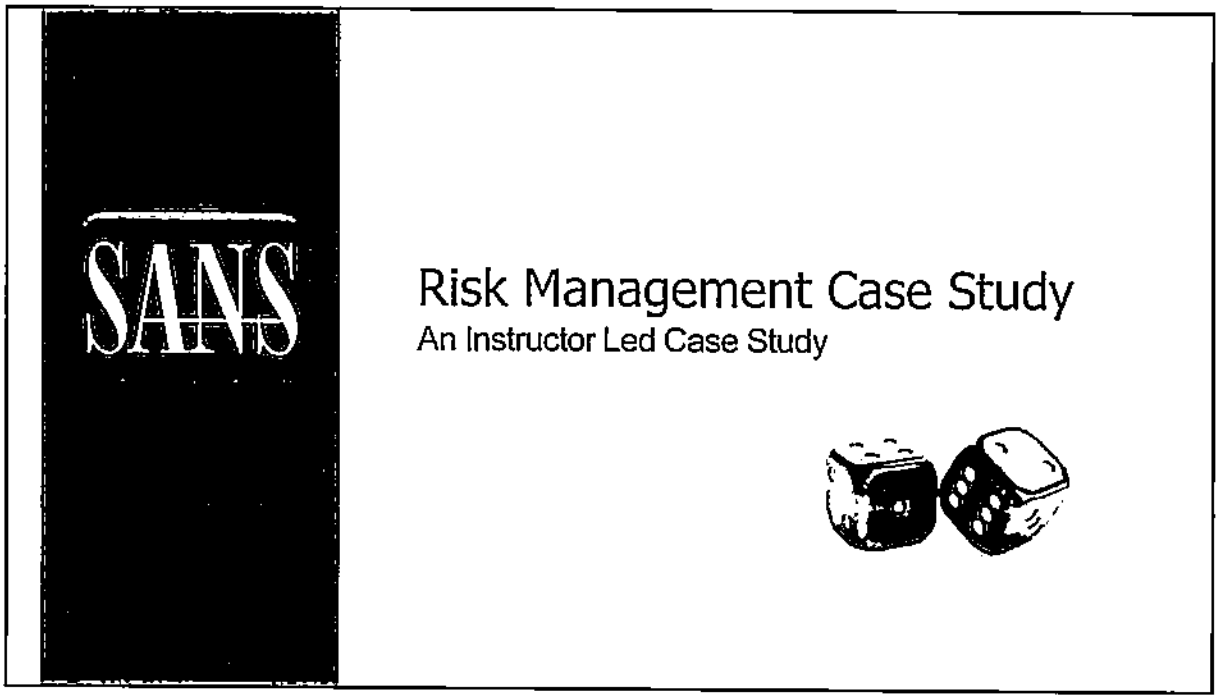
- Event management as a part of risk management eventually leads an organization into the discussion of continuous monitoring
- Rather than one time assessment, continuous monitoring promotes:
  - A combination of control & event based risk management
  - Automated collection of data from risk / security sensors
  - Automated analysis / reporting of data collected from sensors
  - Automated alerting when risk thresholds have been exceeded
- Hopefully this will be the future of risk management
- The Department of Homeland Security in the US has even sponsored a Continuous Diagnostics and Mitigation (CDM) program for all agencies

A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

The more an organization is able to deploy sensors and automate the collection of events, the more an organization starts to move towards a discussion of continuous monitoring. Traditionally organization have relied on audit teams, penetration testers, or generic security assessment teams to assess organizations on a limited basis via one time assessments. Rather than relying on ad hoc one time assessments, continuous monitoring allows an organization to promote the following:

- A combination of control & event based risk management
- Automated collection of data from risk / security sensors
- Automated analysis / reporting of data collected from sensors
- Automated alerting when risk thresholds have been exceeded

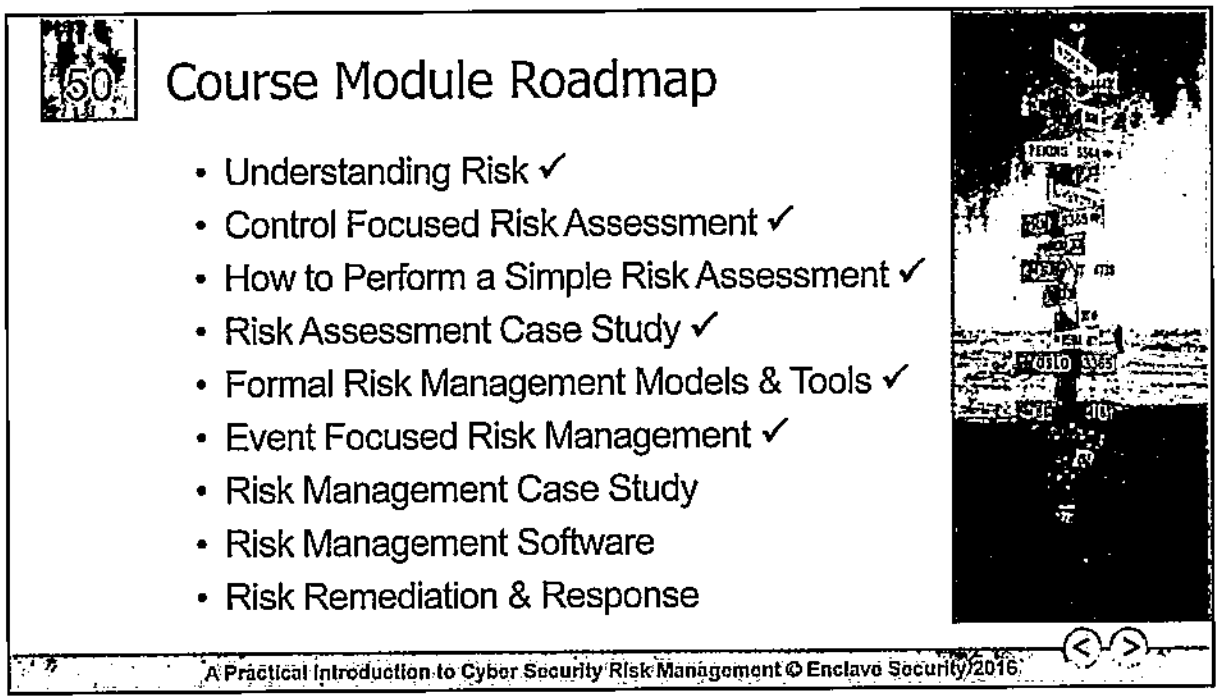
Hopefully the information assurance industry will see this type of monitoring as their future and more and more assessments will be based on data provided in this manner. In the United States there is even an effort within the US Government, sponsored by the Department of Homeland Security, called the Continuous Diagnostics and Mitigation (CDM) program. One can only hope that more instances of these sorts of efforts will be in the industry's future.



Now it's time to put what we've learned into practice. The purpose of the lab activities that we are engaging in during this class is to give the student an opportunity to put into practice what we have been learning about from the instructor. The hope is that by working through the exercises in this lab that you will be better prepared to take this information back to your company in order to put it into practice.

Some of these lab exercises specifically call on students to work as teams. Even if the lab specifically does not call for you to work as a team, in a conference setting you will likely get the most from this activity if you do work as a group with friendly students sitting around you. Not only will you be networking and building relationships with smart students sitting around you, but you will also be able to benefit from their ideas and experiences as well. Every student brings a wealth of information to the class, and participating as a group is one of the better ways to be able to take advantage of those experiences.

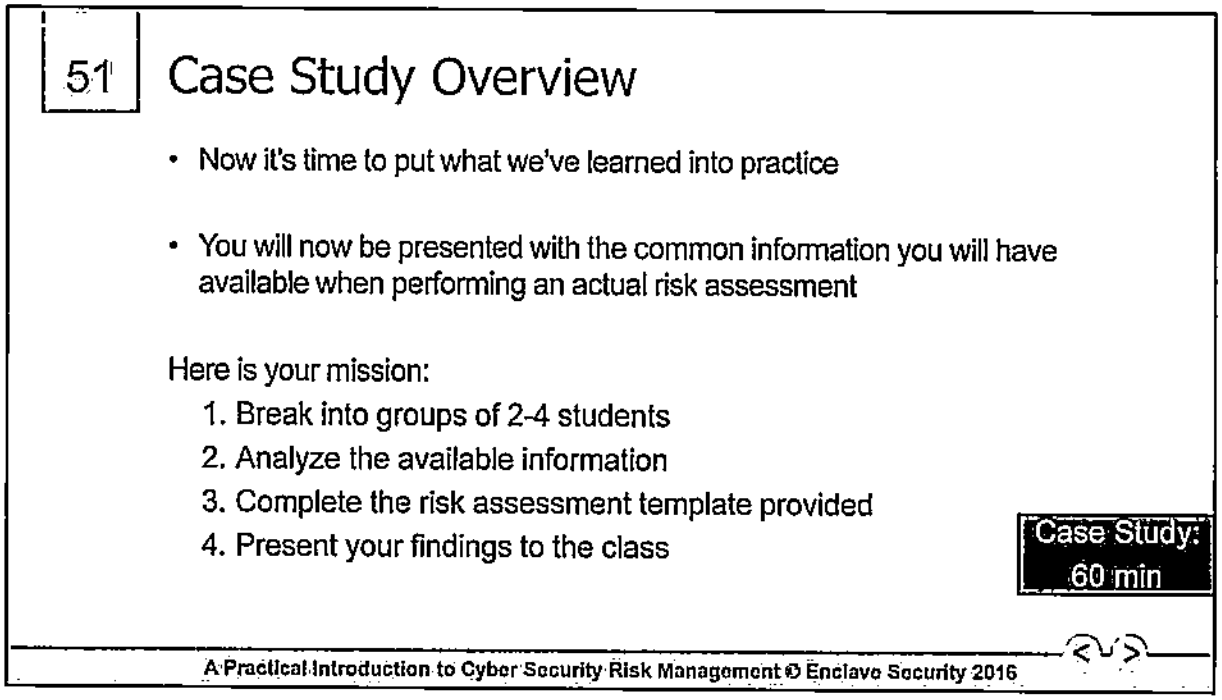
At this point, it's time to turn to the section of the book where this lab is described in more detail. Listen to the specific instructions given by your instructor and follow the instructions in the lab exercises step by step. If you have any technical challenges or questions, don't hesitate to ask, the instructor and/or teaching assistants are here to help.



In this course we will explore the concept of risk and its practical impact on an organization. Ultimately the goal of this course is to prepare students to effectively utilize risk assessment as a tool for enterprise defense. Too many times organizations think of risk assessment and risk management as academic tools with little to no practical application. These concepts are often viewed as a formal task to pursue when an organization has free time rather than as a core business activity that drives other enterprise security efforts. In today's course students will have the opportunity to learn about the proper place of risk assessment and risk management in an enterprise. They will also be given practical skills for how to perform a risk assessment on a step by step basis, from data collection to the point of presenting their findings to business leaders. Students with a desire to perform more in depth analysis will also be given tools and formal models to consider to empower them to create a long term / formal risk management program.

Specifically today we will cover the following subjects:

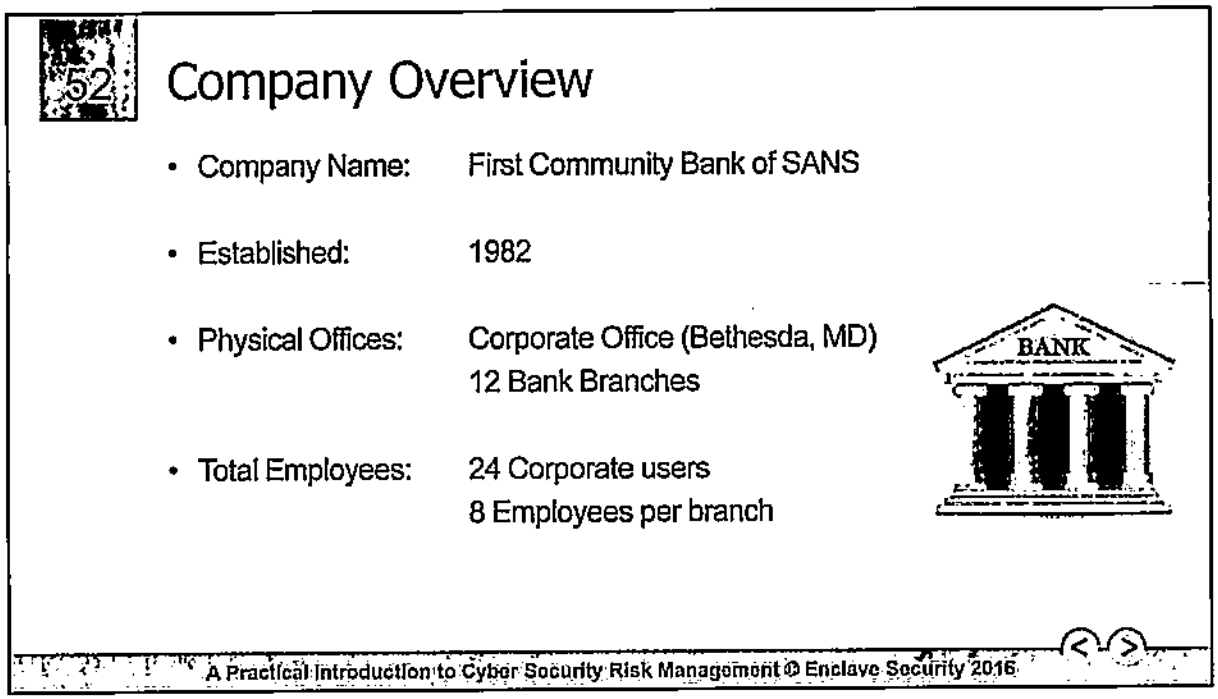
- Understanding Risk
- Control Focused Risk Assessment
- How to Perform a Simple Risk Assessment
- Risk Assessment Case Study
- Formal Risk Management Models & Tools
- Event Focused Risk Management
- Risk Management Case Study
- Risk Management Software
- Risk Remediation & Response



Ok, now it is your turn!

It is time to put into practice what we have just learned in the previous sections of the course. You will now be presented with the common information you will have available when performing an actual risk assessment. Detailed instructions for this section can be found in the lab materials at the end of today's material. However the basic breakdown of the lab activities are:

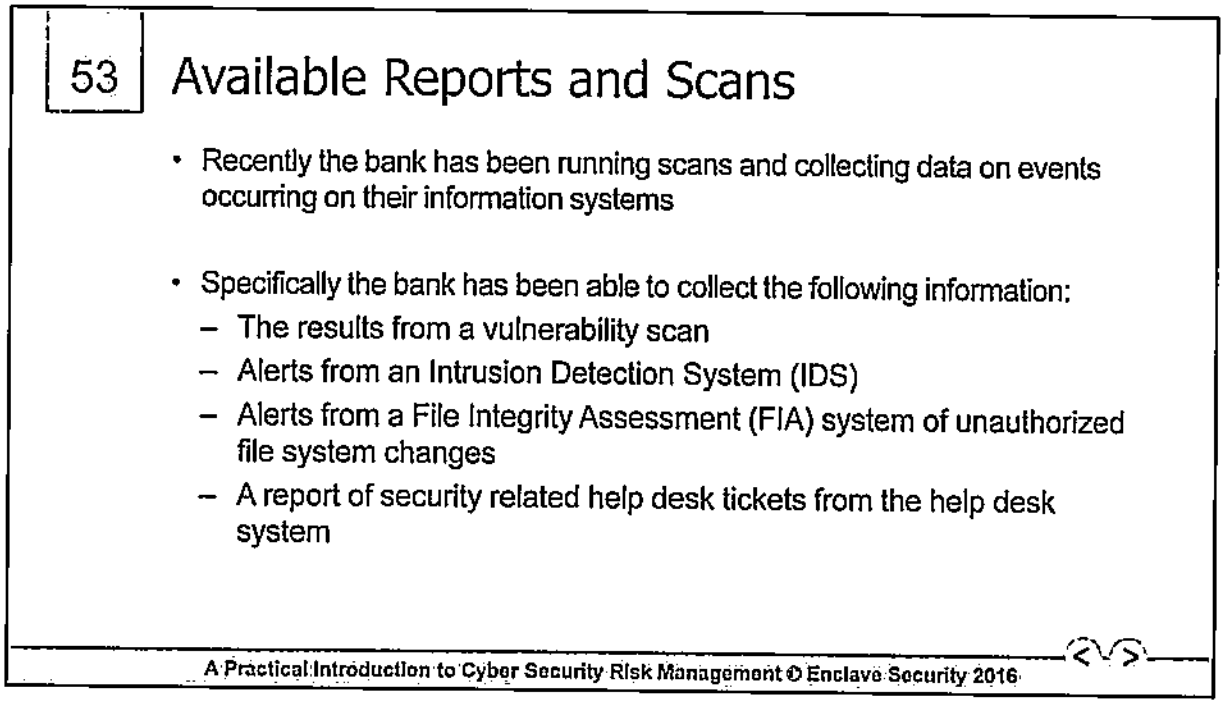
1. Break into groups of 2-4 students
2. Analyze the available information
3. Complete the risk assessment template provided
4. Present your findings to the class



The company you will be assessing is the First Community Bank of SANS. This bank was established in 1982 and is a small regional bank which is headquartered in the Mid-Atlantic region of the United States. Presently they have 12 branch offices, in addition to their corporate office, and there are no current plans to expand into any new markets.

There are 24 corporate employees working out of the main corporate office and there are 8 employees at each of the branches. At the present time all positions have been filled at all of the offices.

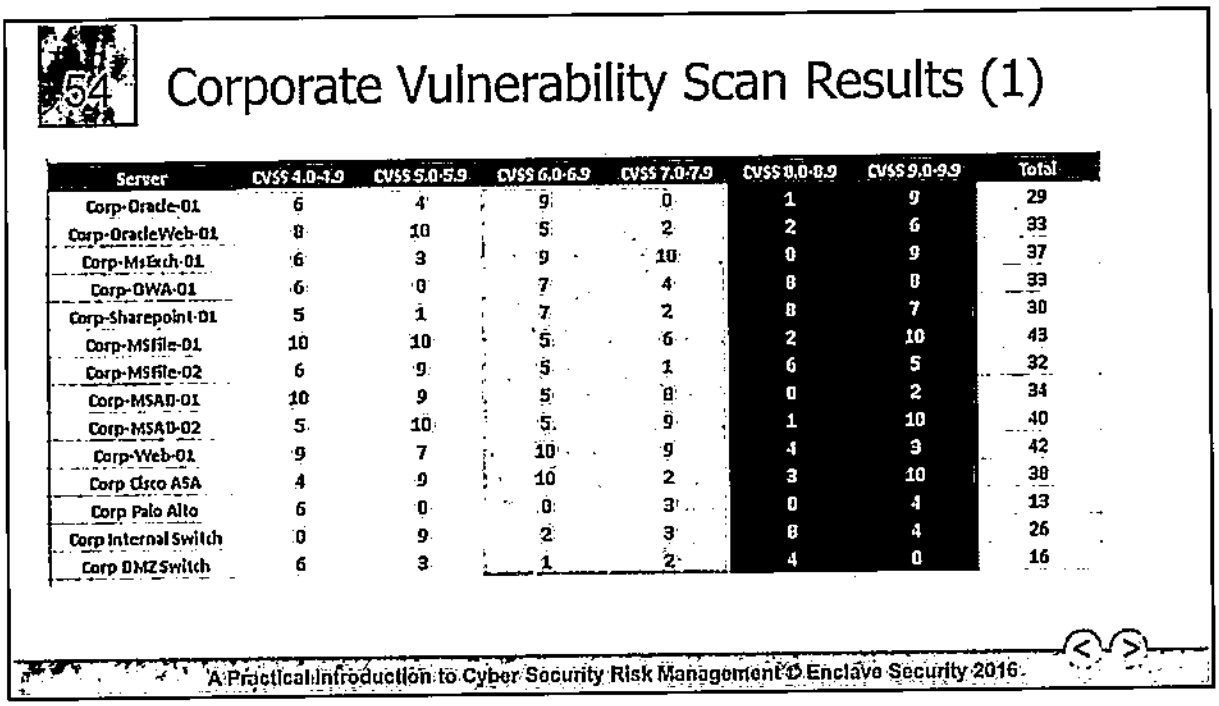
In yesterday's material we started to perform an assessment of this organization's information systems. Today we are going to use the information we gathered from our original risk assessment and add in information from events and vulnerability scans that we have collected on the organization's information systems. This will give us a more detailed view of the organization's true risk levels. We will also use this information later to automate the process and create dashboards for the organization's executives.



When interviewing the organization's key stakeholders you have discovered that the First Bank of SANS has been running security scans and gathering data from some newly deployed security tools within the organization. They're hoping that this information might also be useful when analyzing risk. They are not quite sure how to use the data but they are relying on your expertise to use the information properly to add value to the assessment.

Specifically when interviewing the organization you learn that the following information is available to review:

- The results from a vulnerability scan
- Alerts from an Intrusion Detection System (IDS)
- Alerts from a File Integrity Assessment (FIA) system of unauthorized file system changes
- A report of security related help desk tickets from the help desk system



Server	CVSS 4.0-4.9	CVSS 5.0-5.9	CVSS 6.0-6.9	CVSS 7.0-7.9	CVSS 8.0-8.9	CVSS 9.0-9.9	Total
Corp-Oracle-01	6	4	9	0	1	9	29
Corp-OracleWeb-01	8	10	5	2	2	6	33
Corp-MsExch-01	6	3	9	10	0	9	37
Corp-OWA-01	6	0	7	4	8	8	33
Corp-Sharepoint-01	5	1	7	2	8	7	30
Corp-MSfile-01	10	10	5	6	2	10	43
Corp-MSfile-02	6	9	5	1	6	5	32
Corp-MSAD-01	10	9	5	8	0	2	34
Corp-MSAD-02	5	10	5	9	1	10	40
Corp-Web-01	9	7	10	9	4	3	42
Corp Cisco ASA	4	9	10	2	3	10	38
Corp Palo Alto	6	0	0	3	0	4	13
Corp Internal Switch	0	9	2	3	8	4	26
Corp DMZ Switch	6	3	1	2	4	0	16

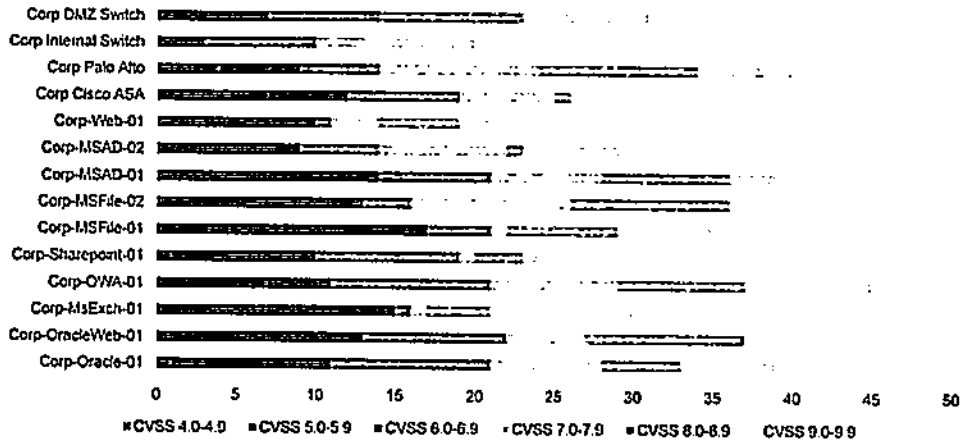
The chart in the slide above represents data that you have collected from one of the organization's security consoles. When your team interviewed the organization's security engineers they provided you this information in the hopes that it would assist you in your event driven risk assessment exercise. You will need to use the information provided to you to complete the exercise.

This data that you see above is the data from a vulnerability scan report.

They were not sure what data would be most useful to you so they provided you a number of different reports that they thought might help. Remember, not all data sets, presented in all formats are useful when analyzing risk. Often times some of the data you receive is simply noise to be ignored. Part of your job is to figure out what data is useful and what is not.

55

Corporate Vulnerability Scan Results (2)

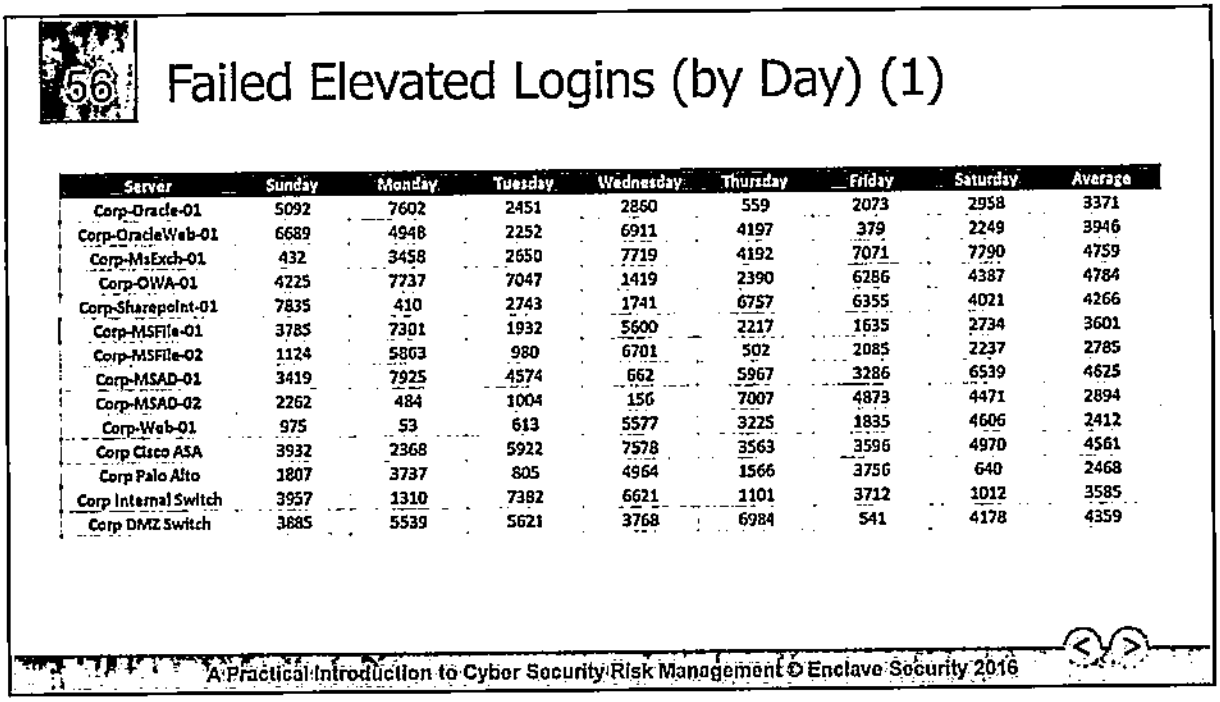


A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

The chart in the slide above represents data that you have collected from one of the organization's security consoles. When your team interviewed the organization's security engineers they provided you this information in the hopes that it would assist you in your event driven risk assessment exercise. You will need to use the information provided to you to complete the exercise.

This data that you see above is the data from a vulnerability scan report.

They were not sure what data would be most useful to you so they provided you a number of different reports that they thought might help. Remember, not all data sets, presented in all formats are useful when analyzing risk. Often times some of the data you receive is simply noise to be ignored. Part of your job is to figure out what data is useful and what is not.

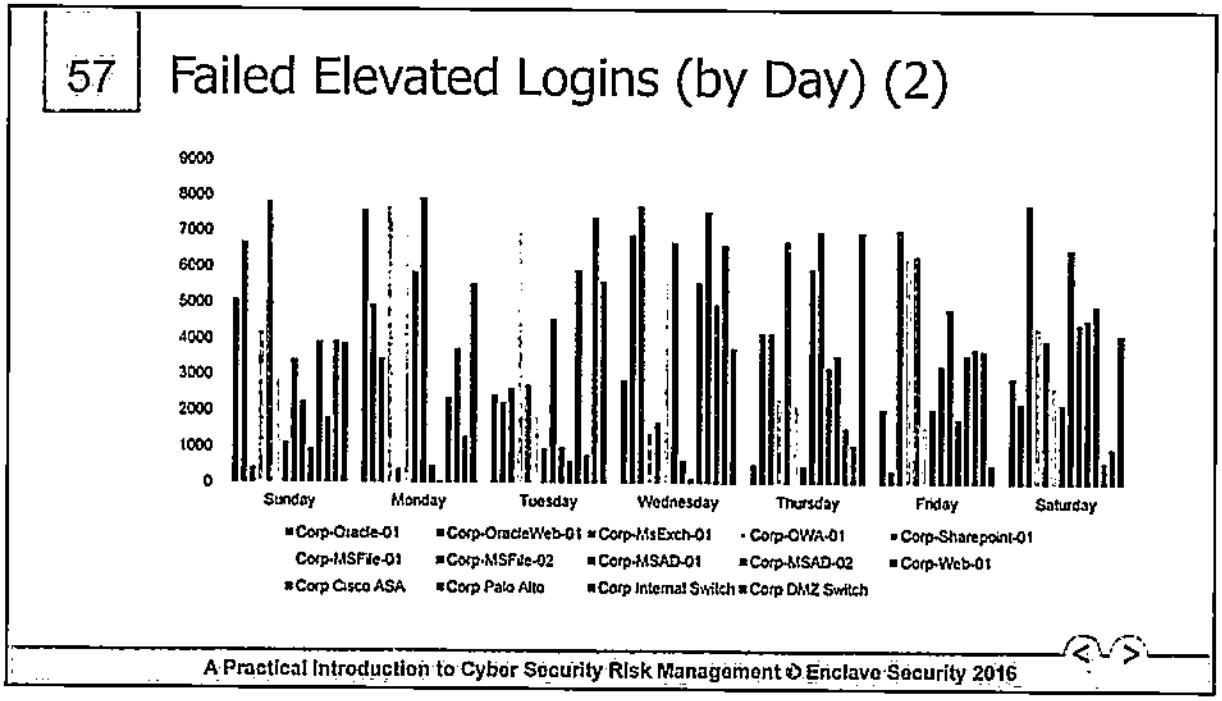


Server	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Average
Corp-Oracle-01	5092	7602	2451	2860	559	2073	2958	3371
Corp-OracleWeb-01	6689	4948	2252	6911	4197	379	2249	3946
Corp-MsExch-01	432	3458	2650	7719	4192	7071	7790	4759
Corp-OWA-01	4225	7737	7047	1419	2390	6286	4387	4784
Corp-Sharepoint-01	7835	410	2743	1741	6757	6355	4021	4266
Corp-MSFile-01	3785	7301	1932	5600	2217	1635	2734	3601
Corp-MSFile-02	1124	5803	980	6701	502	2085	2237	2785
Corp-MSAD-01	3419	7925	4574	662	5967	3286	6539	4625
Corp-MSAD-02	2262	484	1004	156	7007	4873	4471	2894
Corp-Web-01	975	53	613	5577	3225	1835	4606	2412
Corp Cisco ASA	3932	2368	5922	7578	3563	3596	4970	4561
Corp Palo Alto	1807	3737	805	4964	1566	3756	640	2468
Corp Internal Switch	3957	1310	7382	6621	1101	3712	1012	3585
Corp DMZ Switch	3885	5539	5621	3768	6984	541	4178	4359

The chart in the slide above represents data that you have collected from one of the organization's security consoles. When your team interviewed the organization's security engineers they provided you this information in the hopes that it would assist you in your event driven risk assessment exercise. You will need to use the information provided to you to complete the exercise.

This data that you see above is the data from log events on servers.

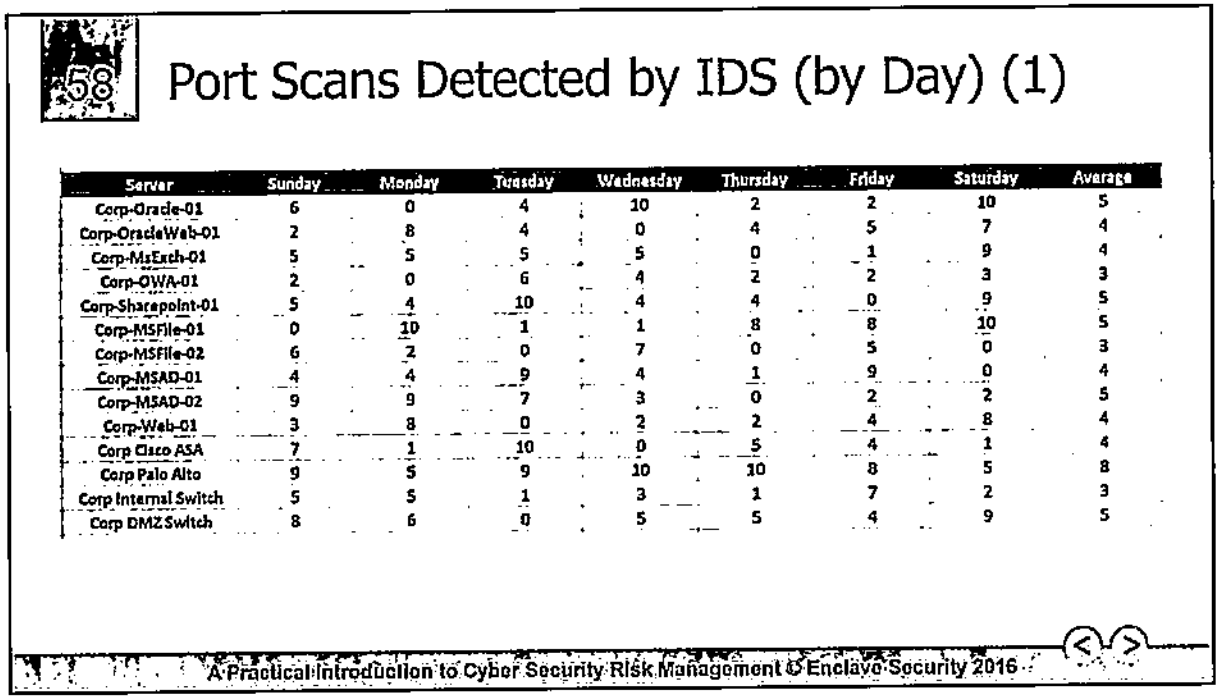
They were not sure what data would be most useful to you so they provided you a number of different reports that they thought might help. Remember, not all data sets, presented in all formats are useful when analyzing risk. Often times some of the data you receive is simply noise to be ignored. Part of your job is to figure out what data is useful and what is not.



The chart in the slide above represents data that you have collected from one of the organization's security consoles. When your team interviewed the organization's security engineers they provided you this information in the hopes that it would assist you in your event driven risk assessment exercise. You will need to use the information provided to you to complete the exercise.

This data that you see above is the data from log events on servers.

They were not sure what data would be most useful to you so they provided you a number of different reports that they thought might help. Remember, not all data sets, presented in all formats are useful when analyzing risk. Often times some of the data you receive is simply noise to be ignored. Part of your job is to figure out what data is useful and what is not.

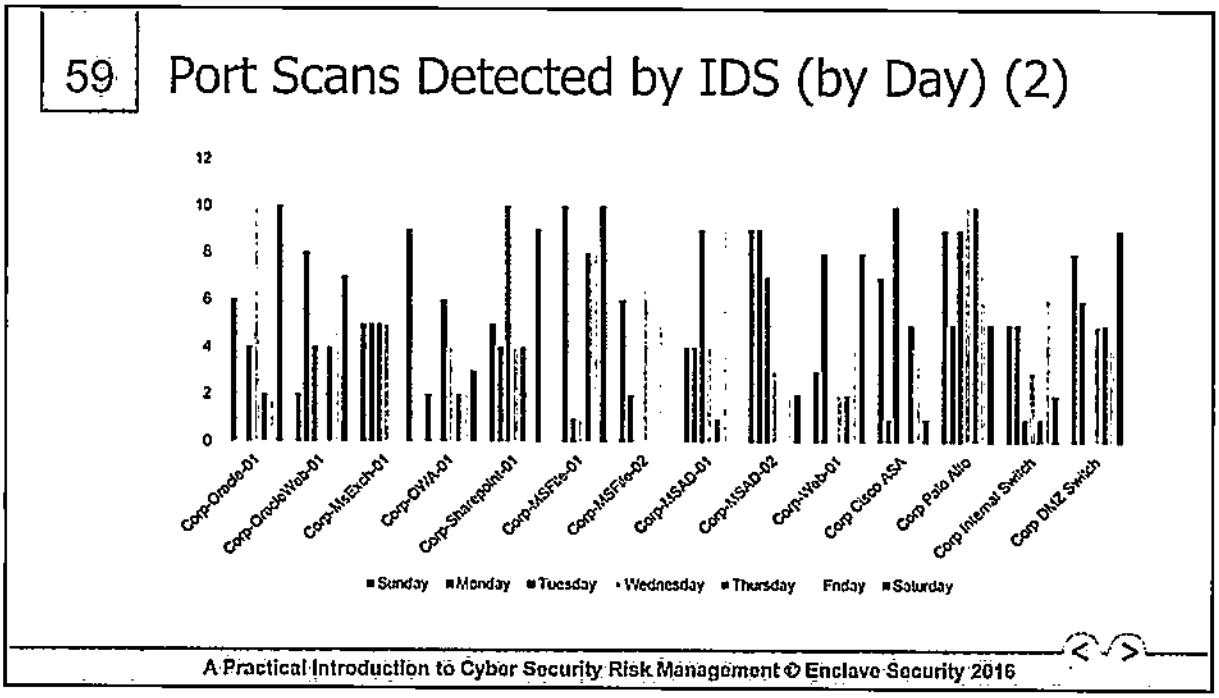


Server	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Average
Corp-Oracle-01	6	0	4	10	2	2	10	5
Corp-OracleWeb-01	2	8	4	0	4	5	7	4
Corp-MsExch-01	5	5	5	5	0	1	9	4
Corp-OWA-01	2	0	6	4	2	2	3	3
Corp-Sharepoint-01	5	4	10	4	4	0	9	5
Corp-MSFile-01	0	10	1	1	8	8	10	5
Corp-MSFile-02	6	2	0	7	0	5	0	3
Corp-MSAD-01	4	4	9	4	1	9	0	4
Corp-MSAD-02	9	9	7	3	0	2	2	5
Corp-Web-01	3	8	0	2	2	4	8	4
Corp Cisco ASA	7	1	10	0	5	4	1	4
Corp Palo Alto	9	5	9	10	10	8	5	8
Corp Internal Switch	5	5	1	3	1	7	2	3
Corp DMZ Switch	8	6	0	5	5	4	9	5

The chart in the slide above represents data that you have collected from one of the organization's security consoles. When your team interviewed the organization's security engineers they provided you this information in the hopes that it would assist you in your event driven risk assessment exercise. You will need to use the information provided to you to complete the exercise.

This data that you see above is the data from the intrusion detection system.

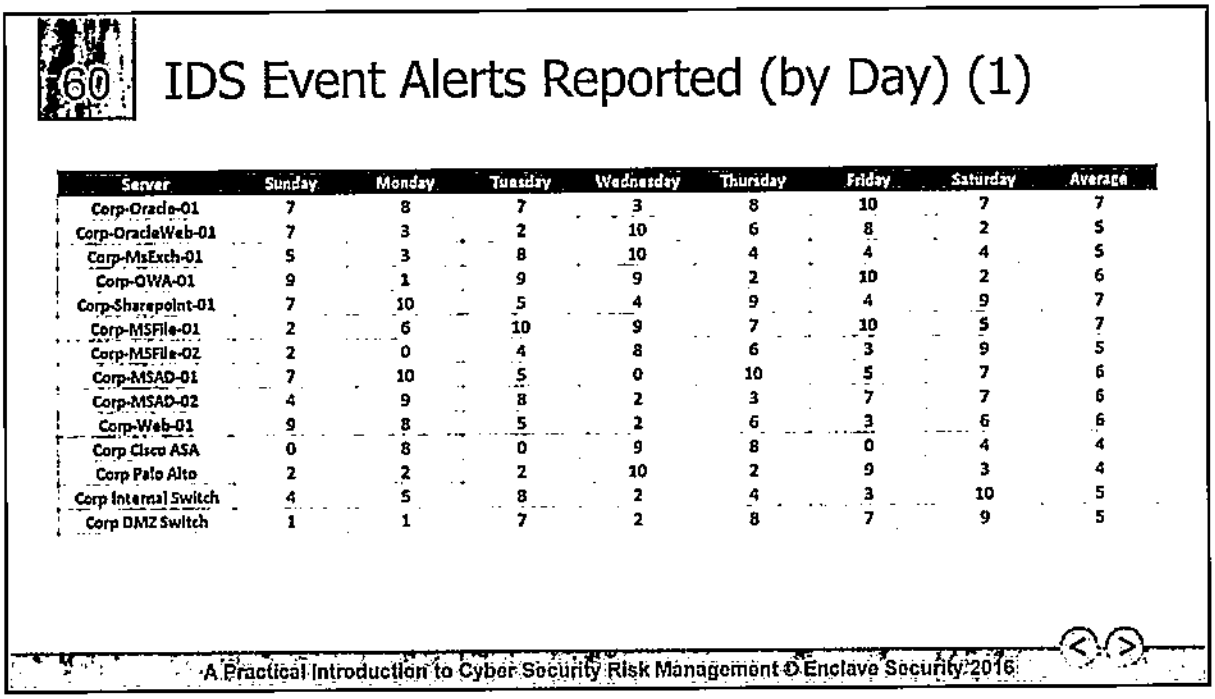
They were not sure what data would be most useful to you so they provided you a number of different reports that they thought might help. Remember, not all data sets, presented in all formats are useful when analyzing risk. Often times some of the data you receive is simply noise to be ignored. Part of your job is to figure out what data is useful and what is not.



The chart in the slide above represents data that you have collected from one of the organization's security consoles. When your team interviewed the organization's security engineers they provided you this information in the hopes that it would assist you in your event driven risk assessment exercise. You will need to use the information provided to you to complete the exercise.

This data that you see above is the data from the intrusion detection system.

They were not sure what data would be most useful to you so they provided you a number of different reports that they thought might help. Remember, not all data sets, presented in all formats are useful when analyzing risk. Often times some of the data you receive is simply noise to be ignored. Part of your job is to figure out what data is useful and what is not.



Server	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Average
Corp-Oracle-01	7	8	7	3	8	10	7	7
Corp-OracleWeb-01	7	3	2	10	6	8	2	5
Corp-MsExch-01	5	3	8	10	4	4	4	5
Corp-OWA-01	9	1	9	9	2	10	2	6
Corp-Sharepoint-01	7	10	5	4	9	4	9	7
Corp-MSFile-01	2	6	10	9	7	10	5	7
Corp-MSFile-02	2	0	4	8	6	3	9	5
Corp-MSAD-01	7	10	5	0	10	5	7	6
Corp-MSAD-02	4	9	8	2	3	7	7	6
Corp-Web-01	9	8	5	2	6	3	6	6
Corp Cisco ASA	0	8	0	9	8	0	4	4
Corp Palo Alto	2	2	2	10	2	9	3	4
Corp Internal Switch	4	5	8	2	4	3	10	5
Corp DMZ Switch	1	1	7	2	8	7	9	5

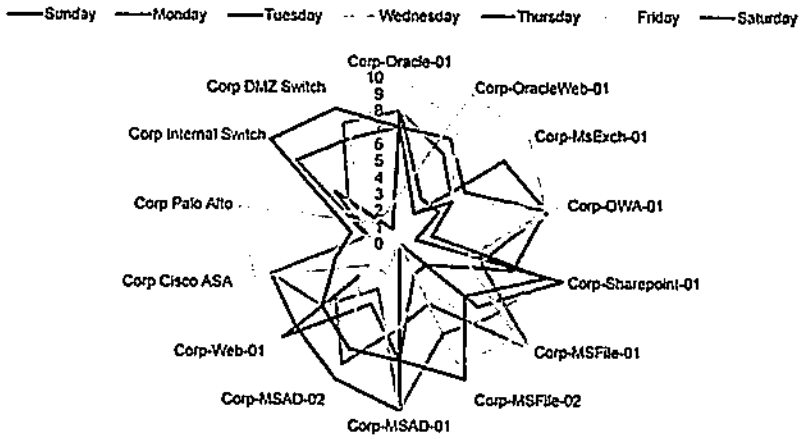
The chart in the slide above represents data that you have collected from one of the organization's security consoles. When your team interviewed the organization's security engineers they provided you this information in the hopes that it would assist you in your event driven risk assessment exercise. You will need to use the information provided to you to complete the exercise.

This data that you see above is the data from the intrusion detection system.

They were not sure what data would be most useful to you so they provided you a number of different reports that they thought might help. Remember, not all data sets, presented in all formats are useful when analyzing risk. Often times some of the data you receive is simply noise to be ignored. Part of your job is to figure out what data is useful and what is not.

61

IDS Event Alerts Reported (by Day) (2)

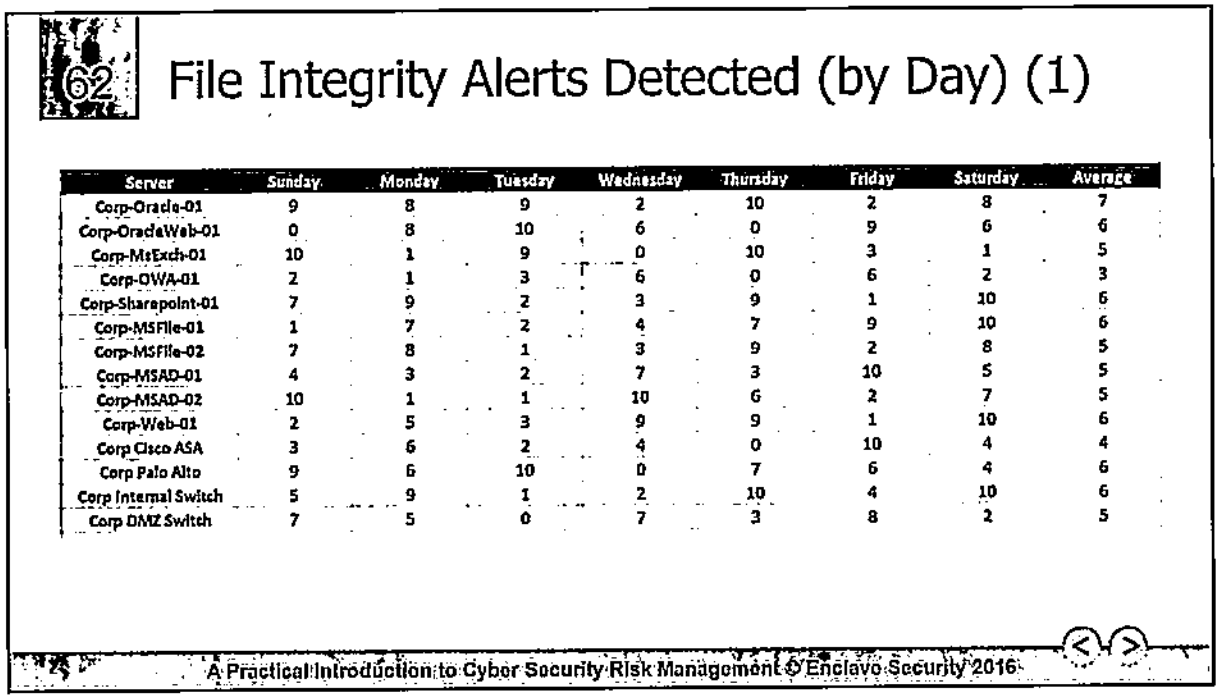


A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

The chart in the slide above represents data that you have collected from one of the organization's security consoles. When your team interviewed the organization's security engineers they provided you this information in the hopes that it would assist you in your event driven risk assessment exercise. You will need to use the information provided to you to complete the exercise.

This data that you see above is the data from the intrusion detection system.

They were not sure what data would be most useful to you so they provided you a number of different reports that they thought might help. Remember, not all data sets, presented in all formats are useful when analyzing risk. Often times some of the data you receive is simply noise to be ignored. Part of your job is to figure out what data is useful and what is not.



Server	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Average
Corp-Oracle-01	9	8	9	2	10	2	8	7
Corp-OracleWeb-01	0	8	10	6	0	9	6	6
Corp-MsExch-01	10	1	9	0	10	3	1	5
Corp-OWA-01	2	1	3	6	0	6	2	3
Corp-Sharepoint-01	7	9	2	3	9	1	10	6
Corp-MSFile-01	1	7	2	4	7	9	10	6
Corp-MSFile-02	7	8	1	3	9	2	8	5
Corp-MSAD-01	4	3	2	7	3	10	5	5
Corp-MSAD-02	10	1	1	10	6	2	7	5
Corp-Web-01	2	5	3	9	9	1	10	6
Corp Cisco ASA	3	6	2	4	0	10	4	4
Corp Palo Alto	9	6	10	0	7	6	4	6
Corp Internal Switch	5	9	1	2	10	4	10	6
Corp DMZ Switch	7	5	0	7	3	8	2	5

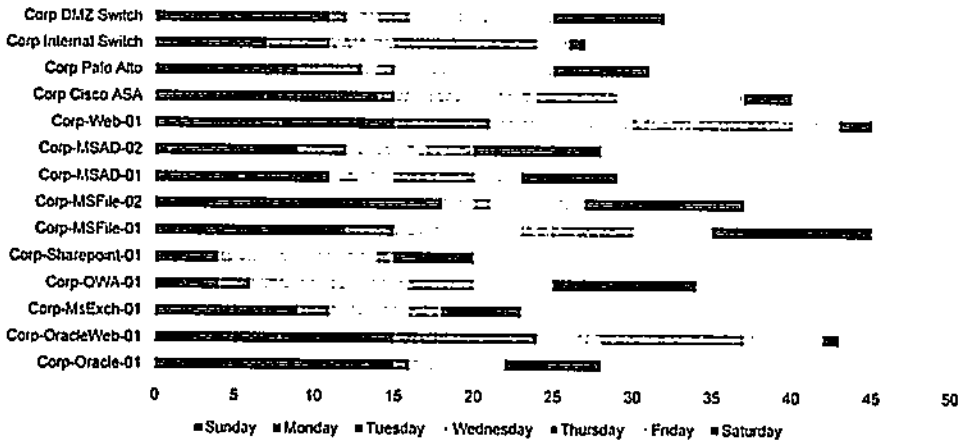
The chart in the slide above represents data that you have collected from one of the organization's security consoles. When your team interviewed the organization's security engineers they provided you this information in the hopes that it would assist you in your event driven risk assessment exercise. You will need to use the information provided to you to complete the exercise.

This data that you see above is the data from the file integrity assessment system.

They were not sure what data would be most useful to you so they provided you a number of different reports that they thought might help. Remember, not all data sets, presented in all formats are useful when analyzing risk. Often times some of the data you receive is simply noise to be ignored. Part of your job is to figure out what data is useful and what is not.

63

File Integrity Alerts Detected (by Day) (2)

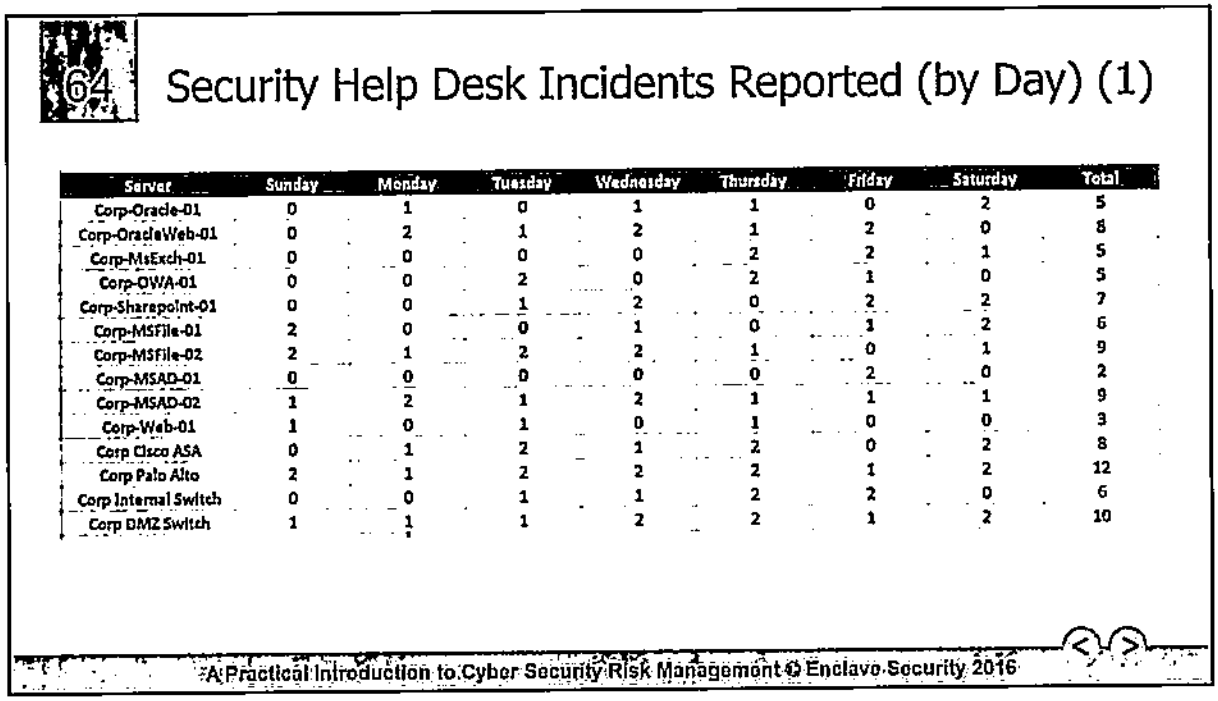


A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

The chart in the slide above represents data that you have collected from one of the organization's security consoles. When your team interviewed the organization's security engineers they provided you this information in the hopes that it would assist you in your event driven risk assessment exercise. You will need to use the information provided to you to complete the exercise.

This data that you see above is the data from the file integrity assessment system.

They were not sure what data would be most useful to you so they provided you a number of different reports that they thought might help. Remember, not all data sets, presented in all formats are useful when analyzing risk. Often times some of the data you receive is simply noise to be ignored. Part of your job is to figure out what data is useful and what is not.

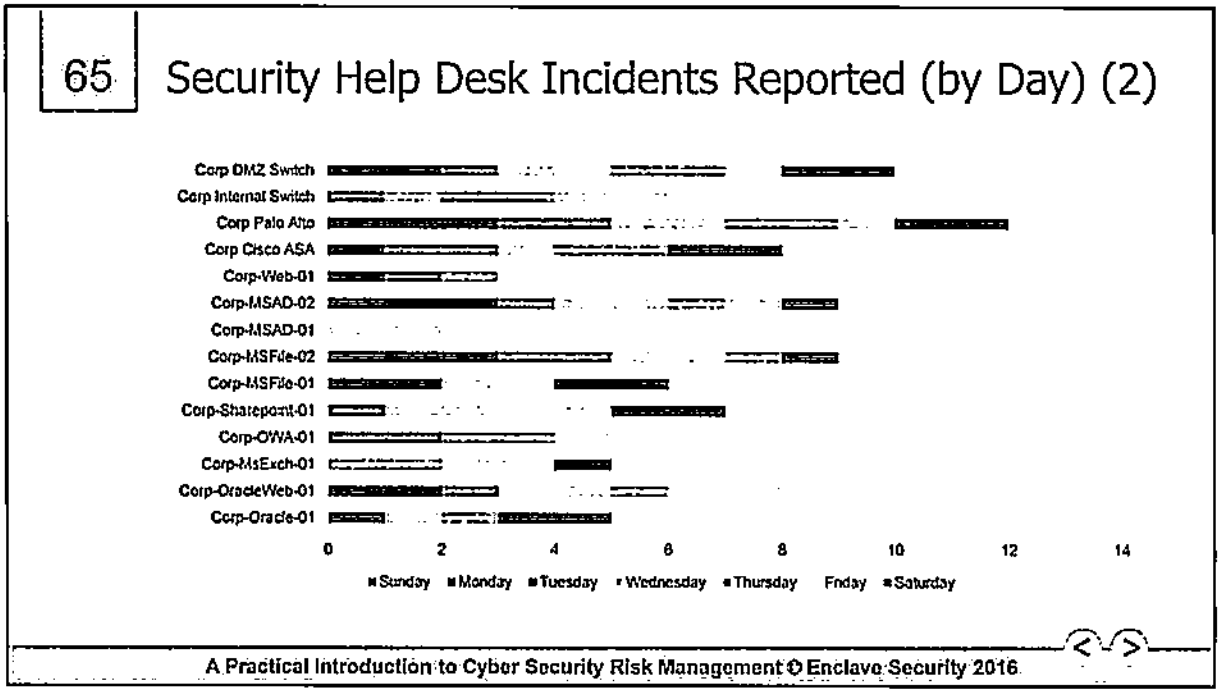


Server	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Total
Corp-Oracle-01	0	1	0	1	1	0	2	5
Corp-OracleWeb-01	0	2	1	2	1	2	0	8
Corp-MsExch-01	0	0	0	0	2	2	1	5
Corp-OWA-01	0	0	2	0	2	1	0	5
Corp-Sharepoint-01	0	0	1	2	0	2	2	7
Corp-MSFile-01	2	0	0	1	0	1	2	6
Corp-MSFile-02	2	1	2	2	1	0	1	9
Corp-MSAD-01	0	0	0	0	0	2	0	2
Corp-MSAD-02	1	2	1	2	1	1	1	9
Corp-Web-01	1	0	1	0	1	0	0	3
Corp Cisco ASA	0	1	2	1	2	0	2	8
Corp Palo Alto	2	1	2	2	2	1	2	12
Corp Internal Switch	0	0	1	1	2	2	0	6
Corp DMZ Switch	1	1	1	2	2	1	2	10

The chart in the slide above represents data that you have collected from one of the organization's security consoles. When your team interviewed the organization's security engineers they provided you this information in the hopes that it would assist you in your event driven risk assessment exercise. You will need to use the information provided to you to complete the exercise.

This data that you see above is the data from the help desk system.

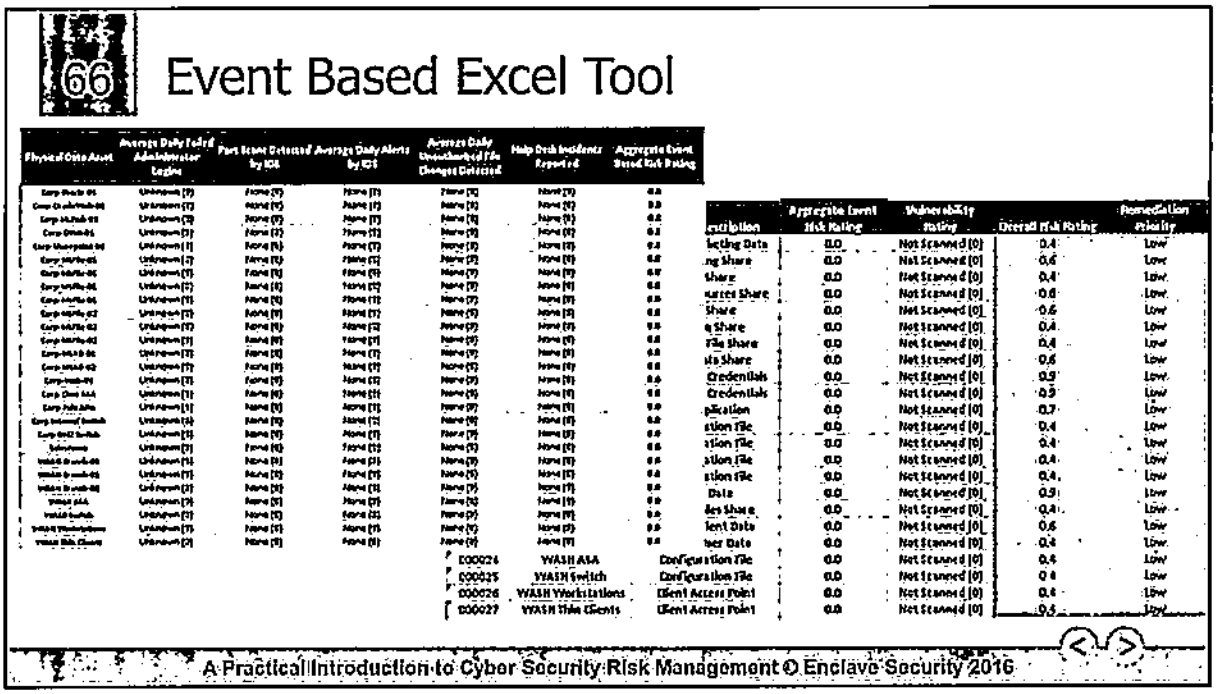
They were not sure what data would be most useful to you so they provided you a number of different reports that they thought might help. Remember, not all data sets, presented in all formats are useful when analyzing risk. Often times some of the data you receive is simply noise to be ignored. Part of your job is to figure out what data is useful and what is not.



The chart in the slide above represents data that you have collected from one of the organization's security consoles. When your team interviewed the organization's security engineers they provided you this information in the hopes that it would assist you in your event driven risk assessment exercise. You will need to use the information provided to you to complete the exercise.

This data that you see above is the data from the help desk system.

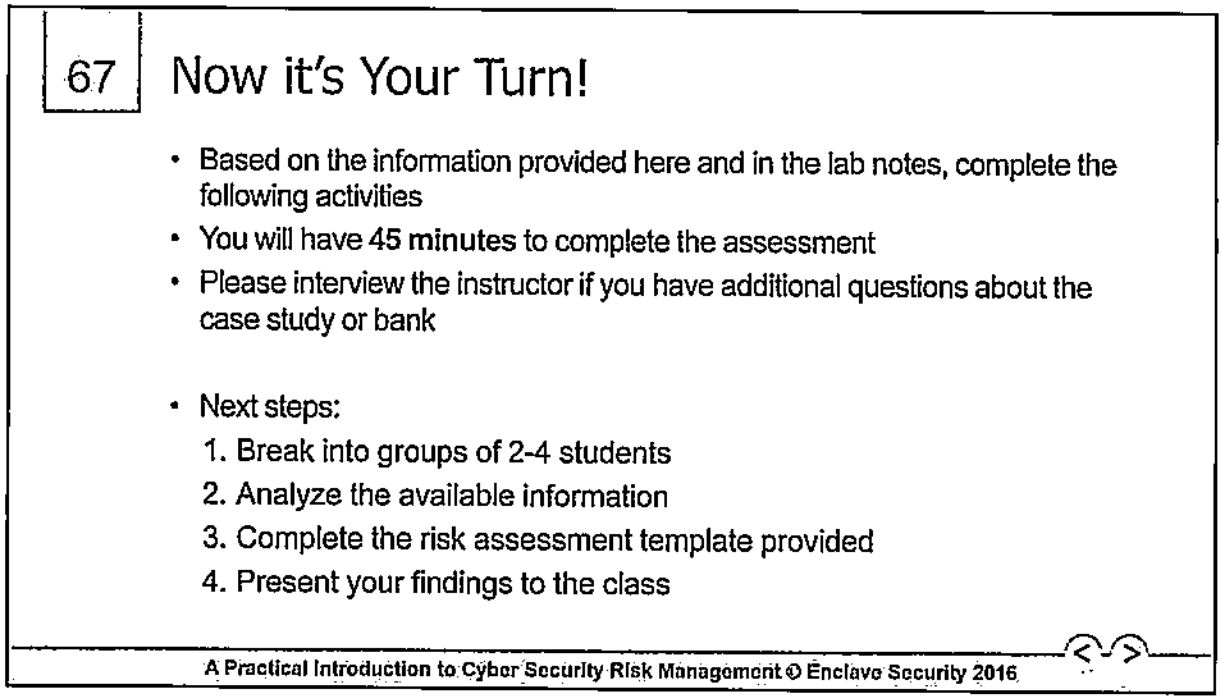
They were not sure what data would be most useful to you so they provided you a number of different reports that they thought might help. Remember, not all data sets, presented in all formats are useful when analyzing risk. Often times some of the data you receive is simply noise to be ignored. Part of your job is to figure out what data is useful and what is not.



Based on the information provided to you it is now time to complete the Excel based risk assessment tool that we began in class yesterday. This time we need to enter in the additional information from the earlier graphs to enhance the risk scoring system.

On the course USB drive there is another version of the Excel based assessment tool labeled the Day 2 - Enclave_Event_Based_Risk_Partially_Blank. The instructor will demonstrate for you which version of the tool we should be using for this exercise.

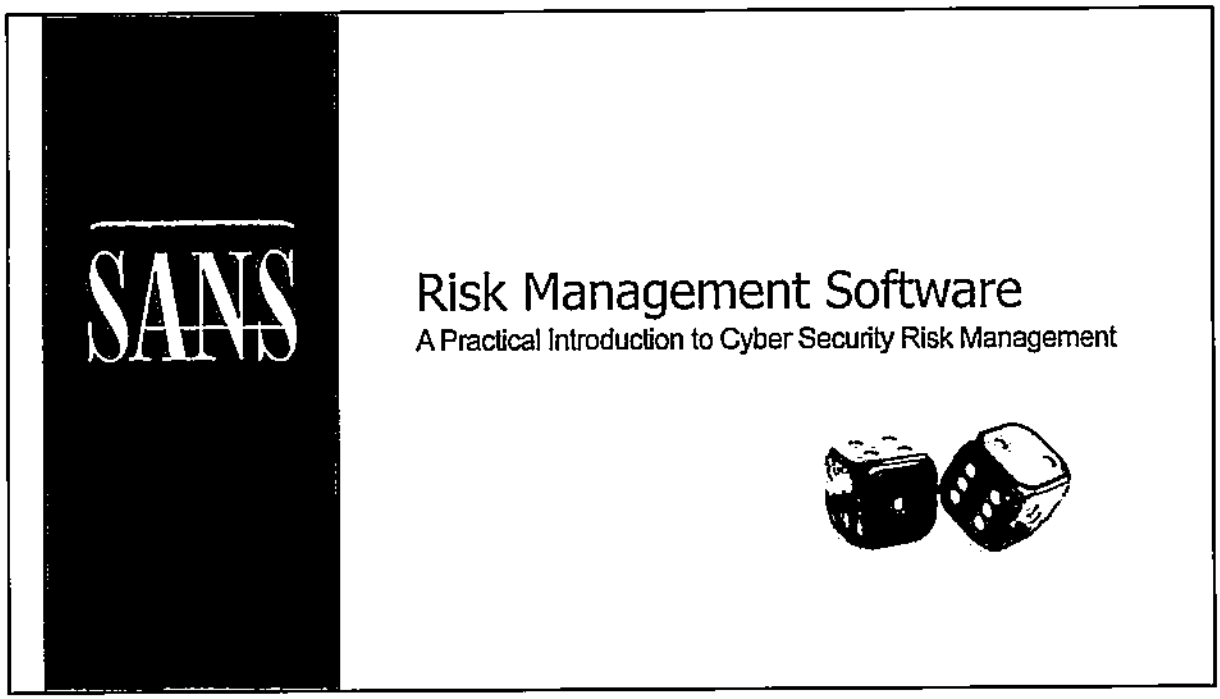
In your small groups follow the instructions in this section and the lab at the end of this book to analyze the results of the new risk assessment.



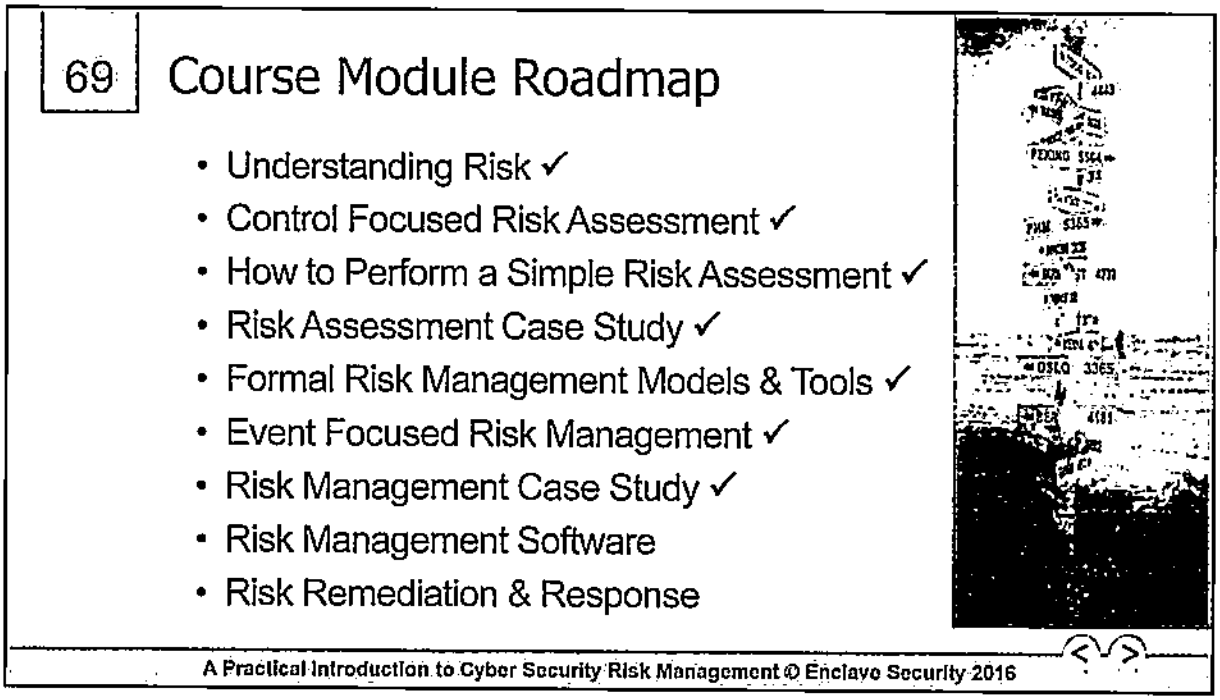
Ok, let's get started! Based on the information that's been provided to you so far and in the lab notes, it is time to complete this case study. You will have about 45 minutes as a team to complete the assignment and be ready to present your findings to the class. It sounds like a long time, but the time will go quickly, so make sure you stay on task.

To evaluate your time, the main activities you will need to complete (with time estimates) are listed below:

1. Break into groups of 2-4 students (2 minutes)
2. Analyze the available information (13 minutes)
3. Complete the risk assessment template provided (30 minutes)
4. Present your findings to the class (15 minutes)



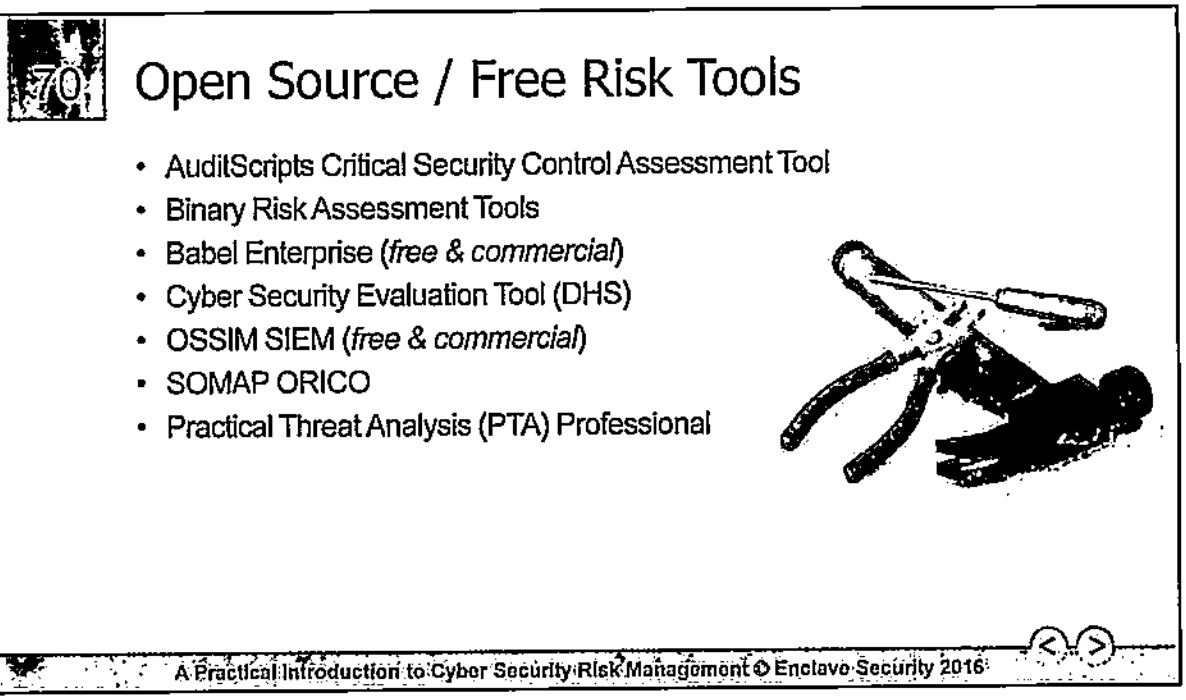
This page intentionally left blank.



In this course we will explore the concept of risk and its practical impact on an organization. Ultimately the goal of this course is to prepare students to effectively utilize risk assessment as a tool for enterprise defense. Too many times organizations think of risk assessment and risk management as academic tools with little to no practical application. These concepts are often viewed as a formal task to pursue when an organization has free time rather than as a core business activity that drives other enterprise security efforts. In today's course students will have the opportunity to learn about the proper place of risk assessment and risk management in an enterprise. They will also be given practical skills for how to perform a risk assessment on a step by step basis, from data collection to the point of presenting their findings to business leaders. Students with a desire to perform more in depth analysis will also be given tools and formal models to consider to empower them to create a long term / formal risk management program.

Specifically today we will cover the following subjects:

- Understanding Risk
- Control Focused Risk Assessment
- How to Perform a Simple Risk Assessment
- Risk Assessment Case Study
- Formal Risk Management Models & Tools
- Event Focused Risk Management
- Risk Management Case Study
- Risk Management Software
- Risk Remediation & Response

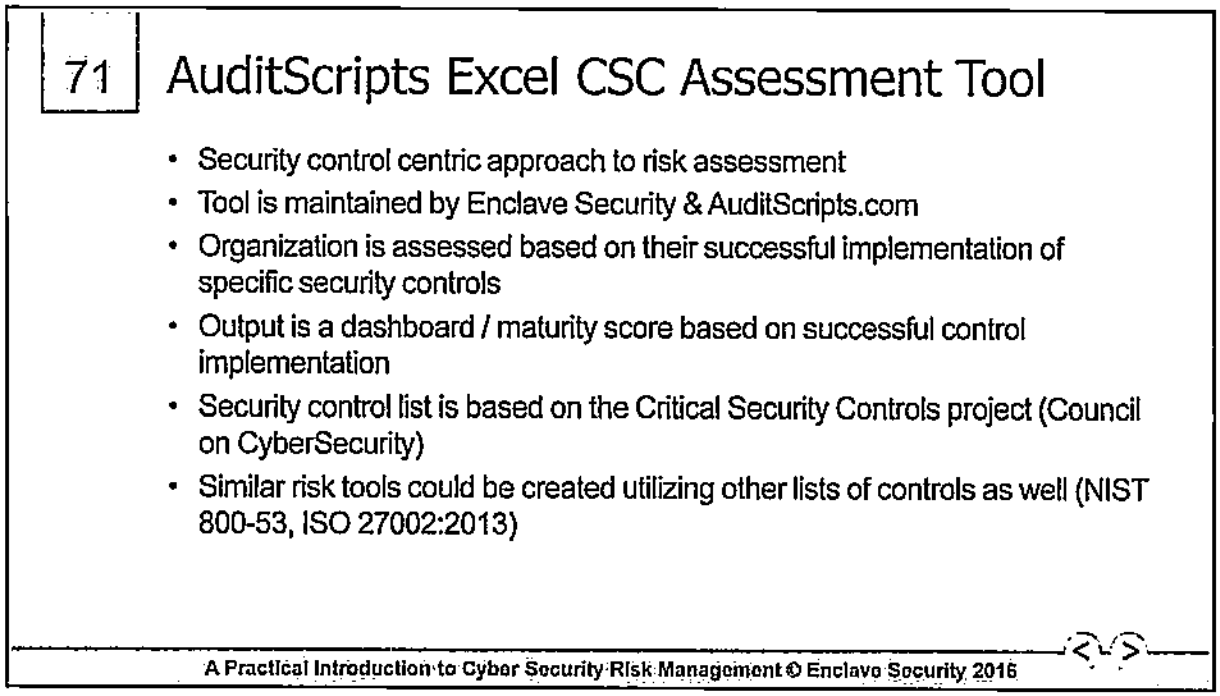


From our experiences, there seem to be two different ways of choosing which risk management method is right for your organization. One approach people take is to evaluate the models that have been defined and choose from the risk models directly. This tends to be the most academic approach and is favored by organizations that tend to be more process and paperwork driven. This is not a value judgment, simply an observation.

Another approach for determining which model makes the most sense is to evaluate the tools that are on the market to help assist with risk management, and then choose one of those tools to guide you through this process. There are a number of tools, well more than a dozen on the market today. Most are commercial tools, but there are a few open source or free tools that you may consider as a starting point for your program.

Three of the open source or free tools that we have seen effectively used by organizations are:

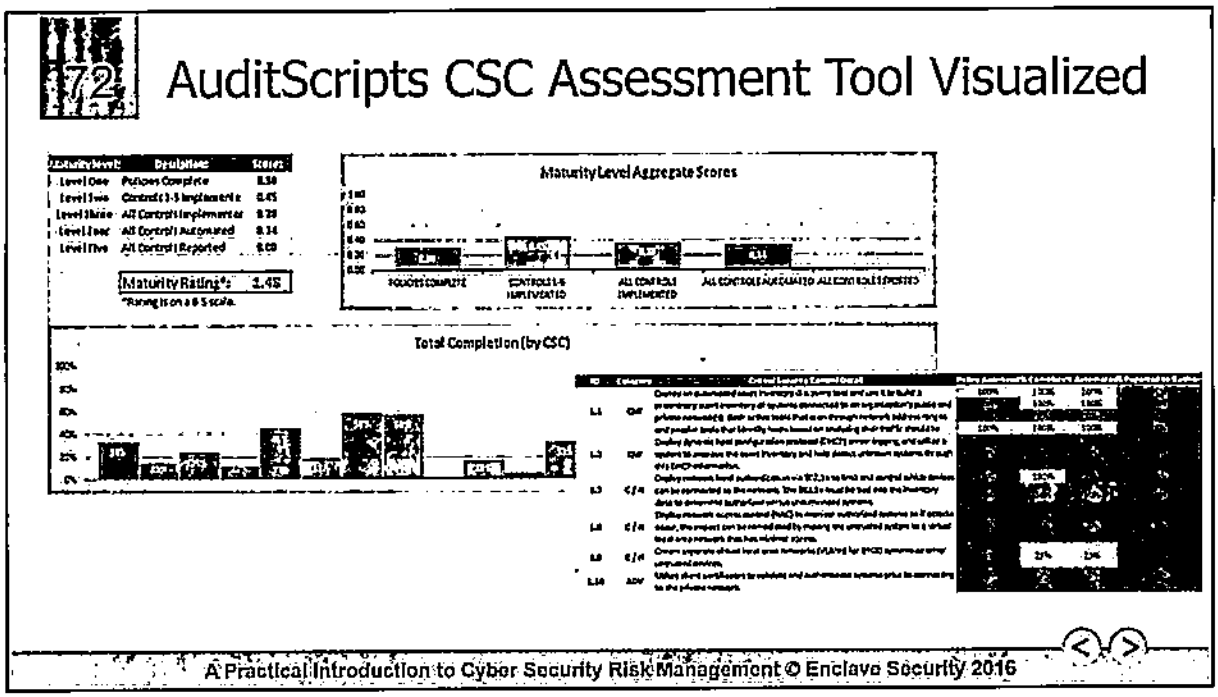
- AuditScripts Critical Security Control Assessment Tool
- Binary Risk Assessment Tools
- Babel Enterprise (*free and commercial*)
- Cyber Security Evaluation Tool (DHS)
- OSSIM SIEM (*free and commercial*)
- SOMAP ORICO
- Practical Threat Analysis (PTA) Professional



One of the free tools that an organization might consider is the free AuditScripts.com Critical Security Control Assessment Tool. This tool takes a security control centric view of risk assessment and scores the organization based on their successful completion / implementation of specific security controls that are defined by the organization. It is a self-assessment tool, and meant to be a more advanced method of utilizing questionnaires to score an organization's maturity level in relation to the control list selected. Currently this tool is being maintained by James Tarala and Kelli Tarala from Enclave Security, and is included in the resource library at AuditScripts.com.

The output of this tool is a dashboard which scores the organization based on their successful implementation of the Critical Security Controls, that have been defined by the Council on CyberSecurity. Part of the outcome of this tool is also a maturity model score that can use used to track the organization's progress over time and visualize improvements in maturity over time.

While this version of the tool is specific to the Critical Security Controls, a similar approach could also be followed for other regulatory frameworks or standards such as NIST 800-53 or ISO 27002.



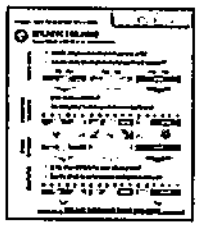
The slide above illustrates the output of the AuditScripts Critical Security Control Assessment Tool. As the participant works their way through a series of questions, based on their successful implementation of the Critical Security Controls, they are given points based on the level which specific controls have been implemented and integrated into the business.

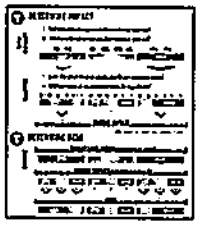
As points are assigned, these points are aggregated and create the summary dashboard located on the fist page of the worksheet. This dashboard will automatically create the organization's maturity level based on the answers to the questions provided throughout the tool. The maturity levels defined correspond to a capability maturity model style of scoring, and organizations will be rated somewhere within the following levels:

- Level One: Policies (statements of management intent) have been documented.
- Level Two: Controls 1-5 have been fully implemented.
- Level Three: All of the controls have been fully implemented.
- Level Four: All of the controls have been fully automated (where possible).
- Level Five: All of the controls are being regularly reported to business owners, who are integrating this knowledge into their business processes.

73 Binary Risk Assessment

- Tool based approach to risk assessment (by Ben Sapiro: http://binary.protect.io/)
- Focus is on quickly creating a risk assessment, facilitate conversations, and provide a subjective tool
- Follows a decision tree format for performing a risk assessment (guided & easy for business owners)
- Free tools include:
  - Desktop Software
  - iPad App
  - Quick Reference Card



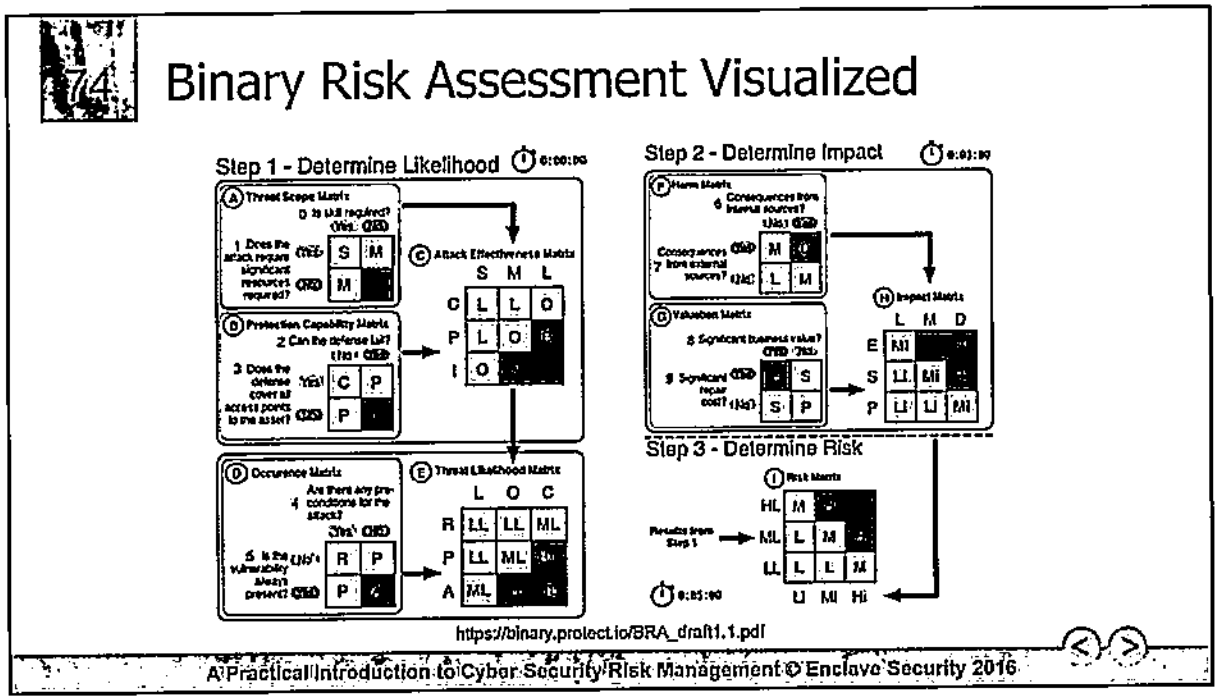


A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

One free risk assessment tool which has been popular with many practitioners is the Binary Risk Assessment tool written by Ben Sapiro. Specific information on the project, including a presentation and other documentation, can be found at http://binary.protect.io.

The focus of this project is the ability of the practitioner to quickly perform a risk assessment and facilitate conversations with business owners. It is not meant to be an in-depth or a quantitative measure. Rather it is meant to be a quick, subjective tool that can be used for simple risk assessments. Organizations who are new to the process of risk assessment should definitely consider this tool as a quick on-ramp to performing initial risk assessments. The project even makes quick references and decision trees for risk assessment available as a part of the approach.

One of the popular and drawing features of this approach are the tools and references that are made available on the project's website. Ben has made a desktop application, an iPad application, and a quick reference card all available on his website for people to freely download and use. In addition to being a sound approach to risk assessment, making the tools available for free have definitely increased the popularity of the project.



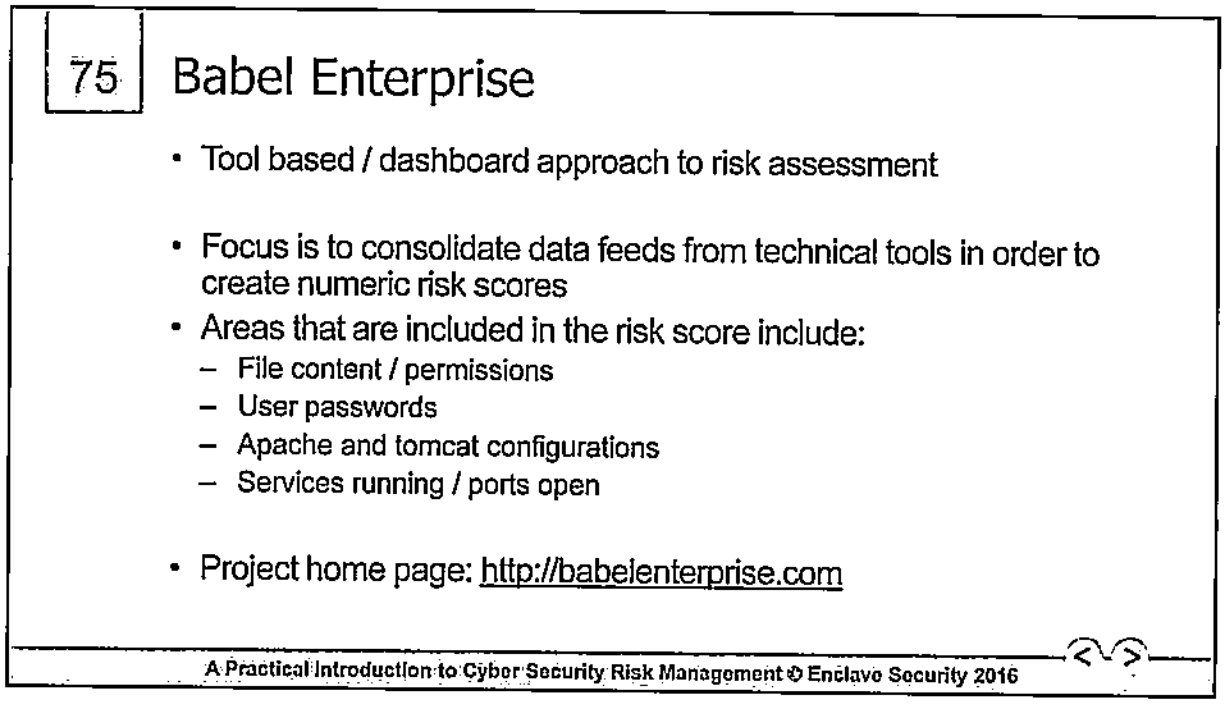
The above diagrams (taken from https://binary.protect.io/BRA_draft1.1.pdf) illustrates the process the binary method uses to determine an organization's risk. In the same guidance mentioned earlier, this tool relies on the academic work of many of the different models and does not try to create a model of it's own. Rather the tool attempts to take the information found in the academic models and integrates them into easily used tools that people can put their hands on quickly.

The three main steps utilized in this approach are the following:

Step One:	Determine likelihood
Step Two:	Determine impact
Step Three:	Determine Risk

Rather than focus on vulnerabilities, this approach focuses more strongly on the concepts of threat, protection capability, and attack effectiveness when determining risk.

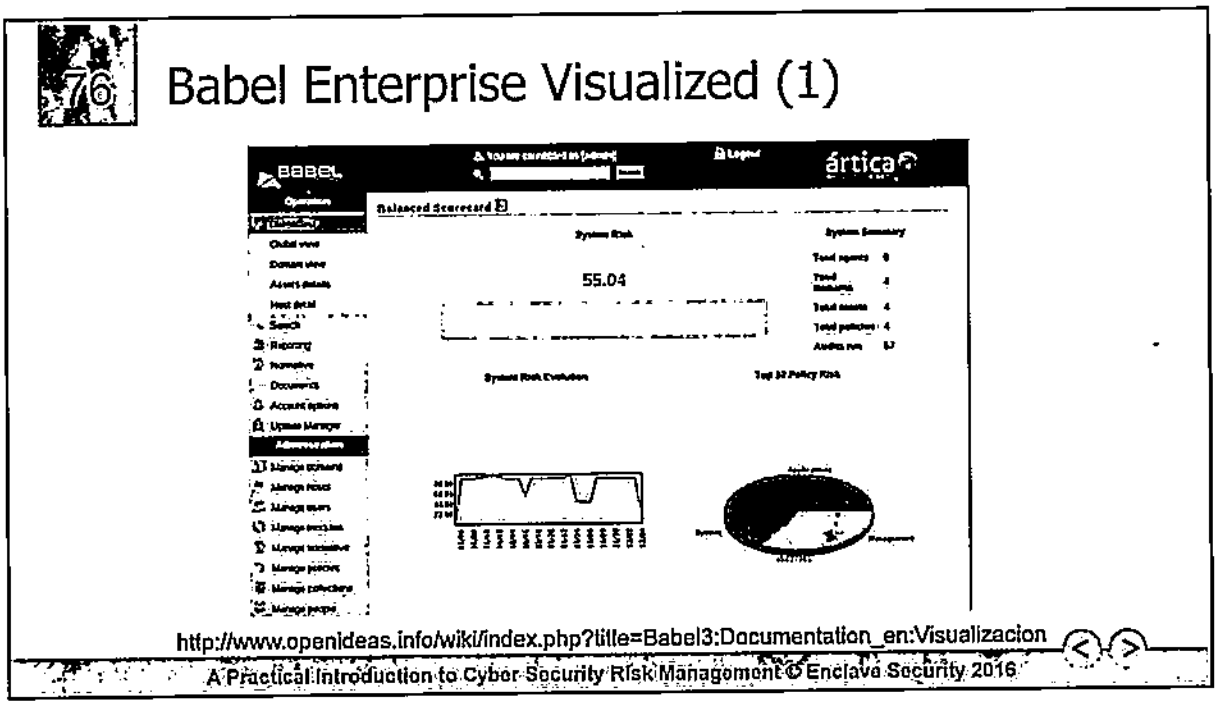
STATE DEPARTMENT



Another free tool (with a commercial cousin) is Babel Enterprise, which can be found at http://babelenterprise.com. This risk assessment tool takes a dashboard approach to risk assessment and integrates inputs from technical tools, rather than questionnaires, when creating its risk scores. The focus of the tool is to consolidate data feeds from multiple technical tools, including agents for numerous operating system platforms, in order to create a risk score for each host which can then be aggregated into scores by department or organization wide.

The software agent that's distributed with the tool can automatically score for a number of risk criteria, but those that are included by default are the following:

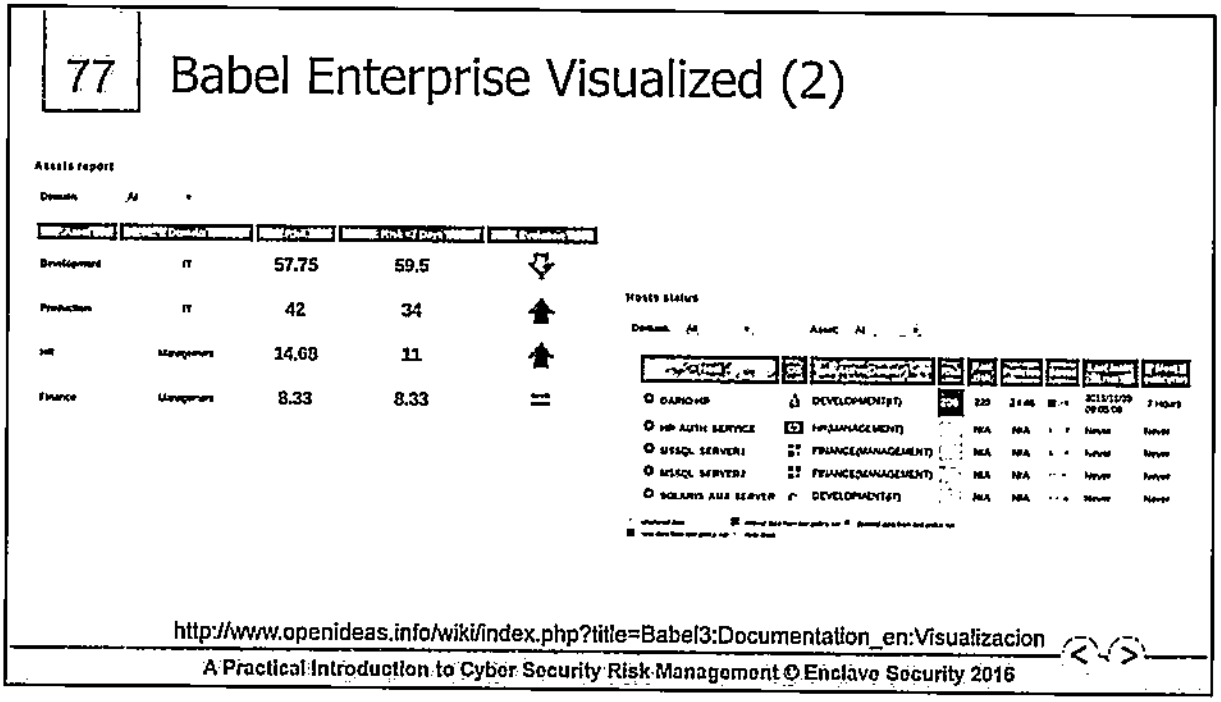
- File content / permissions
- User passwords
- Apache and tomcat configurations
- Services running / ports open



The above dashboard view is the result of input being collected from multiple technical feeds and aggregating those scores into one overall dashboard approach to risk. This dashboard is very similar in concept to the one created by the US Department of State when they created their iPost tool.

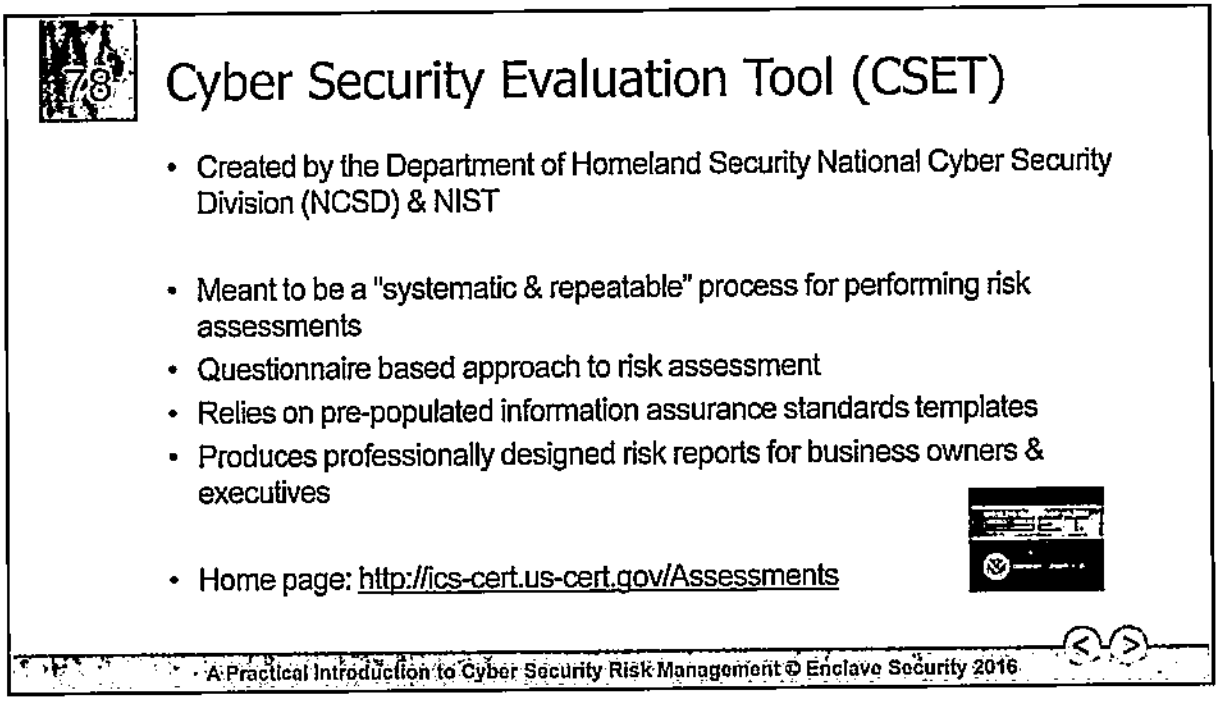
In the left hand column, the user will see the different dashboard views that can be displayed back to the user based on the scores obtained by the agent. These views can be examined Globally, by Domain, by Assets, or by Host.

Although the free version is limited in the amount of customization that can be performed, there still are quite a few characteristics of each host which are examined by this tool. The commercial tool can later be purchased by organizations desiring to have greater control over the policies that are defined for collection.



In addition to dashboard views, Babel Enterprise also provides Asset Reports and Host Reports, both of which can be viewed in the above diagram. These can be useful to see both the current risk state of each host as well as the trending scores for each host or department.

The trending feature viewed above makes this an especially useful tool for organizations as it provides a dynamic utility for business owners to evaluate on a regular cycle to determine the overall score of the hosts in their area of responsibility. This can be done at a host level, asset level, or a domain level as seen above.



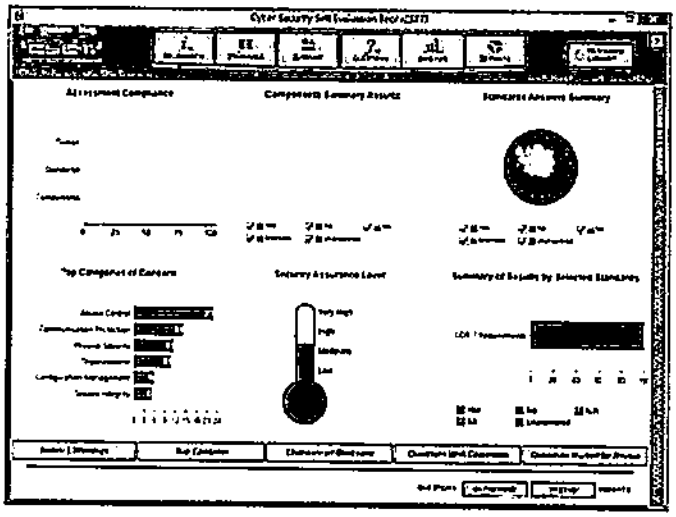
Another free tool an organization may want to consider when performing a risk assessment is the Cyber Security Evaluation Tool (CSET), which was jointly created by the Department of Homeland Security National Cyber Security Division (NCSD) and NIST. The idea behind this tool was to create a "systematic & repeatable" process for performing risk assessments, especially within US government agencies.

Unlike many of the other tools, this tool takes a questionnaire based approach to risk assessment. The person employing the tool indicates which standards the organization is responsible for, and based on those standards indicated the tool interviews the user with questions relevant to that standard. Based on the answers the interviewee gives a risk score is calculated and graphically charted for the user. The tool even has the ability to produce rather professionally designed risk reports for business owners, executives, or information assurance practitioners.

Although the tool is not always up to date with the latest version of each regulatory standard, and the standards in the list are not comprehensive – even for US entities, the tool still provides a good approach and methodology for assessing risk if an organization is looking to expand beyond a simple threat / vulnerability / likelihood / impact model.

79

Cyber Security Evaluation Tool Visualized



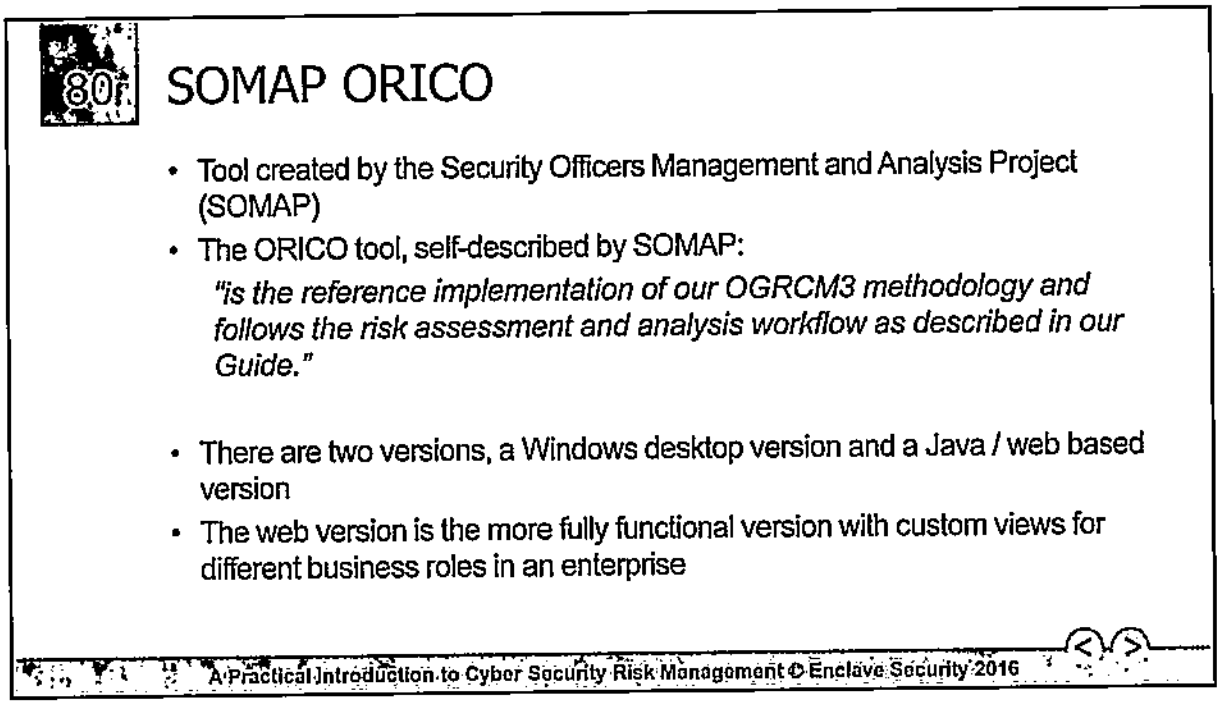
A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

After completing an assessment questionnaire, a screen similar to the one shown above is given to the user for review. These graphs can then be used to graphically illustrate the levels of risk facing the organization based on the interviewee's response to the questionnaire provided.

Overall the process this tool follows is:

1. Information
2. Standards
3. Diagram
4. Questions
5. Analysis
6. Reports

This tool is certainly an easy to use, graphical tool, which is especially useful for those within the US government. It also provides a nice transition into the concepts covered by the traditional commercial Governance, Risk, and Compliance (GRC) software tools.

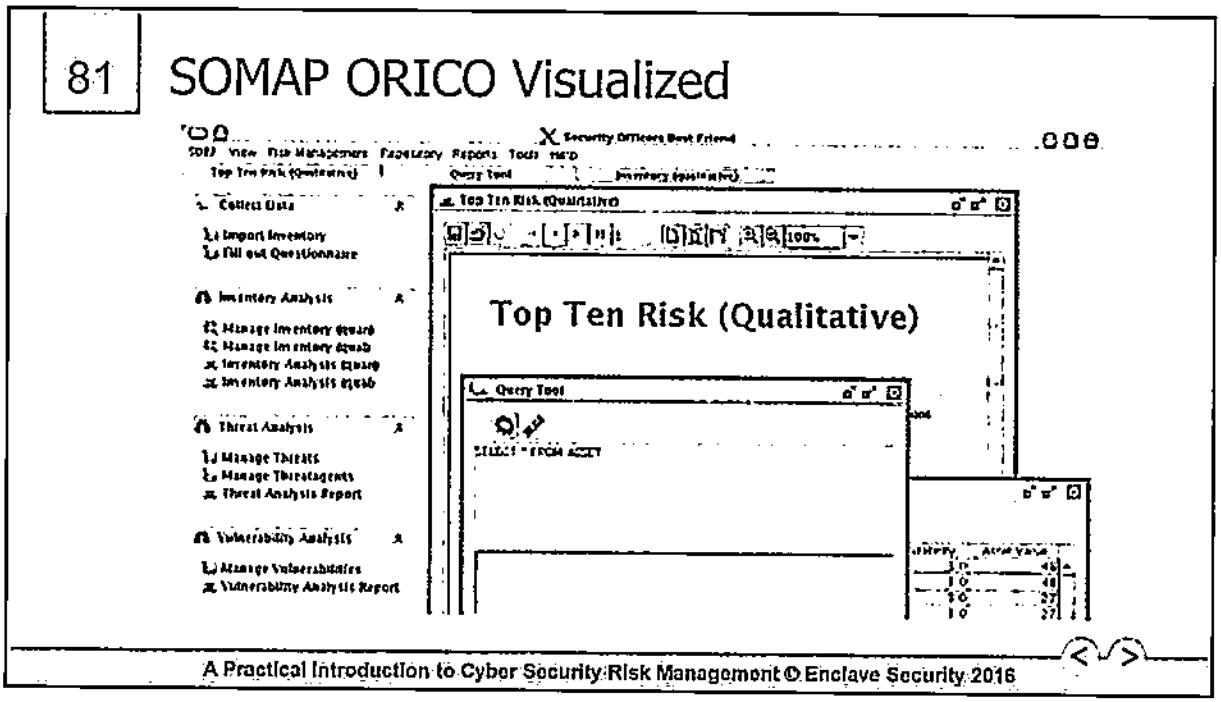


The first of the free tools for us to consider is from the Security Officers Management and Analysis Project (SOMAP) and is called their ORICO tool. As a quick definition, SOMAP defines their ORICO tool as:

"the reference implementation of our OGRCM3 methodology and follows the risk assessment and analysis workflow as described in our Guide." [1]

Currently there are two versions of the tools, one is a standard Windows desktop version of the tool and the other is a Java / web-based tool that can be used for collaboration purposes. If an organization is simply looking for a starter tool to begin working with risk management methods, then possibly the Windows-based tool makes the most sense to use. On the other hand, if a collaborative team, made up of varying business roles, is planning on taking advantage of the tool, then likely it makes the most sense to use the web-based version, which is the more functional of the two versions.

[1] SOMAP.org - Security Officers Management and Analysis Project. (n.d.). SOMAP.org - Security Officers Management and Analysis Project. Retrieved February 1, 2011, from http://SOMAP.org



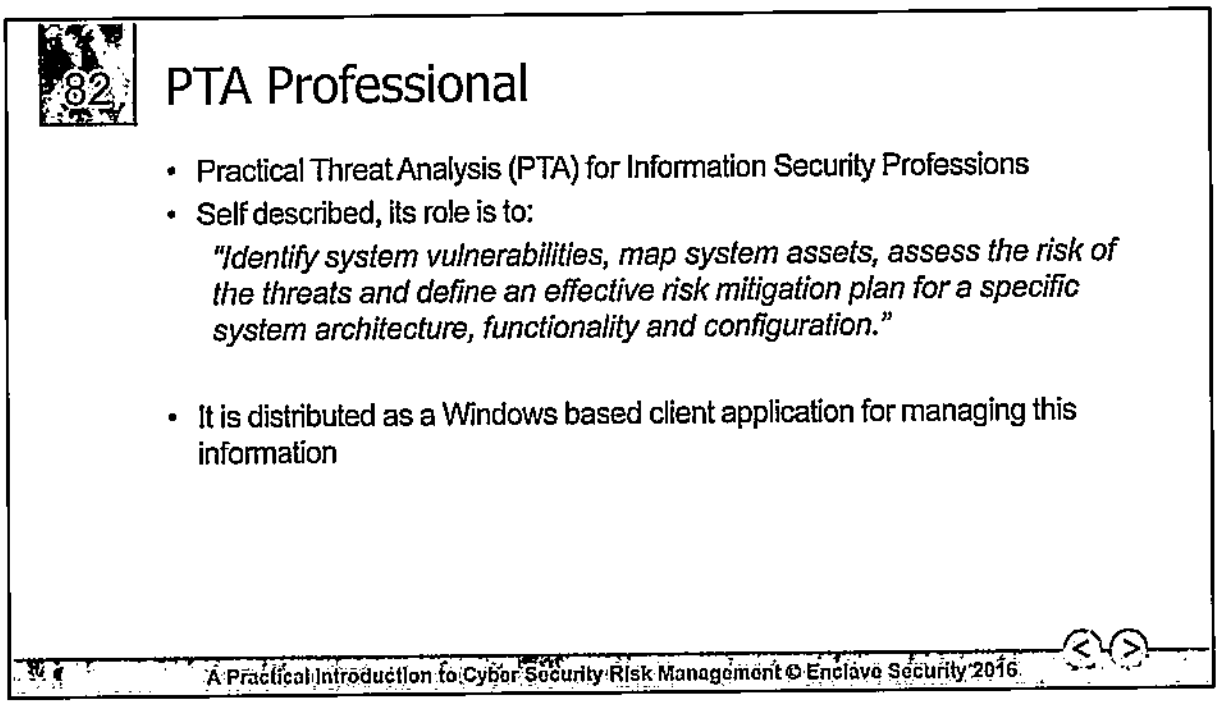
As with the commercial tools, which we will describe later, it may be helpful to hear from the developers of the tool directly what this tool has to offer. So, straight from the vendor's mouth, here is more information on the SOMAP ORICO tool:

"The ORICO Framework is the foundation for the ORICO Tool. Both build an Information Security Governance, Risk and Compliance application which can be used for Gap Analysis, Risk Analysis and as a general IT Security Risk Management tool. The ORICO Tool is the reference implementation of our OGRCM3 methodology and follows the risk assessment and analysis workflow as described in our Guide." [1]

"It is our goal to build the ORICO Tool like an extendable toolset. While all the needed functionality is built into the ORICO Tool, it is possible to extend and personalize that standard feature set with your own changes, scripts and extensions.

"To abstract the database and to access the data more easily, the ORICO tool makes use of the Cayenne Framework. The configuration information is published with the ORICO Tool and it is, therefore, possible to enhance the default configuration with your own data views and tables. Such personalized data views and tables can be used from within your own extensions to enhance the standard feature set of the ORICO tool. The ORICO tool makes heavy use of the structures and references from the Repository and features a layer with personalized data on top the theoretical layer provided by the Repository. The ORICO tool links theoretical information with a concrete inventory to help the security officer in analyzing and managing his or her assets. With the data and calculations from the ORICO Tool a security officer can generate reports about situations, gaps, protection profiles and the state of an environment."

[1] SOMAP.org - Security Officers Management and Analysis Project. (n.d.). SOMAP.org - Security Officers Management and Analysis Project. Retrieved February 1, 2011, from http://SOMAP.org

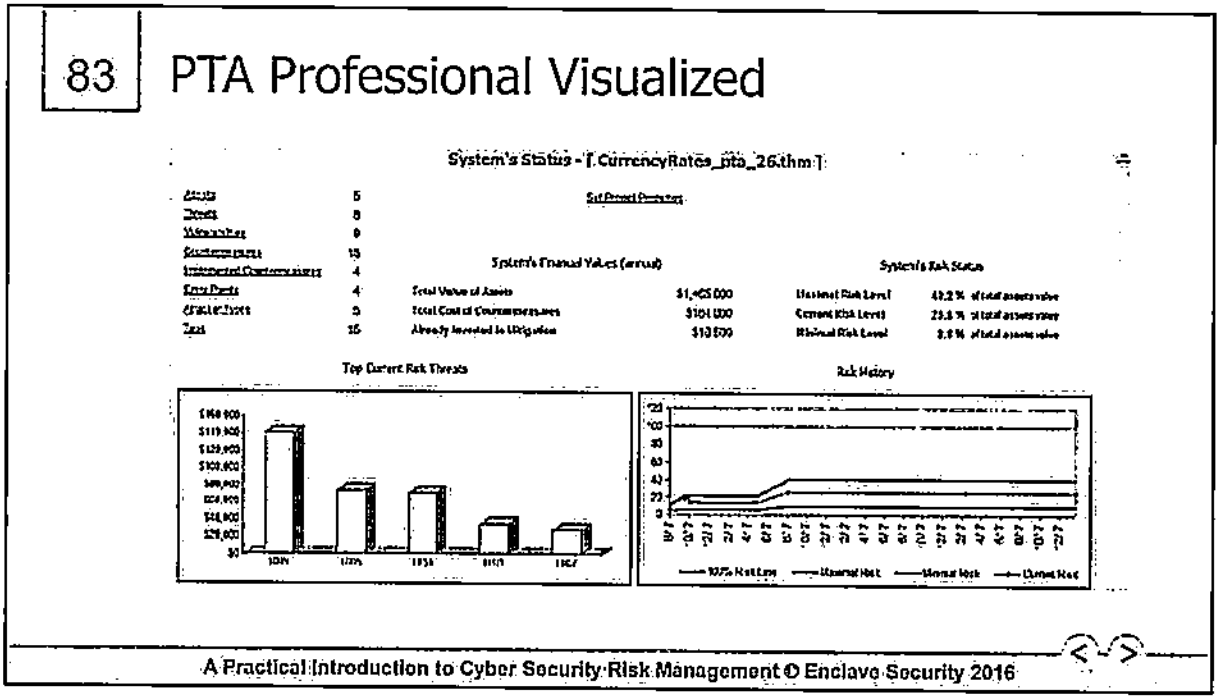


Another tool that organizations may want to consider taking advantage of being the Practical Threat Analysis (PTA) for Information Security Professions or PTA Professional tool. Again, as a self-described summary, this tool's role is to:

"Identify system vulnerabilities, map system assets, assess the risk of the threats and define an effective risk mitigation plan for a specific system architecture, functionality and configuration." [1]

This tool is a Microsoft Windows-based tool only and acts as a stand-alone desktop application. If an organization is simply looking for a more advanced way of utilizing the simple risk assessment model we described in the previous section, using a database driven tool with a few enhancements, then this is likely the best tool to consider. It basically uses a simple database model to reflect the risk information as described in the previous section.

[1] Practical Threat Analysis. (n.d.). http://www.ptatechnologies.com/. Retrieved February 1, 2011, from http://www.ptatechnologies.com/Documents/PTA_Calculative_Tool.pdf



As with the commercial tools, which we will describe later, it may be helpful to hear from the developers of the tool directly what this tool has to offer. So, straight from the vendor's mouth, here is more information on the PTA Professional tool (taken from http://www.ptatechnologies.com/DetailedLeaflet.htm):

"PTA (Practical Threat Analysis) is a risk assessment methodology and a suite of software tools that enable security consultants and organizational users to find the most beneficial and cost-effective way to secure systems and applications according to their specific functionality and environment.

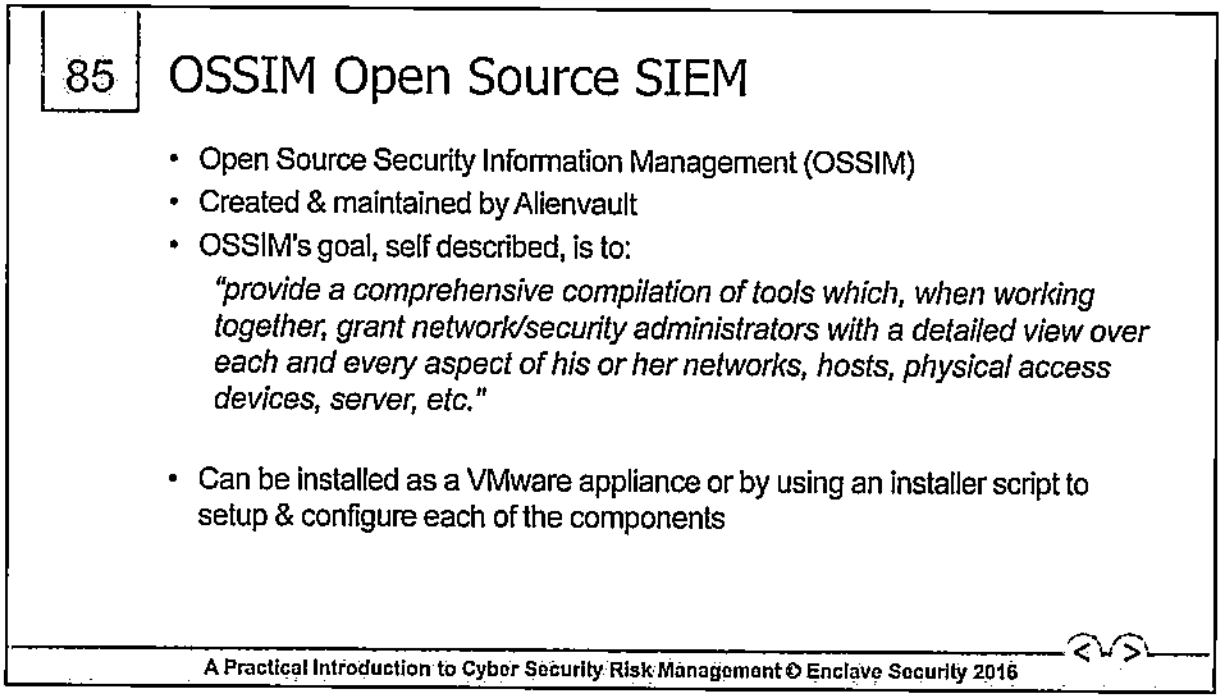
"The threat analysis process begins by describing the specific threats and vulnerabilities of the system. The threats are then associated with assets that might be damaged and the vulnerabilities they exploit. The process continues by automatically finding the exact set of countermeasures that will mitigate different threats. The risk level, potential damage and countermeasures required are all presented in real $ values. PTA automatically calculates the level of risk and the maximum available mitigation and advises on the most cost effective way to mitigate threats and reduce overall system risk.

"PTA was designed to assist the work of security consultants, software analysts and information security officers. PTA is a powerful yet easy to use risk assessment tool for analyzing systems threats. It speaks the practical language of business and enables analysts to clearly explain what is needed to be done in order to mitigate top threats in an optimized cost-effective way."

"Using PTA, analysts can quickly build threat models, analyze risks and decide upon risk mitigation plans and policies relevant to the business's domains. Inputs may be obtained from a variety of external and

internal sources e.g. vulnerability scanners, real-time network analyzers, security standards checklist, security event repositories as well as from the business management resources and accountants reports. The information can be entered manually as well as automatically."

"In addition to recommending the most cost effective countermeasures, PTA presents the current level of security of the monitored system. Once used, PTA enables dynamic changes in each of the defined threats, vulnerabilities, assets and countermeasures parameters. This allows an effective and continuous risk assessment and security management, throughout the business routine without duplicating efforts and at minimal cost."



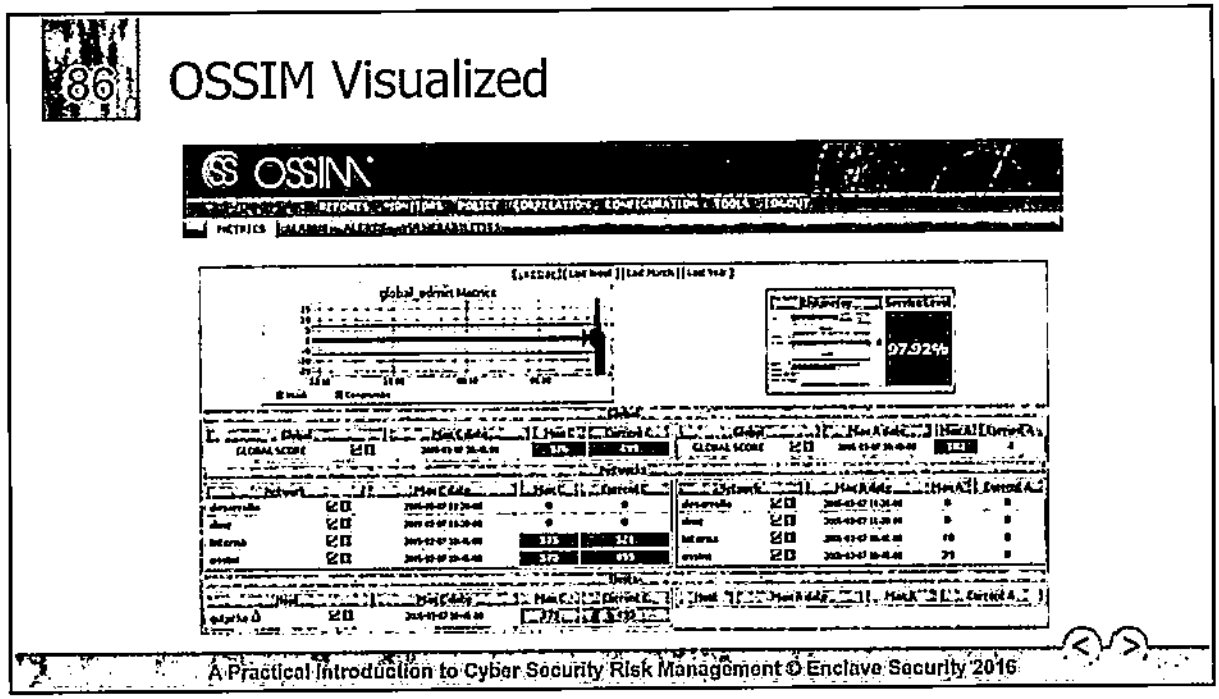
A final free tool is a tool created and maintained by a vendor known as Alienvault – this tool is known as the Open Source Security Information Management (OSSIM) tool. It is meant to be an open source SIEM product, with risk management functions (along with other GRC capabilities) built into the product. To be clear though, Alienvault offers both a commercial and a free version of their tool for organizations to use.

Self described, OSSIM's goal is to:

"provide a comprehensive compilation of tools which, when working together, grant network/security administrators with a detailed view over each and every aspect of his or her networks, hosts, physical access devices, server, etc." [1]

So as you can see, the purpose of this tool is to do more than simply keep track of risk related data sets. It functions partially as a SIEM and partially as a GRC tool, taking pieces from each to provide its overall functionality. OSSIM can be installed as a VMware appliance or by using an installer script to setup & configure each of the components. But in either case this is a complete operating system environment, or a new server, that will be residing on your network in order to achieve these goals.

1 Open-Source Risk Monitoring Platform. (n.d.). https://www.infosecisland.com. Retrieved February 1, 2011, from https://www.infosecisland.com/blogview/3813-Open-Source-Risk-Monitoring-Platform.html



As with the commercial tools, which we will described later, it may be helpful to hear from the developers of the tool directly what this tool has to offer. So straight from the vendor's mouth, here is more information on the OSSIM tool. [1]

"OSSIM stands for *Open Source Security Information Management*. Its goal is to provide a comprehensive compilation of tools which, when working together, grant network/security administrators with a detailed view over each and every aspect of his or her networks, hosts, physical access devices, server, etc.

Besides getting the most out of well known open source tools, some of which are briefly described below, OSSIM provides a strong correlation engine, detailed low, medium and high level visualization interfaces, and reporting and incident management tools, based on a set of defined assets such as hosts, networks, groups and services."

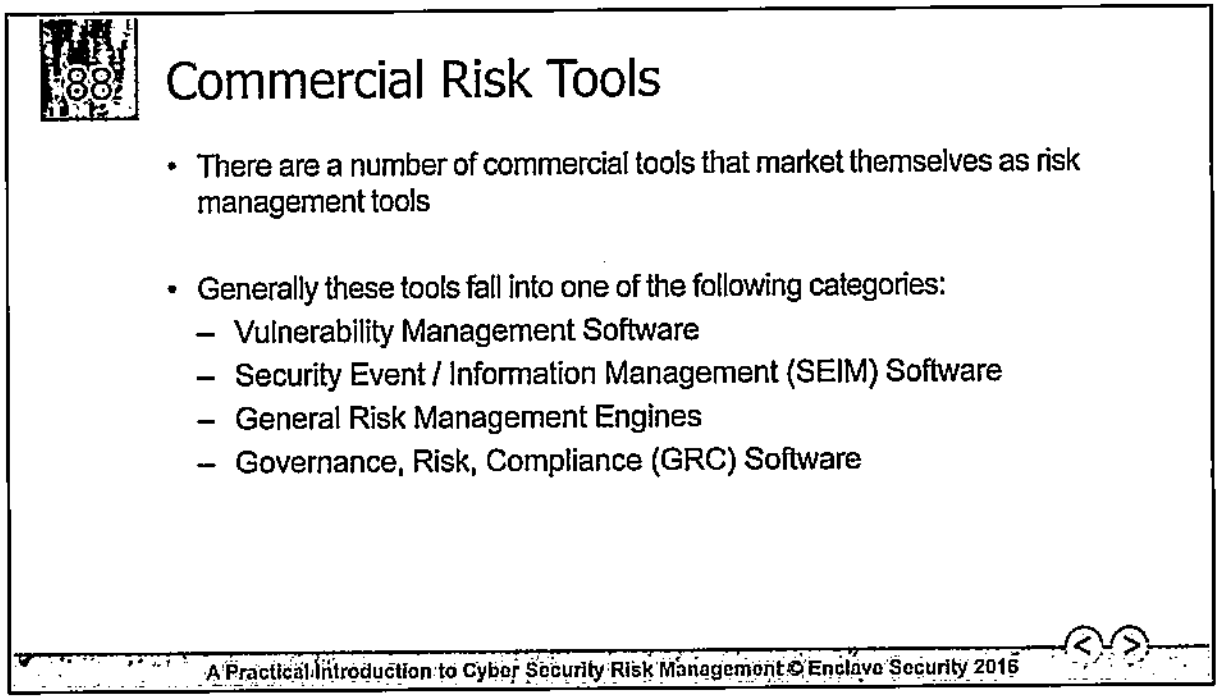
"All of this information can be restricted by network or sensor in order to provide only the required information to specific users; allowing for a fine grained multi-user security environment. Finally, the ability to perform as an IPS (Intrusion Prevention System), using correlated information from virtually any source, will be a useful addition to any security professional's arsenal.

OSSIM features the following software components:

- Arpwatch – used for MAC anomaly detection.
- P0f – used for passive OS detection and OS change analysis.
- Pads – used for service anomaly detection.
- Nessus – used for vulnerability assessment and for cross correlation (IDS vs. Security Scanner).

- Snort – the IDS, also used for cross correlation with Nessus.
- Tcptrack – used for session data information which can prove useful for attack correlation.
- Ntop – which builds an impressive network information database from which we can identify aberrant behavior/anomaly detection.
- Nagios – fed from the host asset database, it monitors host and service availability information.
- Osiris – a great HIDS.
- OCS-NG – cross-platform inventory solution.
- OSSEC – integrity, rootkit, registry detection, and more."

[1] AlienVault - Unified Security Management - Community. (n.d.). AlienVault - Unified Security Management. Retrieved February 1, 2011, from http://www.alienvault.com/community.php?section=Home

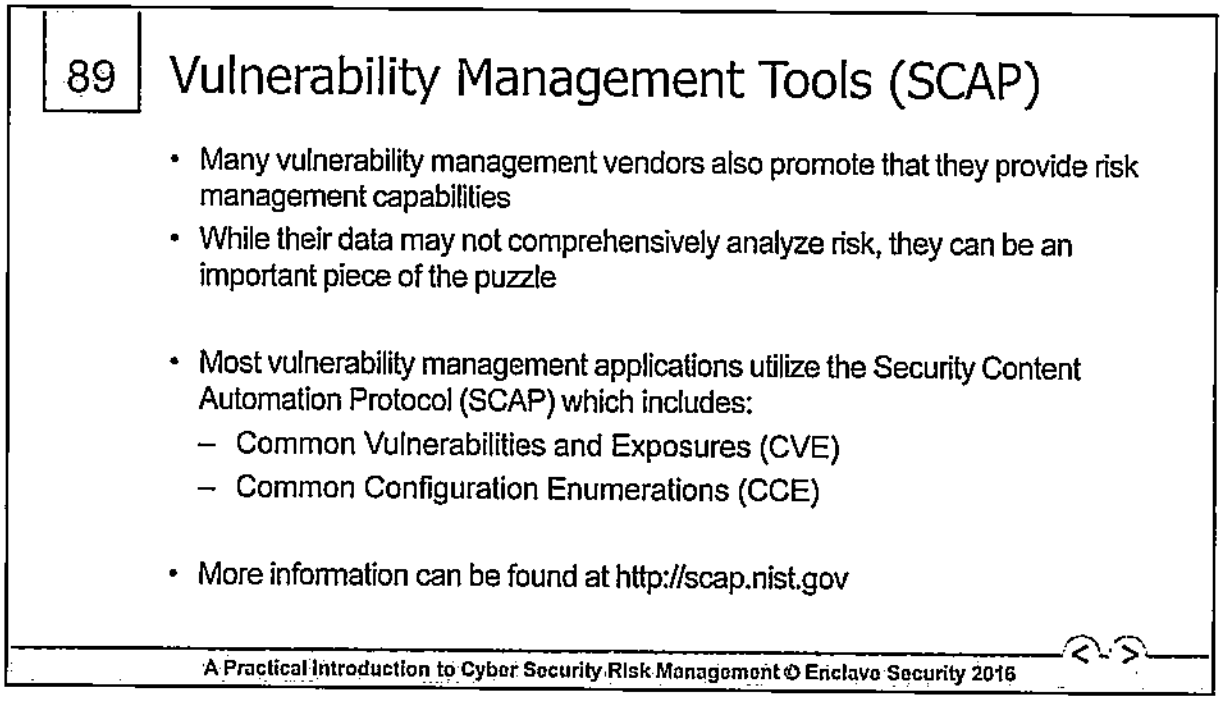


In addition to the open source or free tools we have just considered there are also a number of commercial tools that may also assist organizations in the process of risk management. Often times these software tools may make the process of risk management easier than the risk methodologies themselves.

Generally the software tools we are about to consider fall into the following categories:

- Vulnerability Management Software
- Security Event / Information Management (SEIM) Software
- General Risk Management Engines
- Governance, Risk, Compliance (GRC) Software

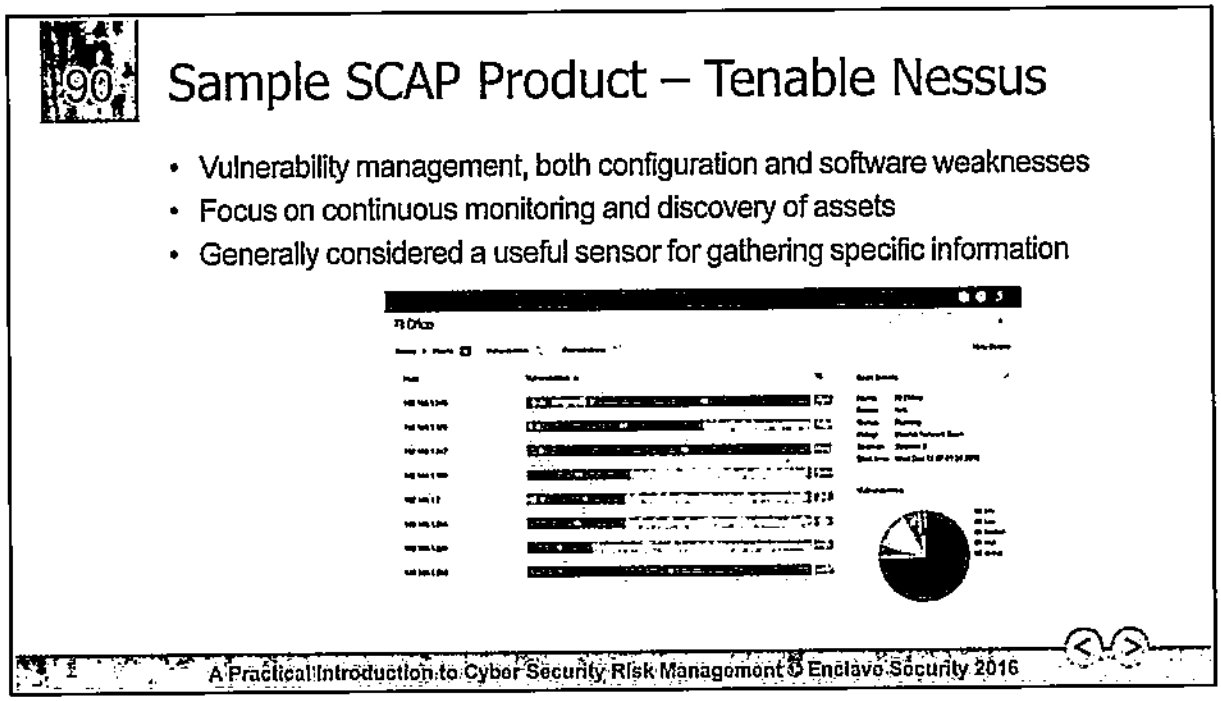
We will not discuss every possible tool in each of the categories listed above. However we will attempt to examine samples from each of these categories to help us better understand what each different tool offers. A thorough product evaluation is definitely necessary before an organization decides to purchase one or more of the tools we are about to discuss. It should also be noted that while we are talking about commercial tools in this section, mentioning such tools does not necessarily mean that we endorse the use of these particular vendors. Thorough product selection and procurement management is always valuable.



One of the types of products that an organization may find useful when performing risk management is a tool that has the ability to measure vulnerabilities on a system based on the technical configuration and state of the system. The US Government maintains a standard for performing such assessment, known as the Security Content and Automation Protocol (SCAP) which has the ability to provide organizations insight into such weaknesses.

Most products listed as vulnerability management products now utilize SCAP as the foundation for performing their assessment. This is primarily performed through the use of the Common Vulnerabilities and Exposures (CVE) and Common Configuration Enumeration (CCE) specifications, although others are available for use.

More information about the SCAP project, including a list of the vendors that have been certified as utilizing the latest version of the protocol can be found at http://scap.nist.gov.



One example of an SCAP based vulnerability scanning product is Tenable's Nessus family of products. This is a traditional SCAP vulnerability management solution with the ability to gather information on both configuration and software based vulnerabilities. It also includes capabilities for asset management and passive vulnerability assessment as well.

In their own words, from the company's website:

"SecurityCenter Continuous View is comprised of SecurityCenter, combined with the active scanning of Nessus, the passive scanning of PVS, and the log collection of LCE.

Nessus®
The most widely deployed vulnerability scanner for broad and deep scans of networks, systems, data and applications. Satisfies internal network scanning requirements for PCI.

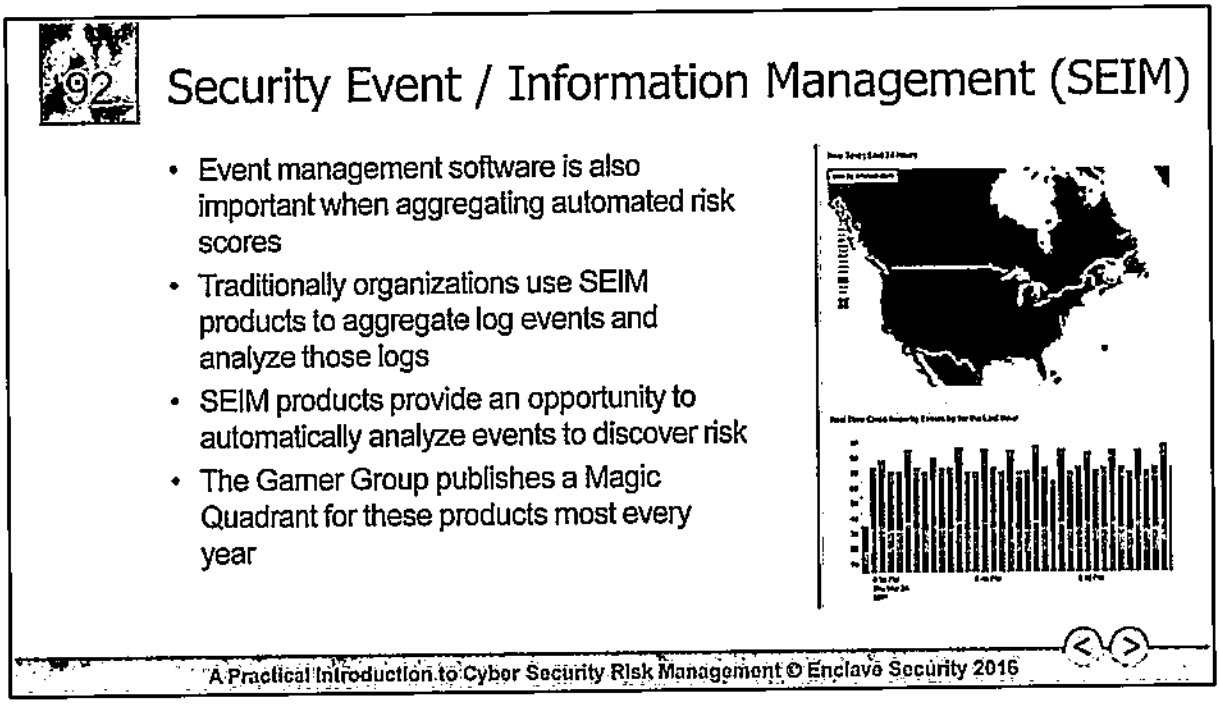
Passive Vulnerability Scanner™
Monitors network traffic in real-time to detect new hosts, services, protocols and applications for security and compliance violations.

Log Correlation Engine™
Collects and aggregates data from network and security infrastructure, raw network traffic and user activity to detect complex malware, isolate threats and compliance issues."

Product Features

- Unlimited active scanners with Nessus
- Industry's largest vulnerability database, with plugins updated daily
- Extensive compliance reporting and auditing
- Granular, customizable dashboards and reports updated via live feed
- Supports IPv6 address space
- Integrates with Mobile Device Management (MDM) and Patch Management Systems Third-party security and threat intelligence
- Detects, classifies, and scans mobile devices
- Real-time botnet and advanced malware detection. Performs attack paths analysis
- Discovers 100% of IT assets for vulnerability assessment
- Continuous, real-time vulnerability analysis through patented passive monitoring
- Performs database monitoring and detects encrypted communications
- Real-time detection and analysis of mobile, virtual systems and cloud-services
- Detects network anomalies and performs event correlation
- Collects, stores, compresses and correlates logs from thousands of network devices and applications
- Aggregates and normalizes data from FWs, IDS/IPS, and DLP solutions, raw network traffic, NetFlow, application logs, user activity, etc."

Taken from http://www.tenable.com/products/securitycenter-continuous-view/features.



Another toolset that organizations may want to consider as a component of their risk management architecture are Security Event / Information Management (SEIM) systems. These systems are generally used to aggregate events from system logs and then analyze those logs for events of interest. SEIMs provide organizations with an automated mechanism to collect and analyze system events for potential indicators of risk.

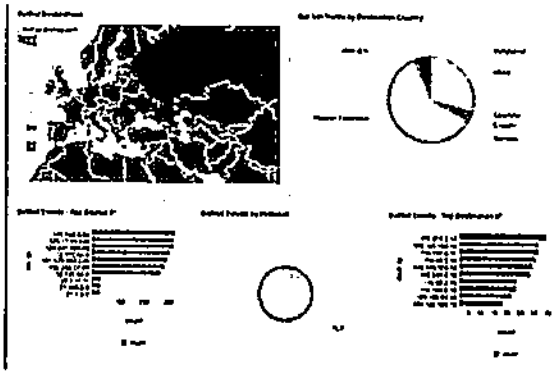
We will discuss more about event based risk assessment in an upcoming session.

As one can vaguely see from the graphic on the slide, the Gartner Group does have a Magic Quadrant study that they publish on this subject. For organizations looking to learn more about the available vendors, this resource may be helpful in performing their vendor selection.

93

Sample SEIM Product - Splunk

- Commercial log aggregation and analysis tool, that also provides risk assessment
- Risk measurements tend to be more event oriented
- Also integrates information from threat intelligence sources



A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

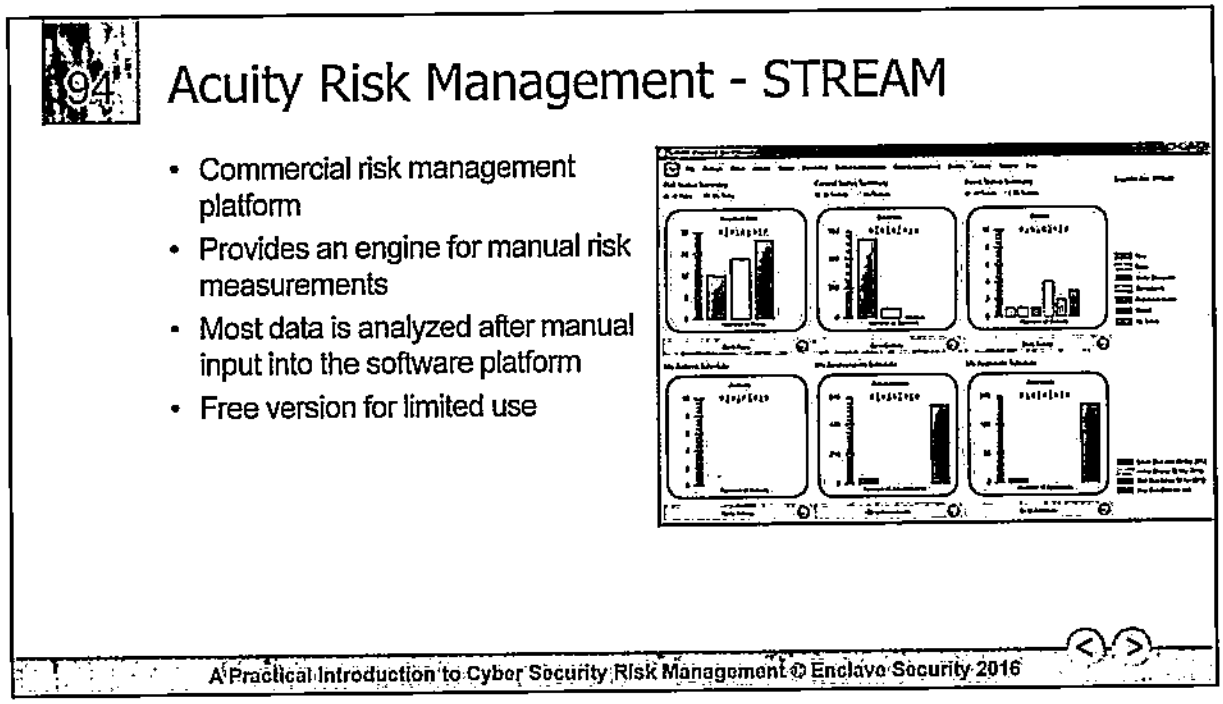
One example of a SEIM product is the commercial Splunk utility. Splunk gives organizations the ability to perform log aggregation from a number of systems and provides an enterprise with a consolidated view of event based risks. Organizations can even use plugins from their Splunkbase to extend the functionality of their analytics engine based on specific types of data aggregated by the system.

In their own words, from the company's website:

"By monitoring and analyzing everything from customer clickstreams and transactions to security events and network activity, Splunk Enterprise helps you gain valuable Operational Intelligence from your machine-generated data. And with a full range of powerful search, visualization and pre-packaged content for use-cases, any user can quickly discover and share insights. Just point your raw data at Splunk Enterprise and start analyzing your world.

Collects and indexes log and machine data from any source
Powerful search, analysis and visualization capabilities empower users of all types
Apps provide solutions for security, IT ops, business analysis and more
Enables visibility across on premise, cloud and hybrid environments
Delivers the scale, security and availability to suit any organization
Available as a software or SaaS solution."

Take from http://www.splunk.com/en_us/products/splunk-enterprise.html.

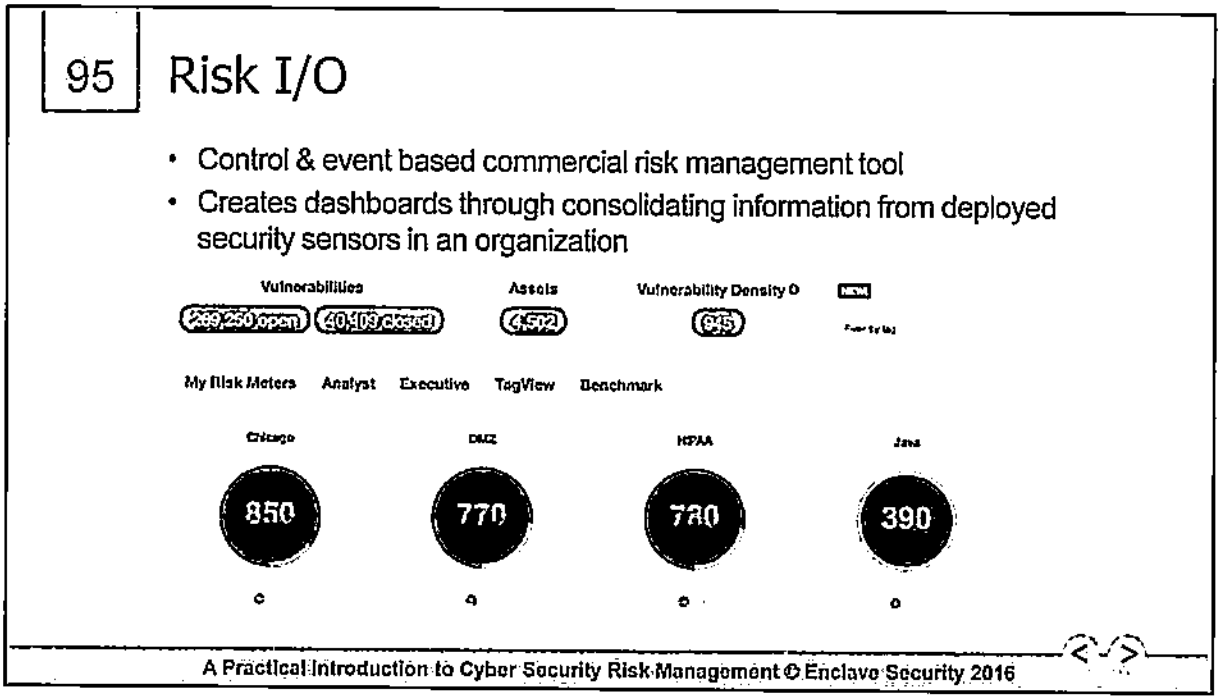


Acuity Risk Management's STREAM software is an example of a traditional risk management solution for organizations where they can analyze manually inputted data sets an report on the risk they have identified. While it may not be as event or sensor based as the other tools, its simplicity makes it easy for organizations to get started using their software. They even make a free version of their tool available for limited use.

In their own words, from the company's website:

"STREAM is an expertly engineered software solution which is easily configurable via the user interface. STREAM can be customized with libraries of controls, risks, incident categories and asset lists within a few hours. Users can upload pre-configured content from Acuity or easily add their own content to quickly build their own integrated solution covering any GRC category - from cyber risk, IT assurance and supply chain management to Enterprise Risk Management. The STREAM Product Portfolio consists of the STREAM software, pre-configured Application content and Productivity Utilities. Multiple editions of the STREAM Single - User (SU) and Multi - User (MU) software are available to match your GRC requirements and budget. Application content includes catalogues of controls, risks, asset classes and assessment schemes with various mappings which can be uploaded to the STREAM software. Productivity Utilities allow you to quickly and easily upload your own content to the STREAM Software."

Taken from http://www.acuityrm.com/.

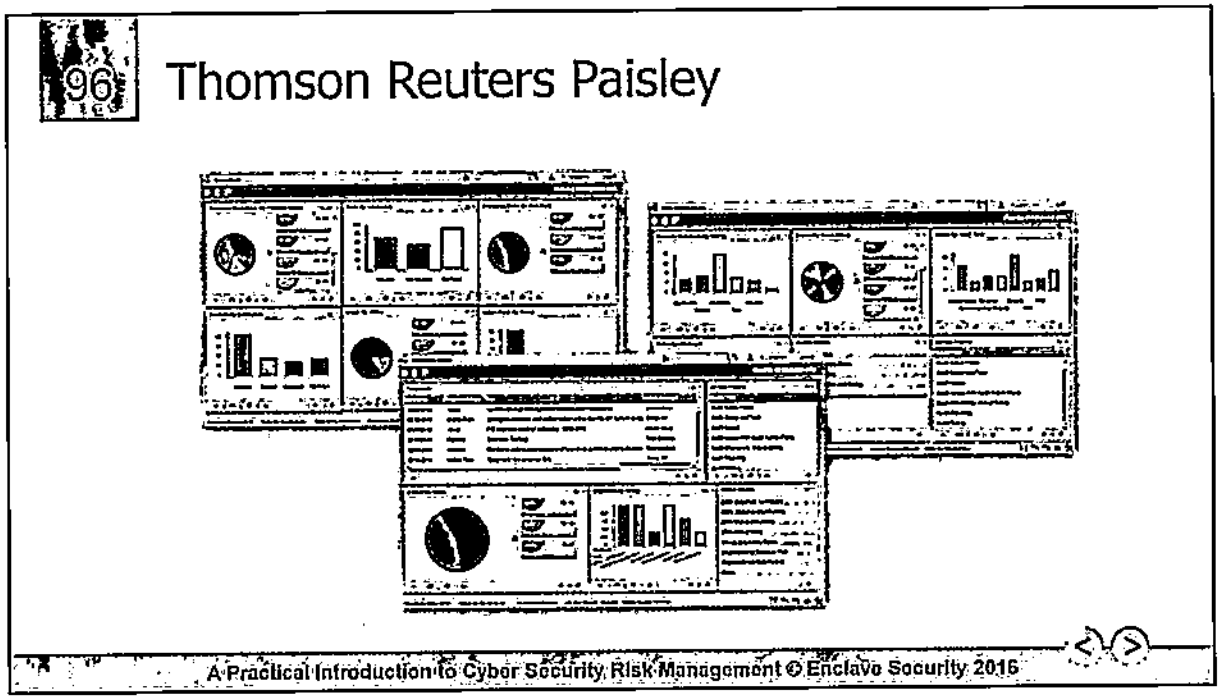


Risk I/O has seen that many organizations are simply using Microsoft Excel to perform their risk assessments and as a result has created an engine to make it easy for organizations not interested in deploying a full GRC engine to take baby steps into risk management. Their commercial solution makes it easy for organizations to create initial risk dashboards based on the sensors they have deployed.

In their own words, from the company's website:

"Risk I/O's threat processing & vulnerability management program continuously aggregates attack data, threat data, and exploit data feeds covering attacks in-the-wild, zero-day vulnerabilities, and active Internet breaches. A single day of Risk I/O threat processing is the equivalent of 475,000 security analysts matching known breaches and attacks against your vulnerabilities. Risk I/O correlates the attack, threat and exploit data aggregated by our threat processing engine against your vulnerabilities twenty-four hours a day, seven days a week. Simply connect your vulnerability scanner to Risk I/O and our vulnerability management program will identify where, when and how your organization is most likely to be attacked. A risk meter is a real-time measure of the risk a group of assets pose to your organization, and can be created for those critical systems in your environment you'd like to monitor. The Risk Meter dashboard gives your team and management a quick, at-a-glance view of your vulnerability and exploit risk across your business, categorized by what's meaningful to you."

Taken from https://www.risk.io/features.



One of the more popular GRC tools available is the Paisley tool by Thomson Reuters. The Paisley tool is one of the top performers consistently indicated in Gartner's magic quadrant on the topic, and, therefore, we are mentioning it here in class.

But rather than trying to explain this tool ourselves, to be fair to the vendor, let's listen to what they have to say regarding their own product .[1]

"The increase in government regulations, growing pressure from financial markets and additional compliance requirements has heightened the focus on integrated governance, risk and compliance. Traditional approaches to governance, risk and compliance have relied upon separate point solutions to address the requirements of each business process and each new wave of regulatory requirements. This fragmented approach leads to inefficiencies, added costs and an inability to maintain compliance initiatives and make informed and accurate decisions.

Thomson Reuters offers a more effective, proven approach to optimizing governance, risk and compliance business processes with Paisley *Enterprise GRC* and **GRC on Demand**. These comprehensive governance, risk and compliance solutions provide unique profiles for each user group, a central data repository and common functionality for risk assessment, reporting and issue tracking across GRC disciplines.

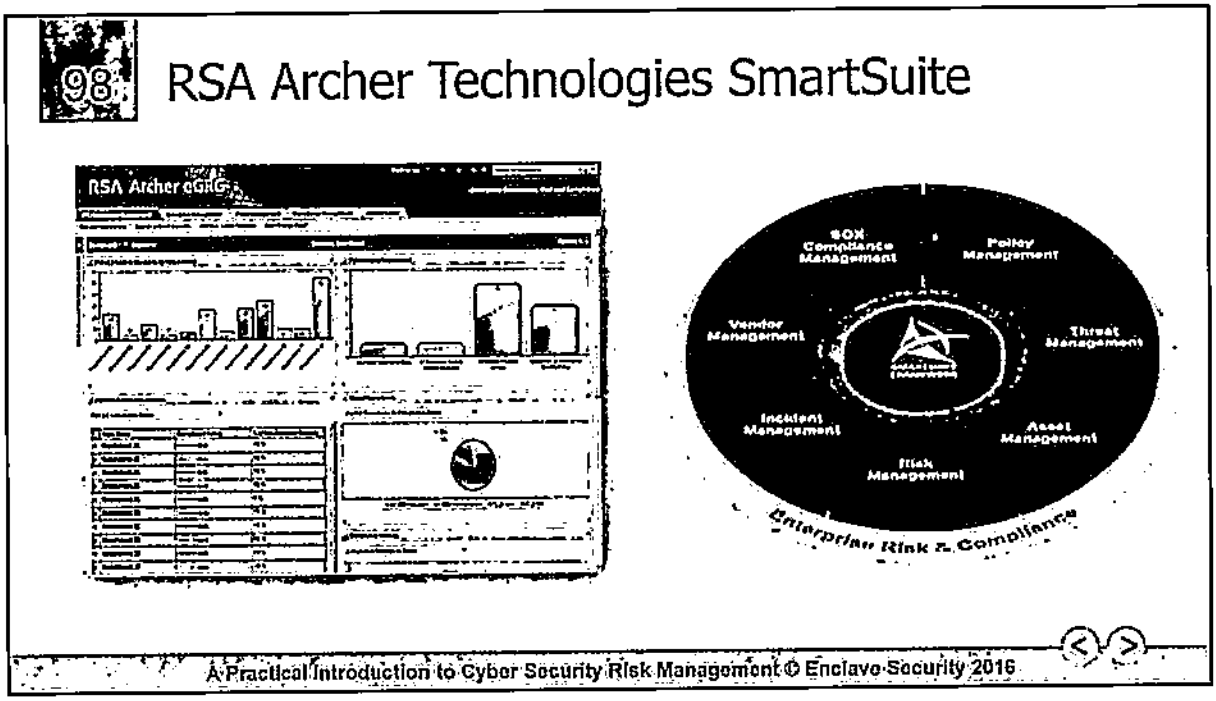
In addition to comprehensive GRC software solutions AutoAudit helps to streamline the audit process, enables audit departments to complete all their work in a single, shared, secure system. The software provides modules for risk assessment, planning, scheduling, work papers, reporting, issue tracking and administration.

Optimized for large enterprise organizations, Paisley *Enterprise GRC* is a comprehensive governance, risk and compliance software solution that is available for either on-site installation or delivery via a hosted application deployment model.

Optimized for mid-market and resource constrained organizations, **GRC on Demand** is a comprehensive governance, risk and compliance solution that is delivered via a Software as a Services model.

A fully integrated audit automation system, AutoAudit allows audit departments to complete their work in a single database. With modules for risk assessment, planning, scheduling, work papers, reporting, issue tracking and administration, it's the most complete way to manage an audit department."

[1] Governance Risk & Compliance, GRC, Financial Controls Process Management - Paisley. (n.d.). Internal Audit, Risk Management, Compliance and GRC Software. Retrieved February 1, 2011, from http://paisley.thomsonreuters.com/website/pcweb.nsf/pages/CIRE-6LTSE2



Another GRC tool commonly employed by organizations for the purpose of managing risk and other GRC issues is Archer Technologies' SmartSuite tool. Like the Paisley tool, it is commonly regarded as one of the more popular GRC and ERM tools for managing these issues at an enterprise level.

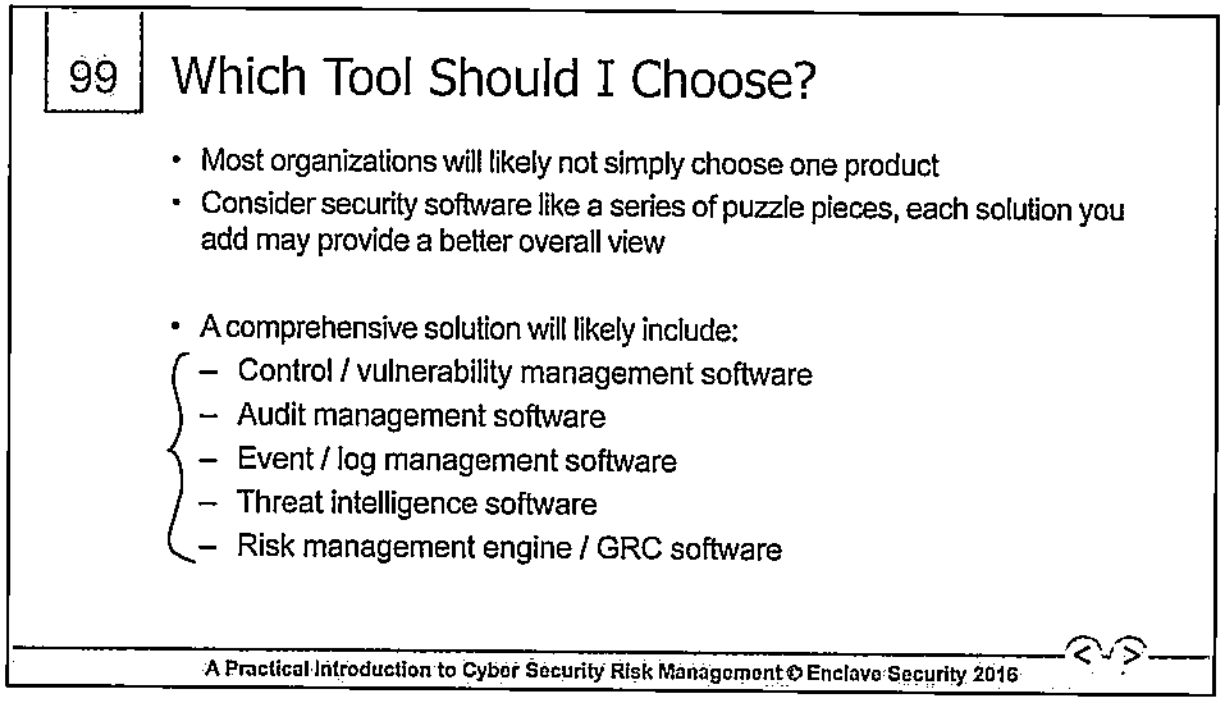
Again, let's see what Archer Technologies has to say about its own tool.[1]

"The Archer SmartSuite Framework is a platform for building on-demand applications and packaging them into solutions to solve business problems. The Framework enables you to choose the most appropriate environment for your applications and to transport them between environments as your needs change.

The applications and solutions you can build with the Archer SmartSuite Framework are limited only by your imagination. Through a simple wizard-driven interface and drag-and-drop functionality, you can build anything from project management applications, to trouble ticketing systems, to customer relationship management solutions.

The Archer SmartSuite Framework puts control into the hands of your business people, allowing them to build and manage their own applications without requiring IT resources. And with a thriving Archer Community and the Archer Exchange, you have an ecosystem of tools, services and collaboration to fuel your success."

[1] Darbyshire, J. (n.d.). GRC Blog | Governance, Risk and Compliance News | Archer Technologies. Enterprise Governance, Risk and Compliance | RSA Archer eGRC Solutions | RSA, The Security Division of EMC . Retrieved February 1, 2011, from http://www.archer.com/solutions/index.html

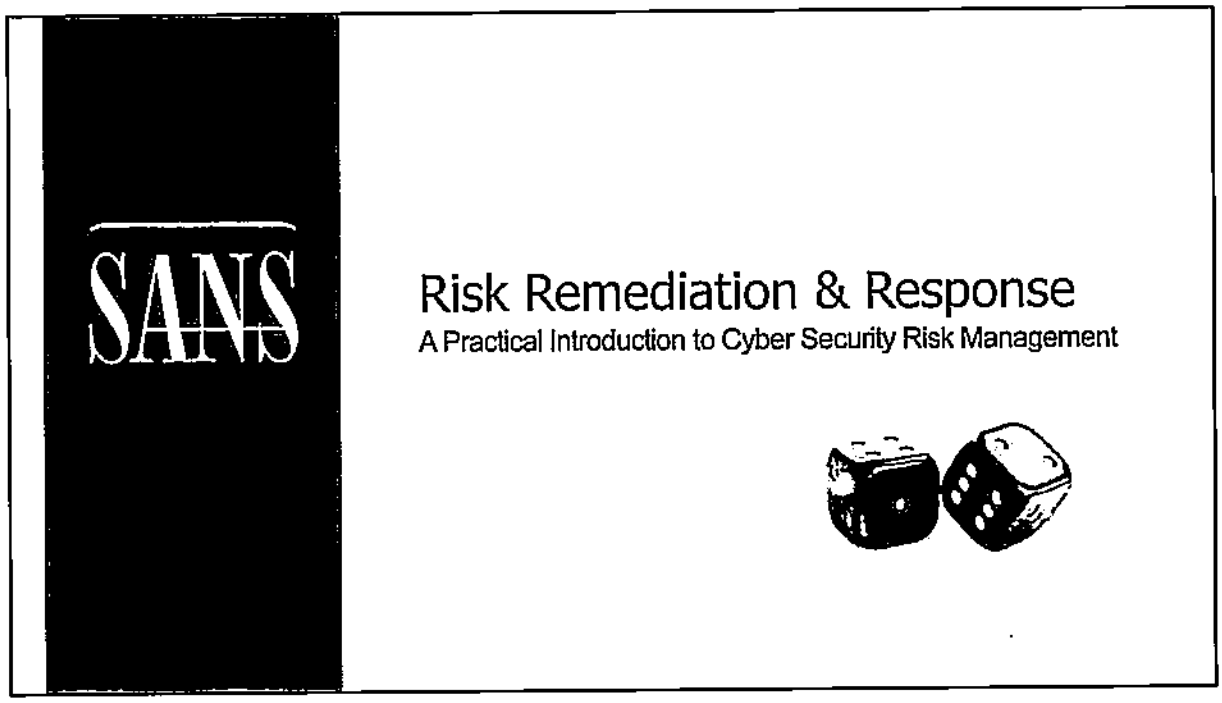


Although each of the tools that were just discussed could be used as a part of a risk management architecture, likely one tool by itself will not provide an organization with all of the capabilities that they are hoping to have in their risk management catalog. Likely a number of data sources, when combined together, will provide an organization with the best view of the risk facing their systems. The best way to think of this picture is to consider security software like a series of puzzle pieces. With each puzzle piece that you implement you receive a bigger view of the overall picture and better insight into the big picture.

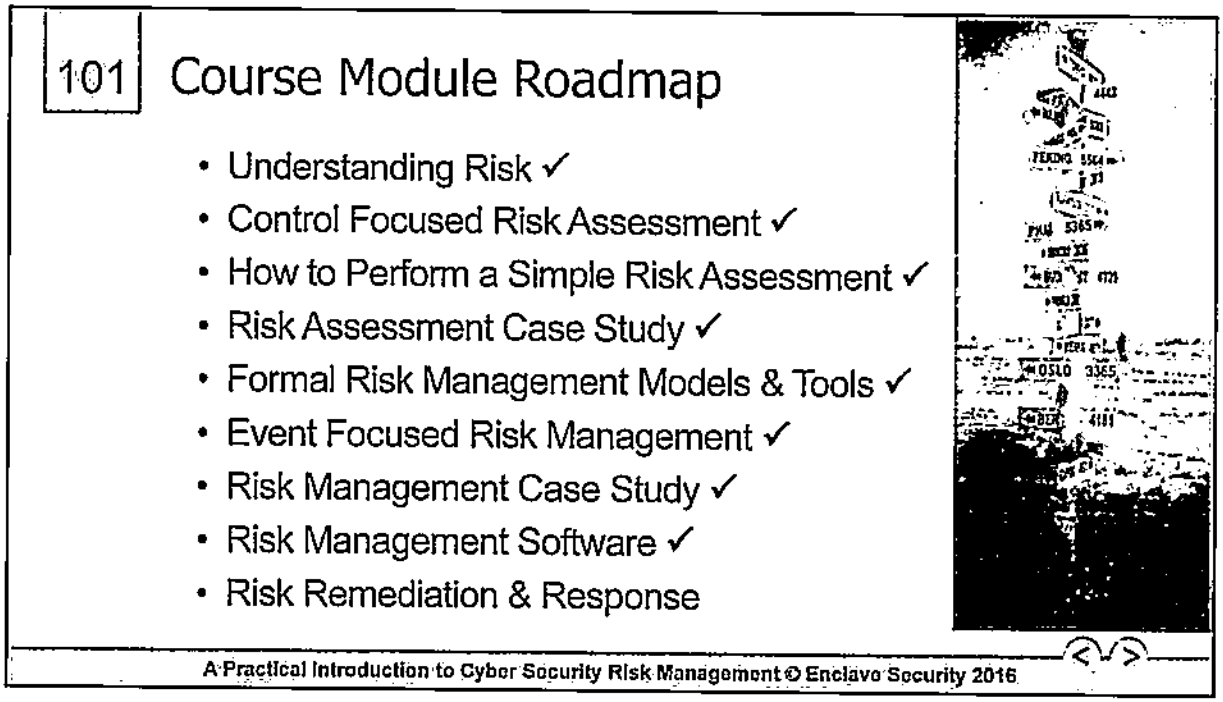
A comprehensive risk management solution, based on security software, will likely include at a minimum the following puzzle pieces:

- Control / vulnerability management software
- Audit management software
- Event / log management software
- Threat intelligence software
- Risk management engine / GRC software

SANS Internet Storm Center.



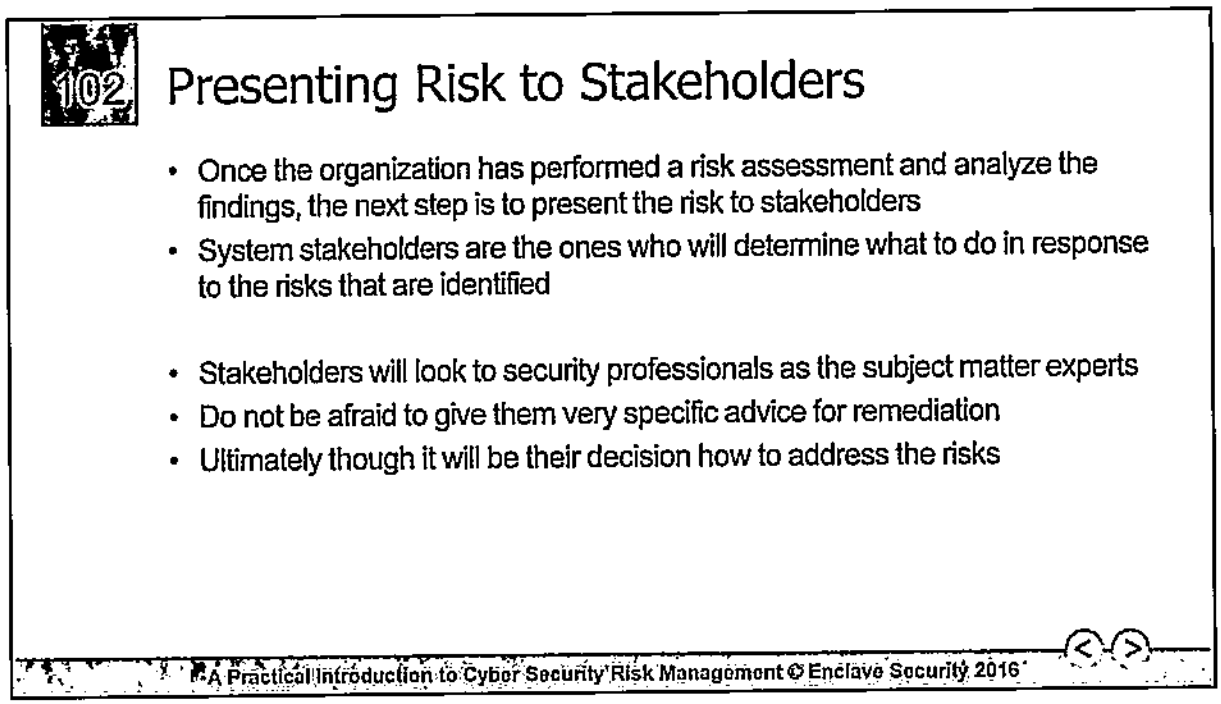
This page intentionally left blank.



In this course we will explore the concept of risk and its practical impact on an organization. Ultimately the goal of this course is to prepare students to effectively utilize risk assessment as a tool for enterprise defense. Too many times organizations think of risk assessment and risk management as academic tools with little to no practical application. These concepts are often viewed as a formal task to pursue when an organization has free time rather than as a core business activity that drives other enterprise security efforts. In today's course students will have the opportunity to learn about the proper place of risk assessment and risk management in an enterprise. They will also be given practical skills for how to perform a risk assessment on a step by step basis, from data collection to the point of presenting their findings to business leaders. Students with a desire to perform more in depth analysis will also be given tools and formal models to consider to empower them to create a long term / formal risk management program.

Specifically today we will cover the following subjects:

- Understanding Risk
- Control Focused Risk Assessment
- How to Perform a Simple Risk Assessment
- Risk Assessment Case Study
- Formal Risk Management Models & Tools
- Event Focused Risk Management
- Risk Management Case Study
- Risk Management Software
- Risk Remediation & Response



We are now at the stage of the risk management cycle where action is required. A risk assessment has been performed, the outcome of the assessment has been analyzed, and therefore the next step in the process is to present the identified risks to the system's key stakeholders. These stakeholders are the people in the organization who ultimately will decide how to address the risks that were documented in the risk assessment.

Often times stakeholders will not be experts, however, in the risks that are identified and therefore they will look to security professionals for specific recommendations. So please do not be afraid to give very specific recommendations in the course of an assessment. Ultimately it is there decision how to proceed. But the advice of security professionals is often taken quite seriously, especially when they can clearly communicate the risk.

103 Defining Business Stakeholders

- So who exactly are business stakeholders?
- From the Project Management Body of Knowledge (PMBOK):
- "An individual, group or organization who may affect, be affected by, or perceive itself to be affected by a decision, activity or outcome of the project."

- Specifically then in terms of risk:
  - Executive leadership
  - System owners / sponsors
  - System custodians
  - End users of the system

The discussion on the previous slide then begs the question – so who exactly is a business or key stakeholder?

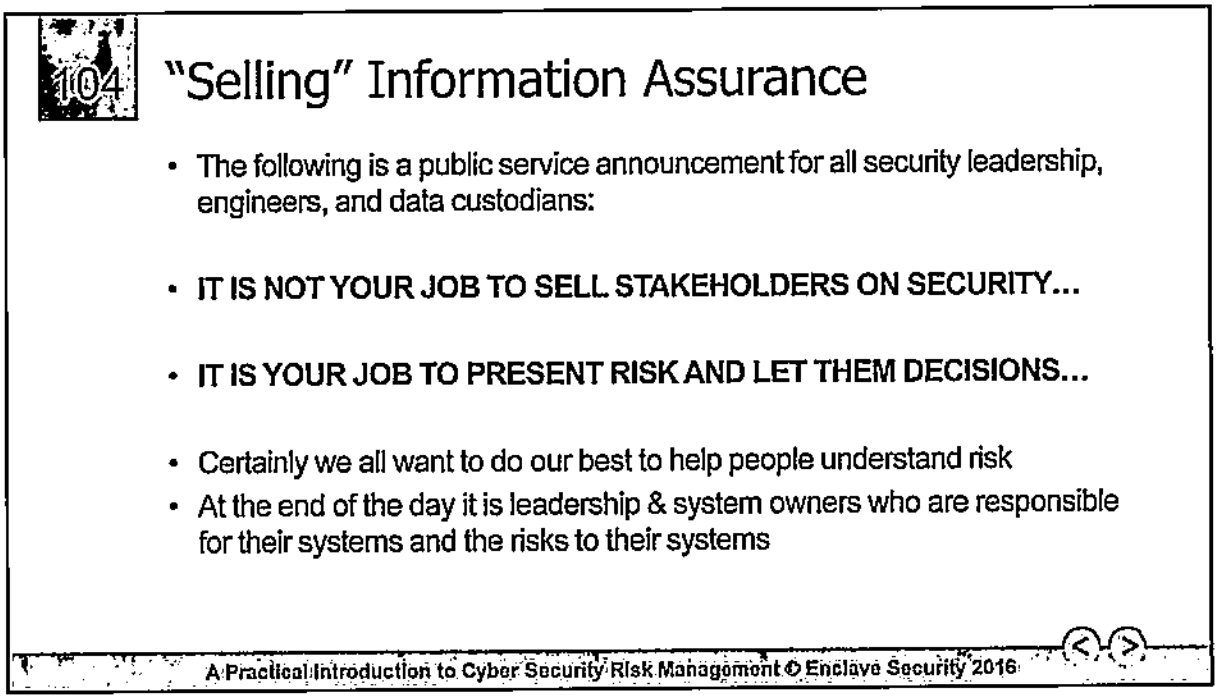
It seems the best way to answer that question is to look to the project / program management community for their definition, since at it's heart this is a project / program management term. Therefore for definitions of terms such as this, most will refer to the Project Management Institute (PMI) and their Project Management Body of Knowledge (PMBOK). The PMBOK defines a stakeholder as:

"An individual, group or organization who may affect, be affected by, or perceive itself to be affected by a decision, activity or outcome of the project."

In terms of risk management and organizational leadership, this means that most likely it will be one of the following roles that fits that description:

- Executive leadership
- System owners / sponsors
- System custodians
- End users of the system

Ultimately though, stakeholders are whoever the organization defines stakeholders to be. Ideally these are formally defined for each system.

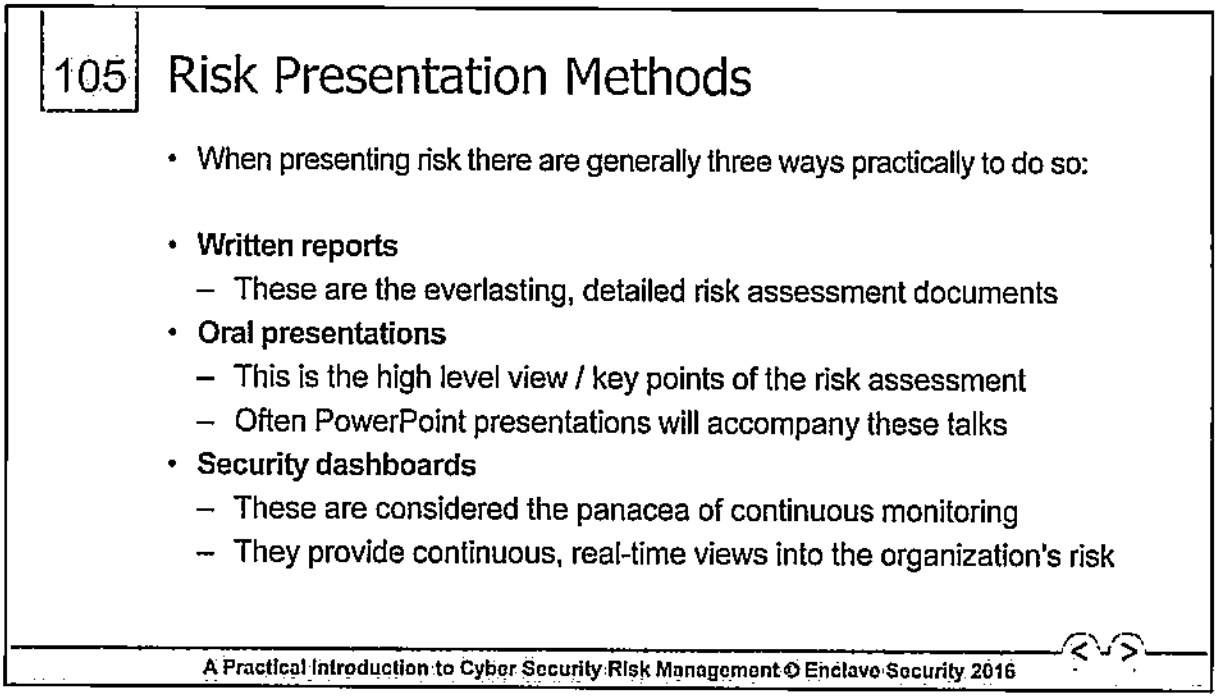


These are important points and we cannot stress them enough. Security professionals tend to take high degrees of ownership when it comes to the security risk on systems. Their role includes security management and therefore they often assume security risk. However, unless your role includes the ability to approve budgets and allocate how sufficient personnel spend their time:

IT IS NOT YOUR JOB TO SELL STAKEHOLDERS ON SECURITY...

IT IS YOUR JOB TO PRESENT RISK AND LET THEM DECISIONS...

It is most definitely our job to communicate risk to our best ability and be a resource to data owners. However it is not our job to "Sell" security. Business owners either believe in its importance or they do not. If a manage treats employees unethically, it is not our job to "Sell" them on the importance of ethics. That's a decision they need to make for themselves. We can mentor the people who report to us on the importance of security, but it is not our job to "Sell" the concept to those higher up in the food chain. Convince where you can, but let them take the responsibilities that comes with their title.

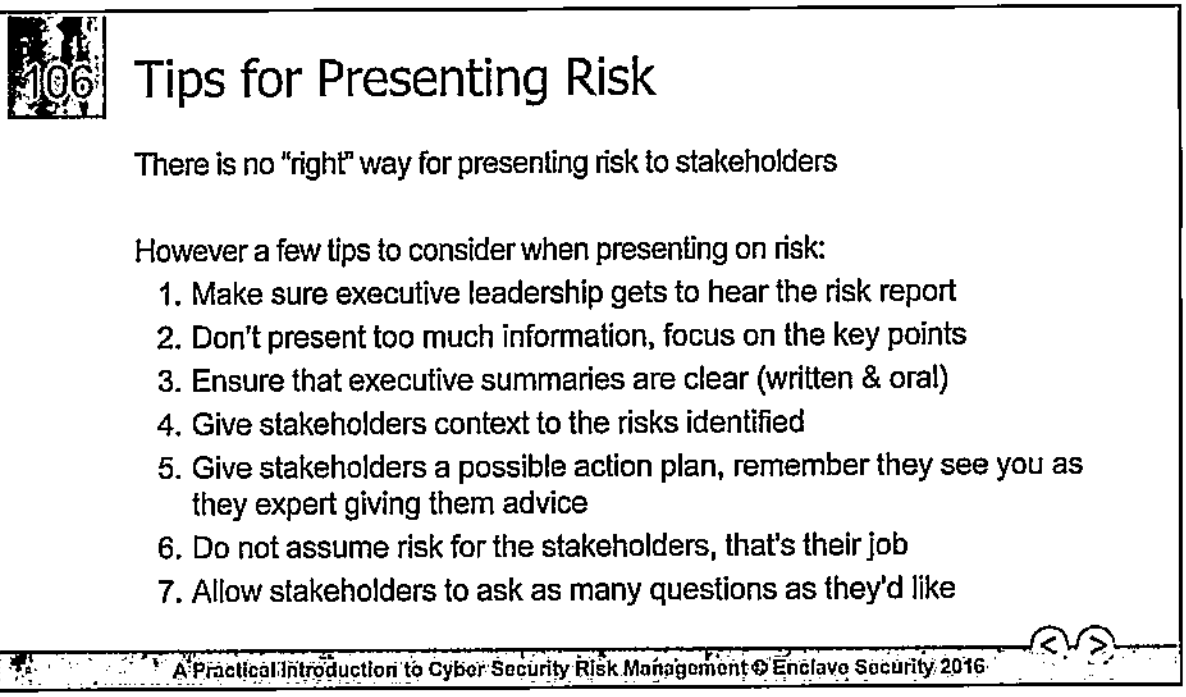


When it comes time to formally presenting risk, there are a few methods data custodians can take. Generally there are three common ways that data custodians can take to present information to key stakeholders. Those methods are:

1. Written reports:
   When formally presenting risk, these are the lasting documents that communicate the details about the risks you have identified during a risk assessment. Most other mechanisms are ephemeral or documented at a high level. These documents will describe in detail the risks identified for future generations and are the core component of any risk presentation. Like any executive presentation they should be written colorfully and in a way that is easy to understand, even for non-technical readers.

2. Oral presentations:
   Oral presentations are most often used to supplement the written reports that are submitted. They are generally written at a much higher level and include the key points of the risk assessment, but not necessarily every detail. Most organizations will use PowerPoint as a tool to complement these presentations, but are not always used. Some organizations we have encountered have moral opposition to the software – so always check before you present.

3. Security dashboards:
   Many organizations are moving their reporting capabilities to security dashboards for more continuous monitoring focused risk assessments. Rather than quarterly / annual risk presentations, there is real time monitoring available to all key stakeholders through the use of a security dashboard. Stakeholders who use these systems are able to stay informed on a more regular basis and with more effectiveness than the other options listed.



When it comes down to it, there really is no "right" way to present risk to stakeholders. Everyone will have ideas about what is right for their organization. However there are some tips that the course authors have learned over the years regarding how to make it more effective to present risk to stakeholders.

You will need to figure out what works best in your organization to effectively communicate these risks, but a few of the tips we would suggest are:

1. Make sure executive leadership gets to hear the risk report
2. Don't present too much information, focus on the key points
3. Ensure that executive summaries are clear (written & oral)
4. Give stakeholders context to the risks identified
5. Give stakeholders a possible action plan, remember they see you as they expert giving them advice
6. Do not assume risk for the stakeholders, that's their job
7. Allow stakeholders to ask as many questions as they'd like

107 Potential Responses to Identified Risks

- Once the organization (stakeholder) has been presented with the identified risks, then a decision must be made
- Ideally an organization will always fully remediate all risks, but often that choice is just not practical

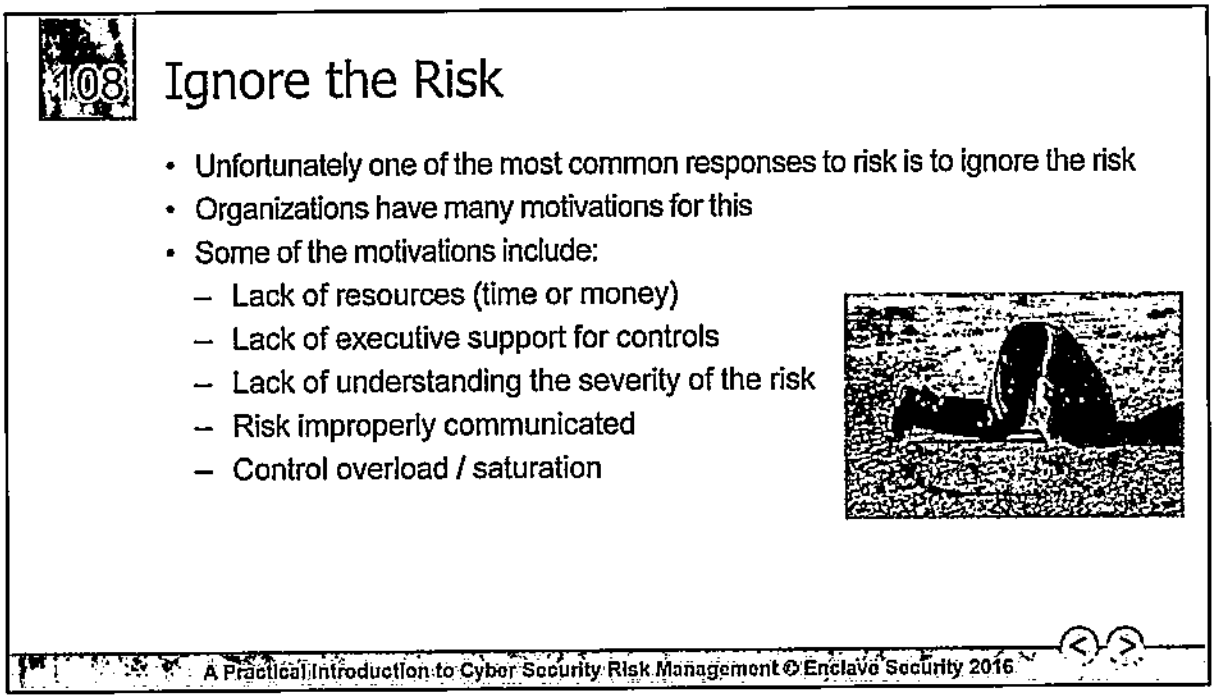
- There are generally five possible responses to identified risks:
  - Ignore the Risk
  - Accept the Risk
  - Mitigate the Risk
  - Remediate the Risk
  - Transfer the Risk

A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

Once the organization has identified the potential risks to their information systems, the next step is for the organization to determine how they are going to respond to those risks. In an ideal world every organization would identify all of their risks and completely remove those risks from becoming reality. Unfortunately though personnel and financial resources are limited for most companies, so the idea of completely removing all risk is simply unrealistic. It's not practical to address risk to the level we would always like.

Therefore, organizations must make the hard business decision sometimes, how to respond to the risk that's been identified. Generally speaking most would determine that there are five possible responses to identified risks:

- Ignore the Risk
- Accept the Risk
- Mitigate the Risk
- Remediate the Risk
- Transfer the Risk

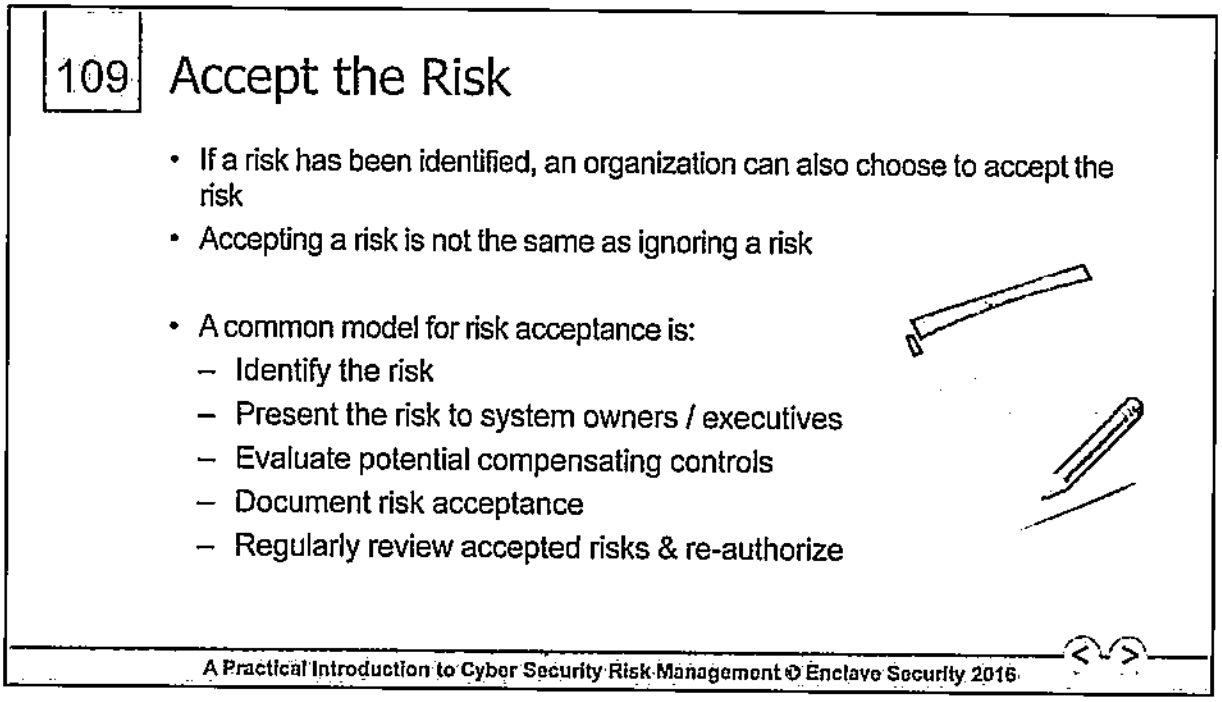


The first potential answer to risk is for an organization to decide to ignore the risk that has been identified.

Unfortunately this is one of the most common responses to identified risks today. Rather than properly deal with the risk in a decisive manner, organizations choose to simply ignore the risk and hope that it goes away. They ignore the risks in the hope that no one will notice, and there will not be any significant loss to the organization as a result. This is the, "let's cross our fingers and hope for the best", approach to risk management.

There are certainly many motivations why an organization may choose to go down this road. While none of these are acceptable reasons, and none of these reasons justify the response, these are common reasons why this might occur:

- Lack of resources (time or money)
- Lack of executive support for controls
- Lack of understanding the severity of the risk
- Risk improperly communicated
- Control overload or saturation



The second choice, although it does not actually do anything to lower risk levels, is at least a more appropriate risk response than to simply ignore the risk. Just because an organization has identified a risk, it does not mean that the organization necessarily has to do anything about it.

For example, most of us realize if we look at the history of the earth that every once in a while large rocks (meteors) fall from the sky and land on the earth, causing substantial damage along the way. That being said there is always a risk that our data centers might be hit by one of these falling objects and be completely taken offline. In spite of this, most of us do not have meteor shields covering our data centers in the case of falling objects. Instead, we choose to accept the risk of these meteors and not respond with additional controls. This is risk acceptance and it is a normal part of risk management.

However, if an organization decides that the most appropriate response is to accept a risk, then they need to document that they have accepted the risk and assign a person's name next to who has chosen to accept the risk. Most often this is the data owner or the person responsible for funding controls.

A common model for risk acceptance therefore would be:

- Identify the risk
- Present the risk to system owners or executives
- Evaluate potential compensating controls
- Document risk acceptance
- Regularly review accepted risks and re-authorize the acceptance of risk

Who Accepts Risk? Who does Not?

- Security leadership needs to be clear on who is responsible for risk
- Too many security leaders assume risk they cannot accept
- Who is able to formally accept system risk?
  - Formally defined system business / data owners
  - Executive management
  - Those in the organization with budgetary authority
- Who is not able to formally accept system risk?
  - Security leadership
  - Security engineers
  - System / network administrators
- This only changes in cases of custodial neglect or error

Although it's been stated earlier in the course it is important to repeat that security leadership needs to be clear on who is responsible for risk and who is allowed to accept risk inside of an organization. Too many security leaders or engineers assume responsibility for risk that they simply cannot accept.

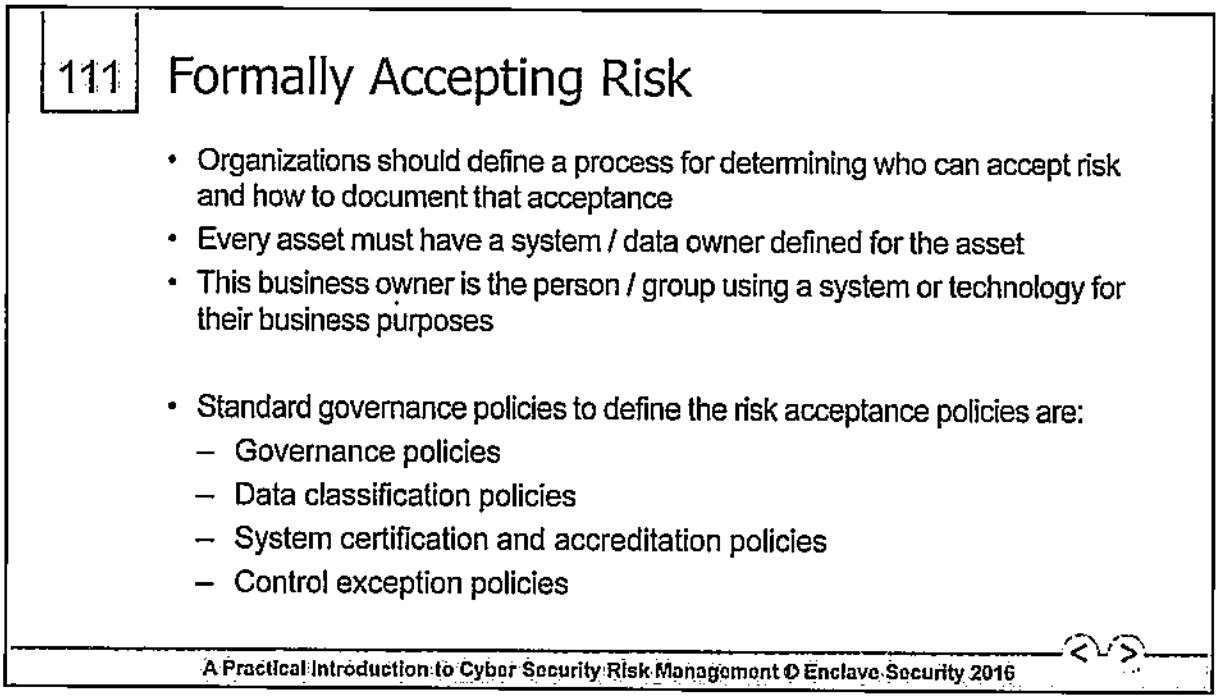
So, then who can accept risk? Who in the organization can take this responsibility? In the opinion of the course authors, only the following stakeholders can accept risk:

- Formally defined system business / data owners
- Executive management
- Those in the organization with budgetary authority

Said another way, who then cannot accept risk? It is the belief of the authors of this course that the following stakeholders should not be accepting risk:

- Security leadership
- Security engineers
- System / network administrators

The only time this really changes is in the case of data custodian neglect or error. Even then, business owners should have monitoring processes in place to look for these issues. Again, it is the business owner that ultimately owns all risk.



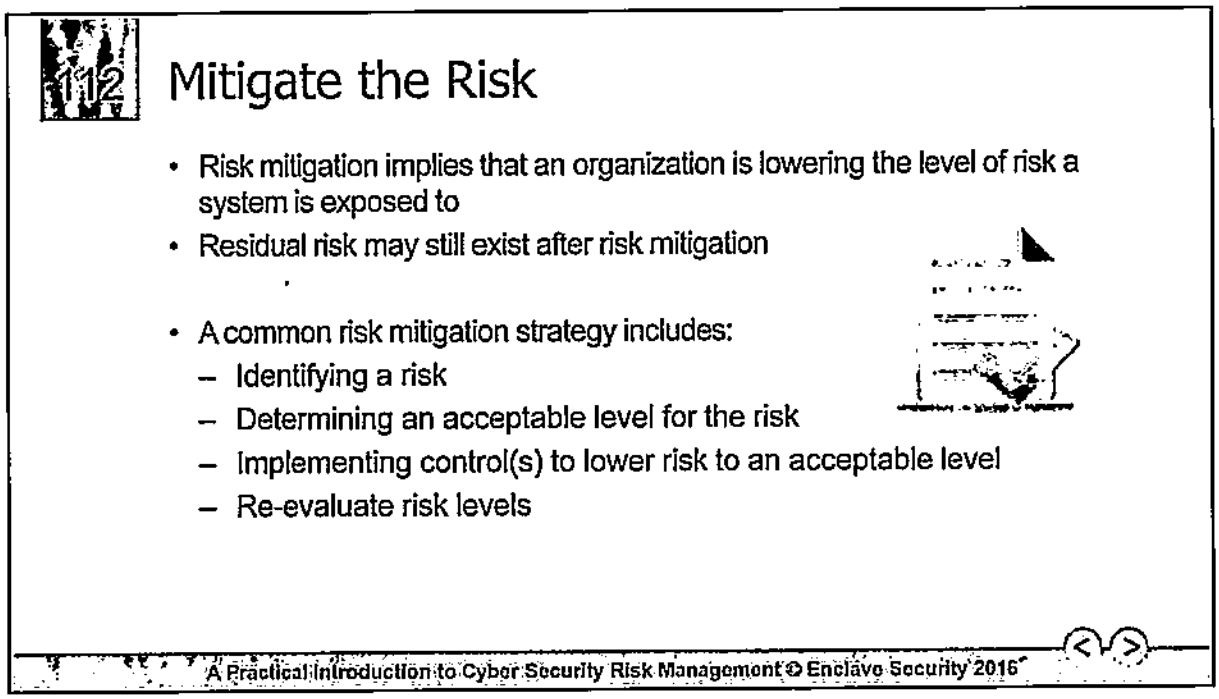
Having defined who can and who cannot accept risk, the question must also be considered, how can a stakeholder formally accept risk? This process is generally left to every organization uniquely, but involves a documentation process. There should be a formally documented definition somewhere in the organization for both who is allowed to accept risk and how that accepted risk is to be documented so everyone clearly understands the process.

Every information system or information asset should have a formally assigned data owner. That owner is most often the person in the organization who benefits the most from the implementation of the system or maintenance of the information. Or said another way, often they are the stakeholder that paid for the system and maintains it.

Most organizations will document this process is one or more of a few specific policies. The policies which most often contain this information are:

- Governance policies
- Data classification policies
- System certification and accreditation policies
- Control exception policies

There may be other names for these policies, but they will be similar to those listed above.

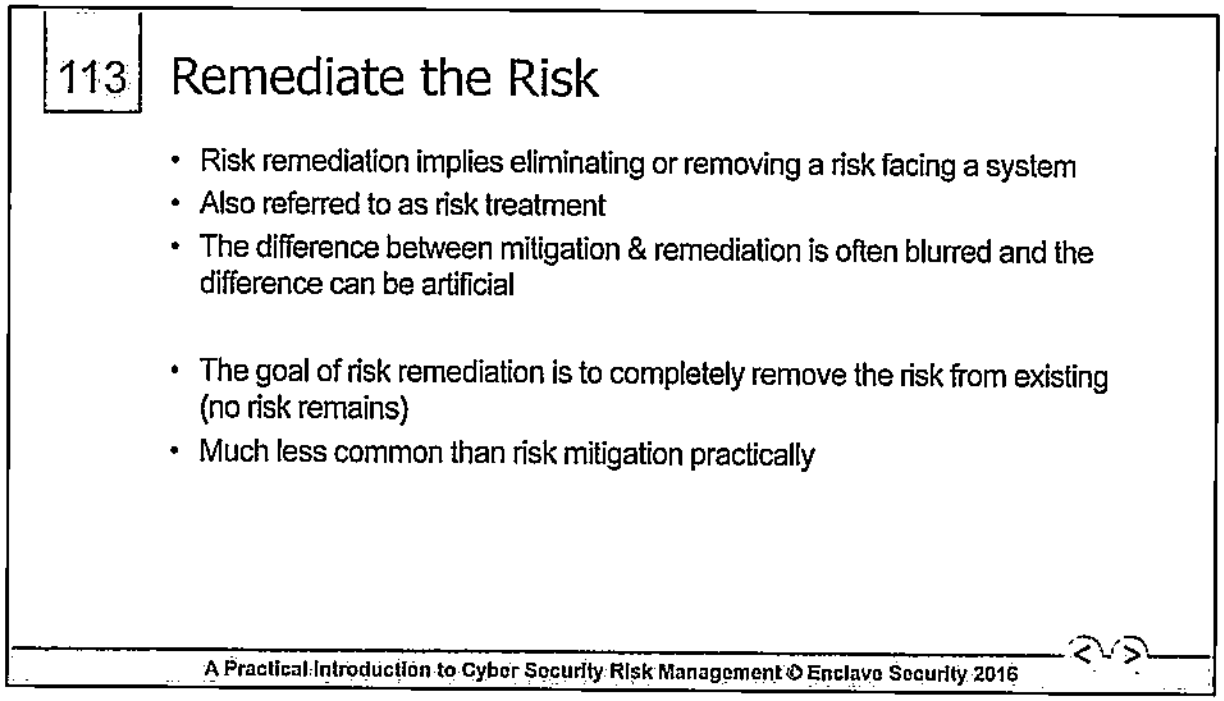


Another option organizations have is to choose to mitigate the risk. Risk mitigation implies that an organization is lowering the level of risk a system is exposed to, rather than completely eliminating the risk. The thing to remember about this option is that residual risk levels will still exist even after risk mitigation has occurred.

This approach is what most organizations choose to do when they implement an information assurance control. They know that the control will not absolutely protect them, but it will do a good enough job of lowering the risk to an acceptable level. For example, when you install whole disk encryption on mobile devices, it lowers the risk, but it does not eliminate the risk of data theft. An attack still might compromise user credentials or break the encryption employed. Therefore, a risk still exists, although lowered, and the control would be an example of a mitigating control.

One strategy for risk management that you may employ when your organization chooses to perform risk mitigation includes:

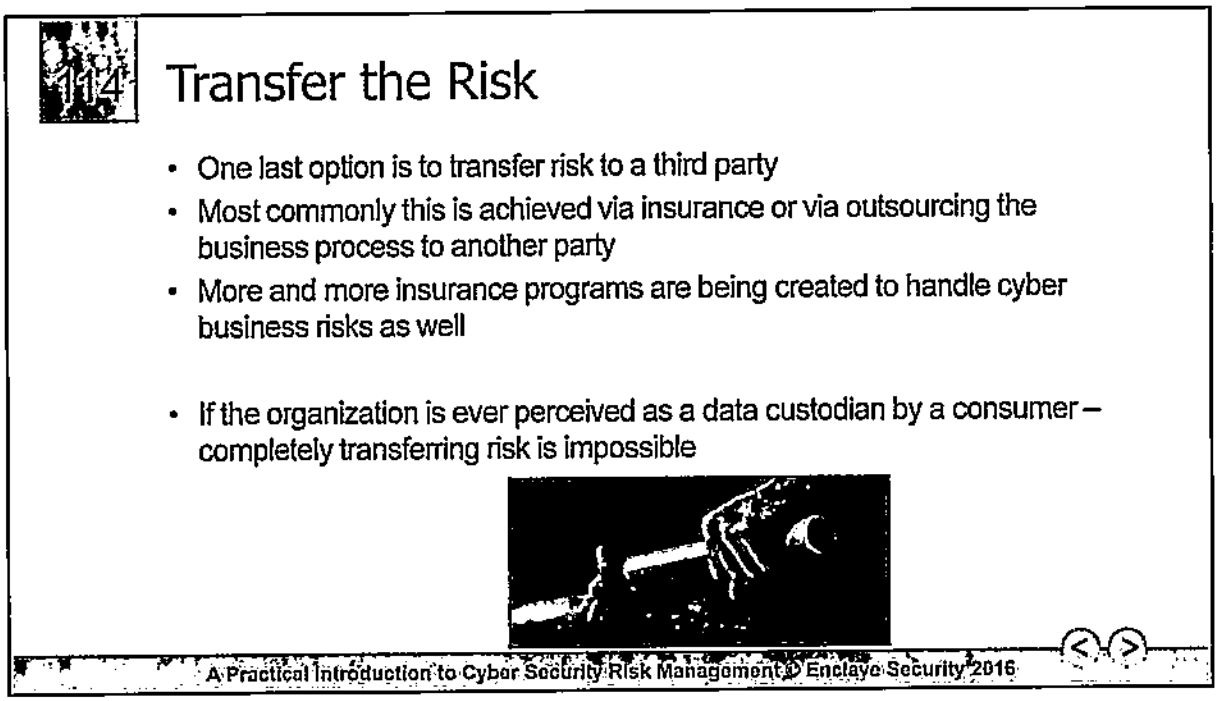
1. Identifying a risk
2. Determining an acceptable level for the risk
3. Implementing control (s) to lower risk to an acceptable level
4. Re-evaluate risk levels



Close to the idea of mitigation is the idea of remediating a risk. Risk remediation implies eliminating or removing a risk facing a system and is also known as risk treatment.

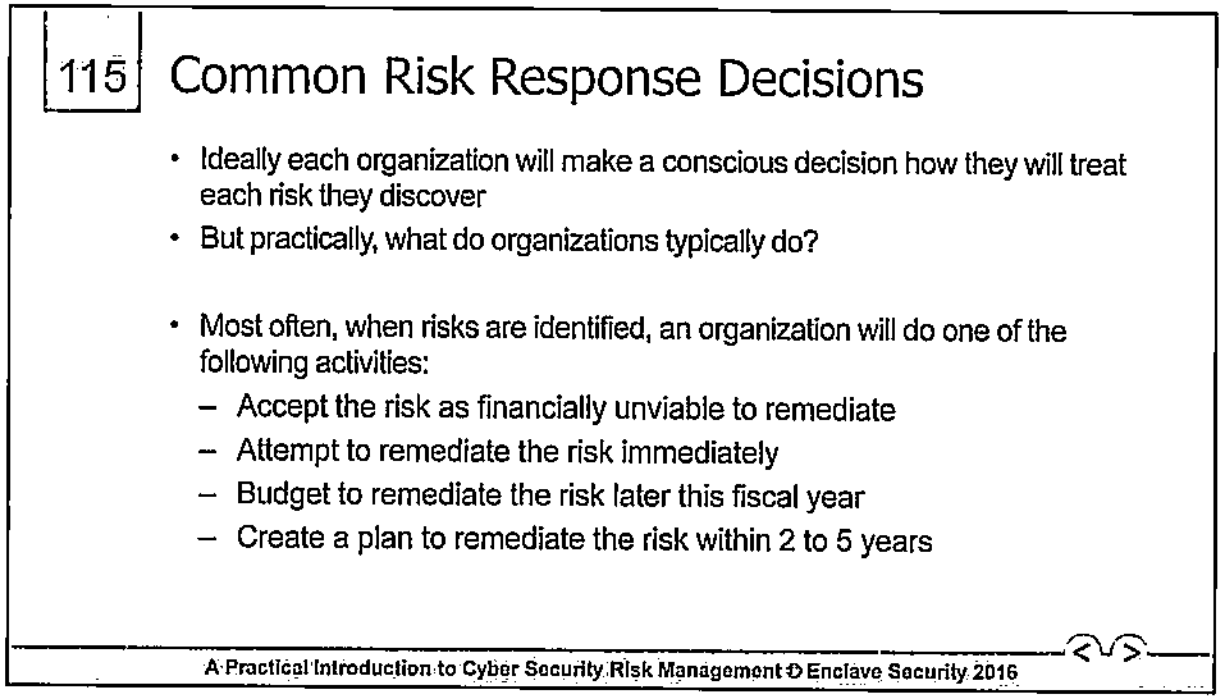
In this case, prior to implementing a control, a risk existed; now after the control has been implemented, the risk has been completely remediated. It no longer exists. A good example of this is the case of an operating system vulnerability. In this case, flawed code exists within an operating system, which could lead to a data disclosure, but the vendor chooses to release a patch that fixes the vulnerability completely. Previously there was a risk, but after the patch is installed, the risk of that particular vulnerability is gone. Other operating system flaws may still exist, but for the sake of that one vulnerability – it has been remediated.

The difference between mitigation and remediation is often blurred, and the difference can be artificial, so be careful when choosing this route; you do not want to be deceived into a false sense of security. This is much less common than risk mitigation. However, it is an option in some cases and that is why we mention it here.



A final option in this process is to transfer the risk. In this case an organization decides that they do not personally want to assume the responsibility for a particular asset or the risks that go along with it; they therefore choose to transfer a particular risk to another party. In order to achieve this option, businesses will choose either to insure against a particular risk occurring or they will outsource the business process to another third party to handle on their behalf.

But, do not be fooled. Just because you outsource a business process to a third party, that does not completely absolve you from risks associated with a data asset. It might lower the risk, but it will still be there. Consumers tend to blame the person they gave their information to if that data is breached, even if it is actually because of negligence on the part of a third party. They will tend to hold the person they gave the information to as responsible for the loss. You are a shared participant of risk when you choose to transfer it.



As was discussed earlier, there are a number of ways that an organization might respond to the risks that they have identified. The five options listed above are the comprehensive list of choices that everyone organization can ultimately make. However one has to wonder, what are the practical responses that most organizations will take in light of the identified risks? Most companies will not simply insure the problem away or ignore all the risks, so how are they practically treated?

Every risk cannot be handled the same way, so most often each risk will be dealt with on a case by case basis. What most organizations will do when confronted with risk is to choose one of the following options:

- Accept the risk as financially unviable to remediate
- Attempt to remediate the risk immediately
- Budget to remediate the risk later this fiscal year
- Create a plan to remediate the risk within 2 to 5 years

What is most important is that the organization documents their decision in each case. This allows for the creation of formal organizational priorities and project plans to help remediate the discovered risks.

Common Risk Management Cycle

- Many successful organizations create a risk management cycle which often hinges on the organization's budgeting cycle
- Normally this cycle is annual and tied to the same schedule as budgeting
- A common risk management cycle would include:

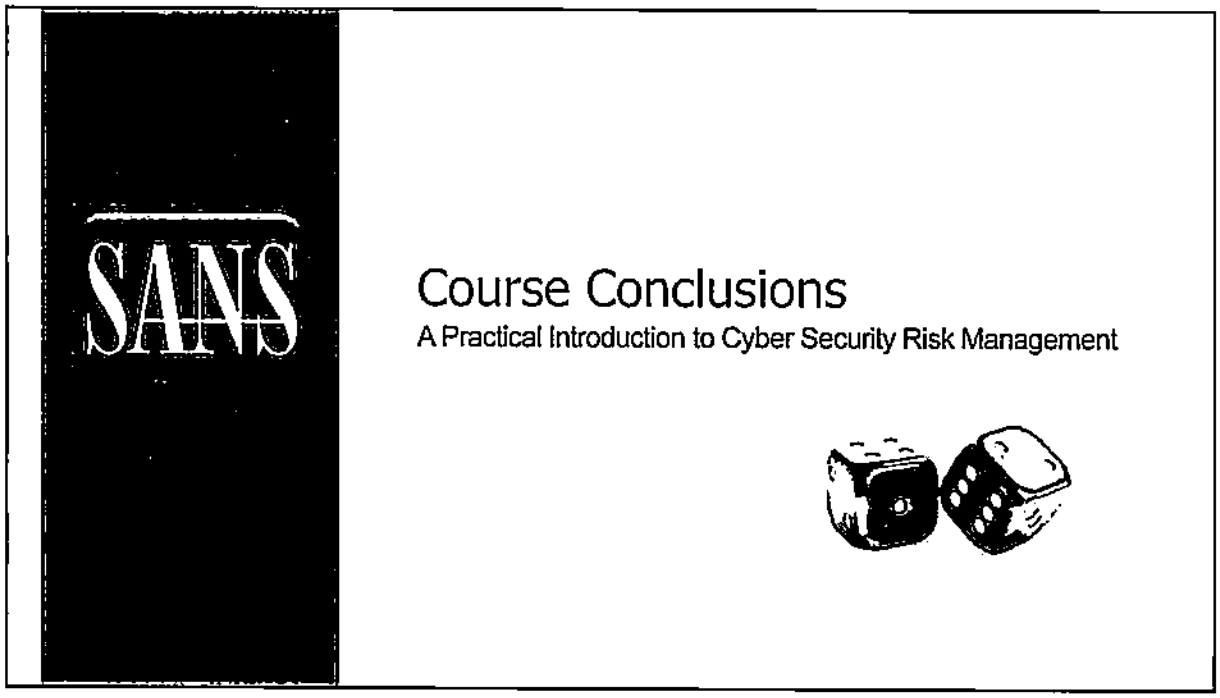
1. Performing a Risk Assessment
2. Defining Remediation Plans
3. Updating Organizational Policy
4. Budgeting for Additional Controls
5. Implementing Additional Controls
6. Auditing Control Implementation
7. Performing a Risk Assessment

A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

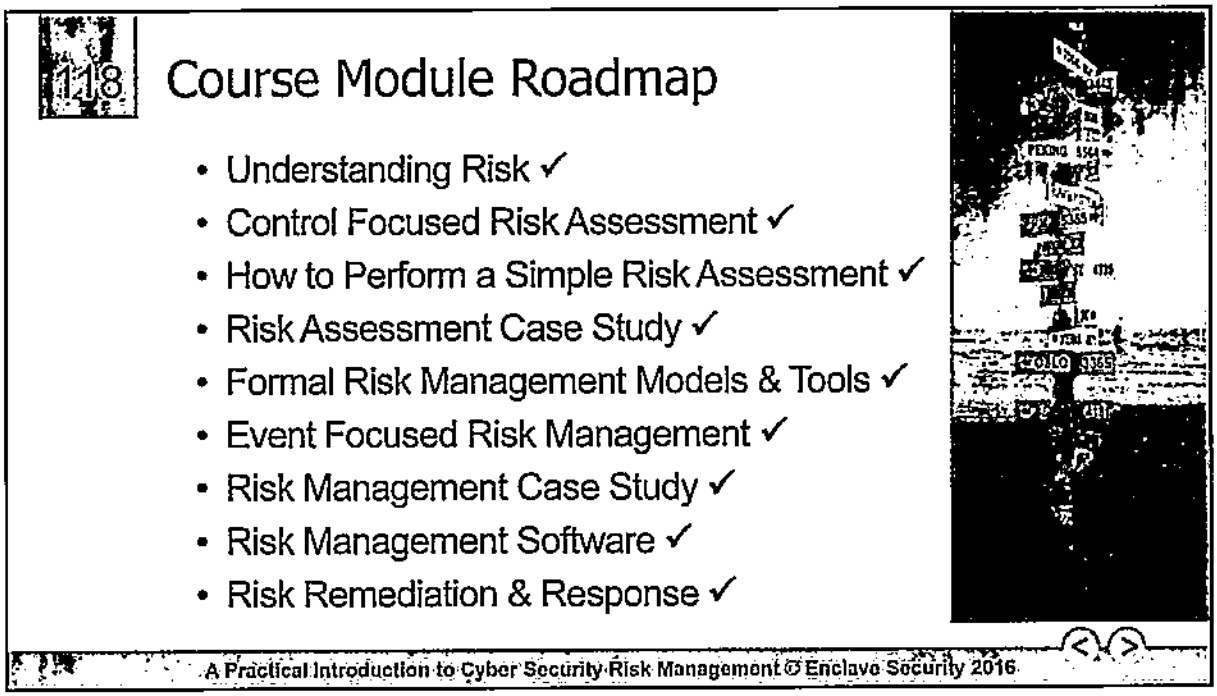
Some of the organizations that are the most successful when handling risk are those that create risk management cycles that hinge around the organization's budgeting cycle. Since resource constrains are generally the largest reason why controls cannot be limited, by centering the risk management cycle around the budgeting cycle, organizations are able to focus their efforts to get the most return on their investment.

With this idea in mind, a common cycle for risk management might be something similar to the following:

1. Performing a Risk Assessment
2. Defining Remediation Plans
3. Updating Organizational Policy
4. Budgeting for Additional Controls
5. Implementing Additional Controls
6. Auditing Control Implementation
7. Performing a Risk Assessment



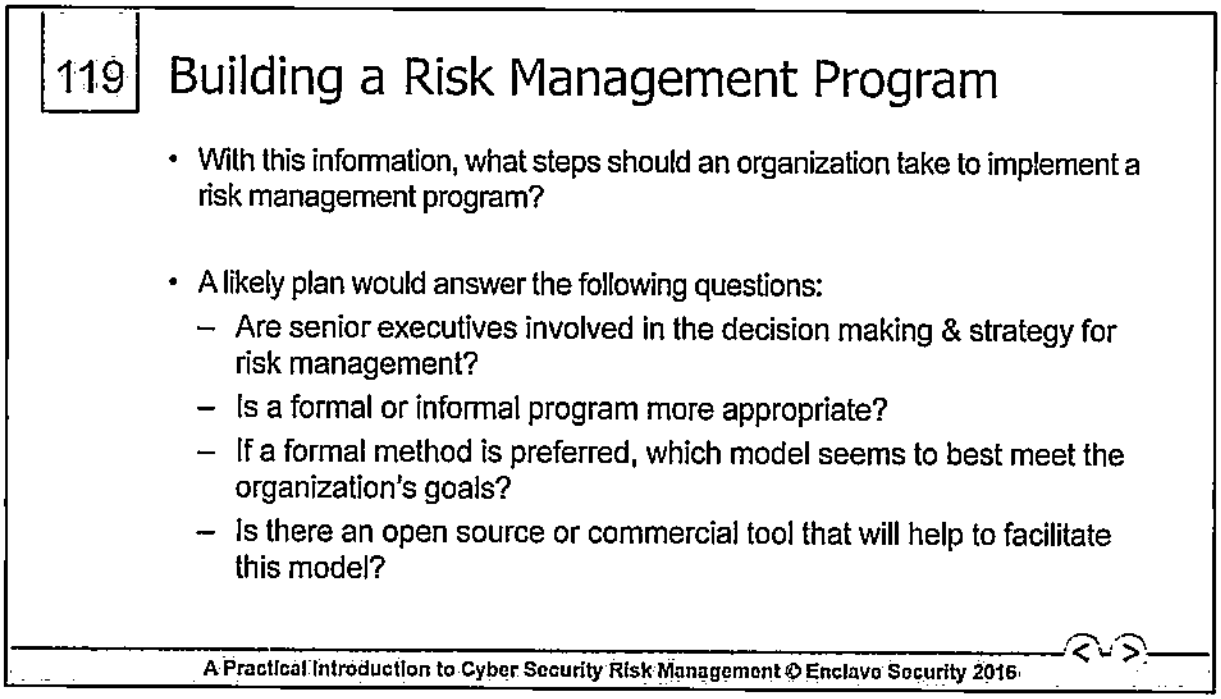
This page intentionally left blank.



In this course we will explore the concept of risk and its practical impact on an organization. Ultimately the goal of this course is to prepare students to effectively utilize risk assessment as a tool for enterprise defense. Too many times organizations think of risk assessment and risk management as academic tools with little to no practical application. These concepts are often viewed as a formal task to pursue when an organization has free time rather than as a core business activity that drives other enterprise security efforts. In today's course students will have the opportunity to learn about the proper place of risk assessment and risk management in an enterprise. They will also be given practical skills for how to perform a risk assessment on a step by step basis, from data collection to the point of presenting their findings to business leaders. Students with a desire to perform more in depth analysis will also be given tools and formal models to consider to empower them to create a long term / formal risk management program.

Specifically today we will cover the following subjects:

- Understanding Risk
- Control Focused Risk Assessment
- How to Perform a Simple Risk Assessment
- Risk Assessment Case Study
- Formal Risk Management Models & Tools
- Event Focused Risk Management
- Risk Management Case Study
- Risk Management Software
- Risk Remediation & Response

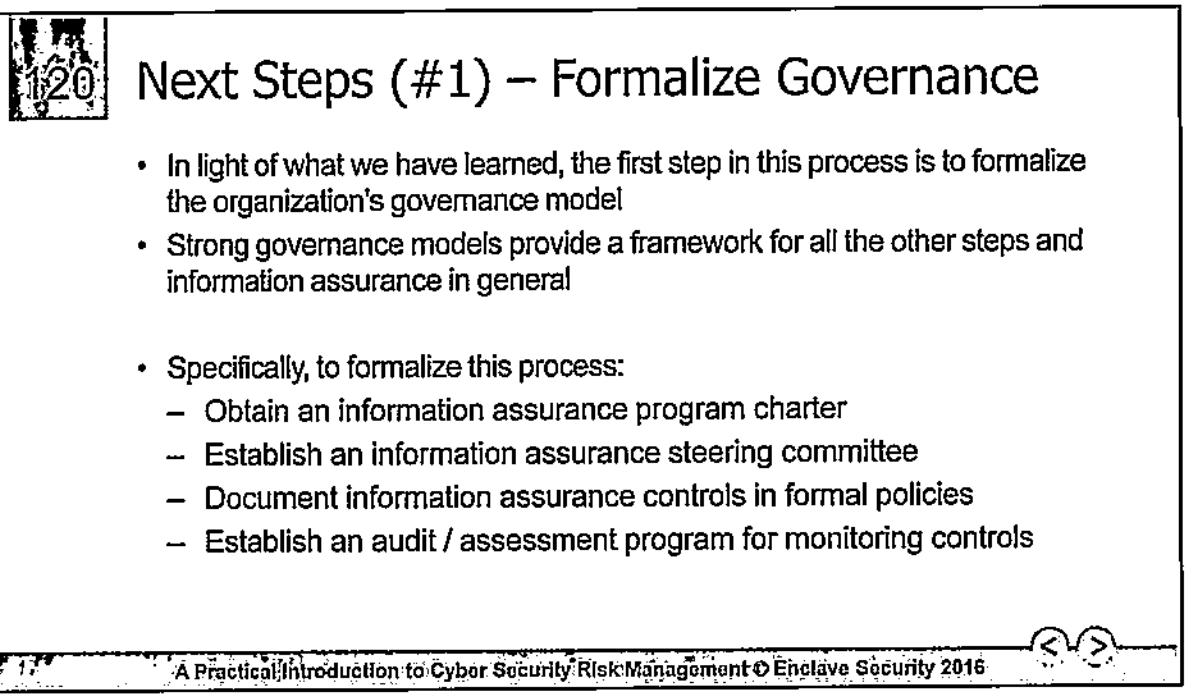


So with all the information covered today, what steps should an organization take to implement fully functional GRC and ERM program in their organization? The thing to remember in this case is that every GRC program will be different, depending on the individual needs of the organization. Every organization will have to ask questions similar to these, determine their business goals, and then decide on a plan of action for how to move forward integrating these concepts. When used properly, these tools can significantly enhance an organization's overall capability to detect and respond strategically to risk.

A likely plan would answer the following questions as a part of an organization's strategic direction:

- Are senior executives involved in the decision making & strategy for risk management?
- Is a formal or informal program more appropriate?
- If a formal method is preferred, which model seems to best meet the organization's goals?
- Is there an open source or commercial tool that will help to facilitate this model?

Now is the time to consider action items you may want to bring back with you to your organization. Remember, this information is only useful if it is applied and put into practice.

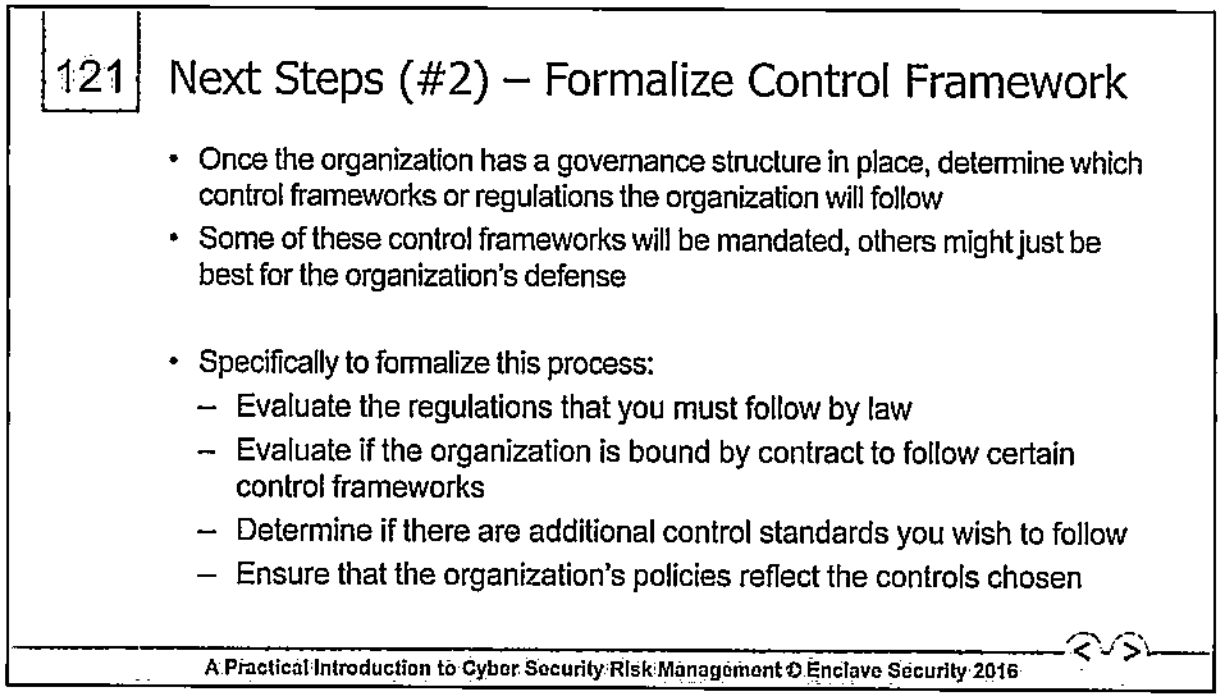


In light of what we have learned in class over the past couple days, what should an organization practically hope to achieve? What steps could they perform practically to begin a risk management program in their organization?

The first step in this process would be to formalize the organization's governance model. Before an organization can start pursuing risk measurements, they must have a framework that they can use to measure themselves against. Governance provides the foundation for all the other work that needs to be accomplished.

In this step of the process, specific steps and deliverables that the organization should consider are to:

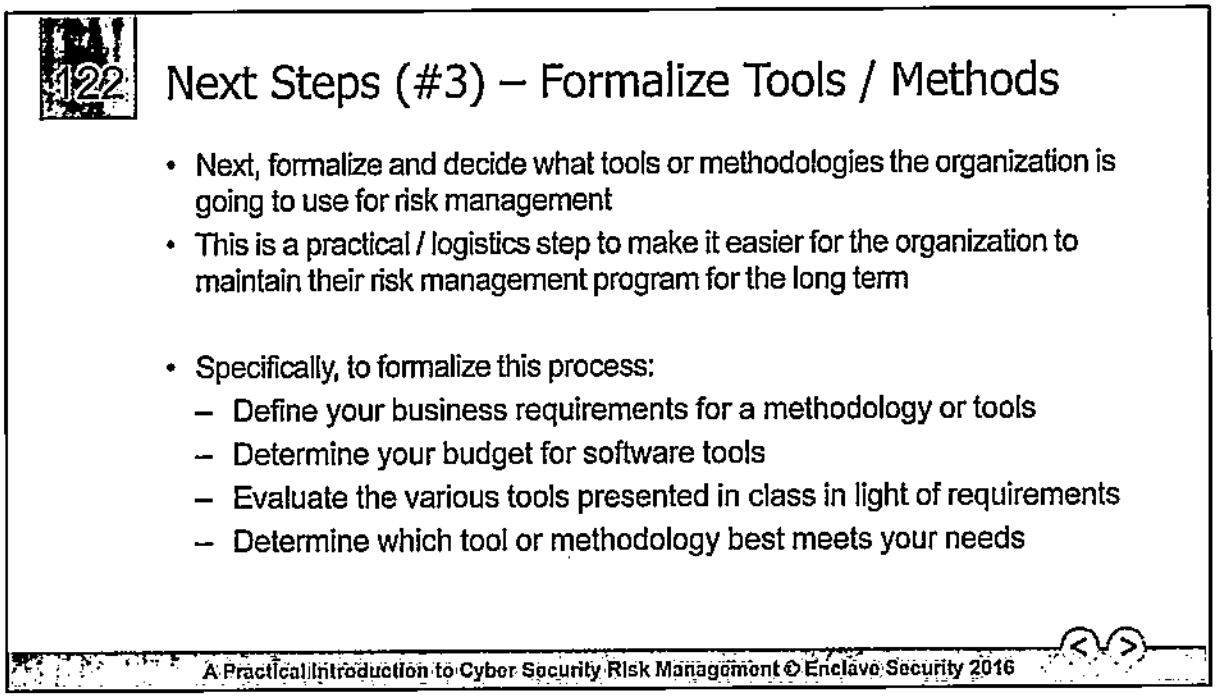
- Obtain an information assurance program charter
- Establish an information assurance steering committee
- Document information assurance controls in formal policies
- Establish an audit / assessment program for monitoring controls



Once the organization has established their governance model, the next step is to formalize their control framework. They must understand what regulations, standards, and contract obligations they are responsible for and determine what controls must be implemented in light of the answer to that question. There are dozens of groups that have created formal control models, and organizations can even choose to create their own. But this list of controls will provide the basis for assessment later in the process.

In this step of the process, specific steps and deliverables that the organization should consider are to:

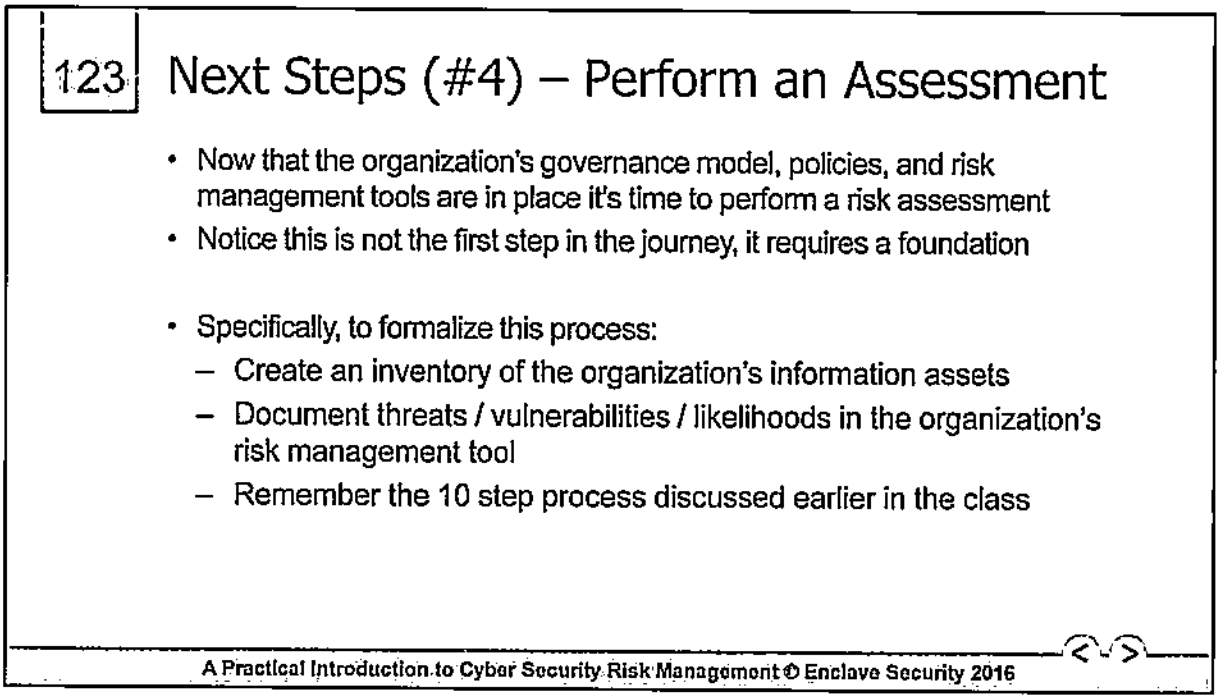
- Evaluate the regulations that you must follow by law
- Evaluate if the organization is bound by contract to follow certain control frameworks
- Determine if there are additional control standards you wish to follow
- Ensure that the organization's policies reflect the controls chosen



Once governance and control frameworks have been selected, the next step is to formalize the tools and methods that the organization plans to use in order to actually measure risk. Will the organization choose one of the academic models discussed? Will they focus on using a particular tool to manage risk? It's easier for the organization to manage their program in the long term if they can answer this question earlier in the process.

In this step of the process, specific steps and deliverables that the organization should consider are to:

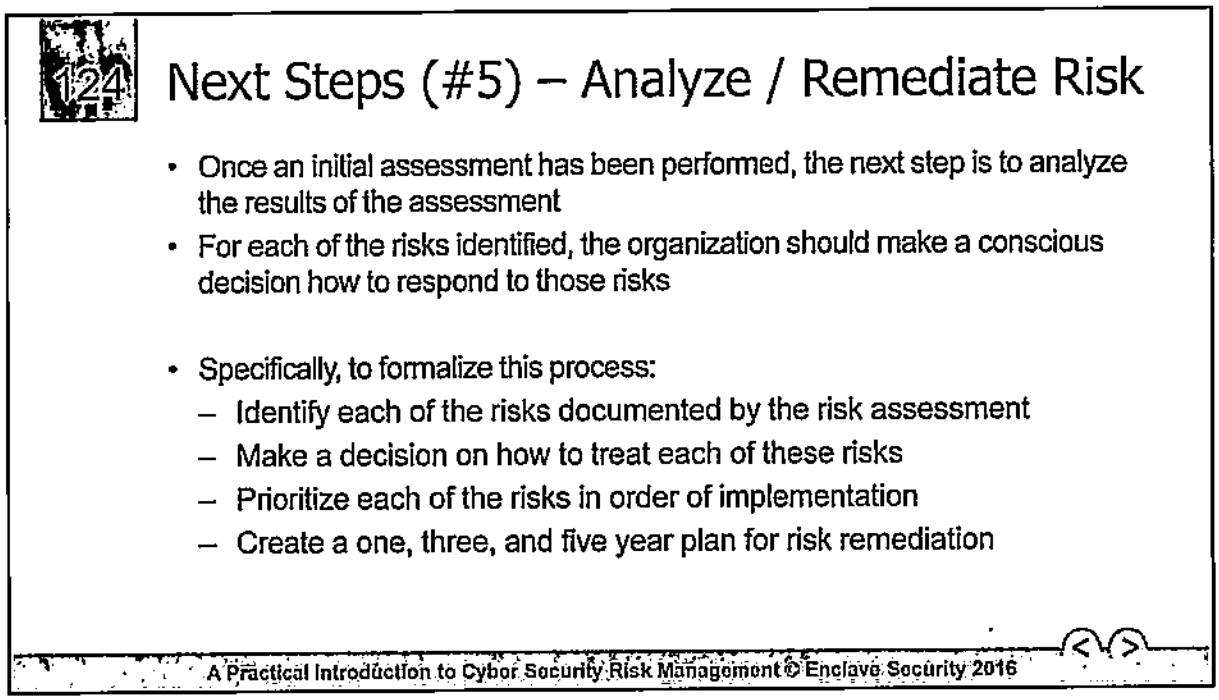
- Define your business requirements for a methodology or tools
- Determine your budget for software tools
- Evaluate the various tools presented in class in light of requirements
- Determine which tool or methodology best meets your needs



Once the previous steps have been performed, it is finally time to actually dig in and perform a risk assessment using the resources and decision points agreed upon earlier in the process. The most important thing that an organization can remember at this point is that this is not the first step in the journey, there were other more foundational decisions that were made to get the organization to this point.

In this step of the process, specific steps and deliverables that the organization should consider are to:

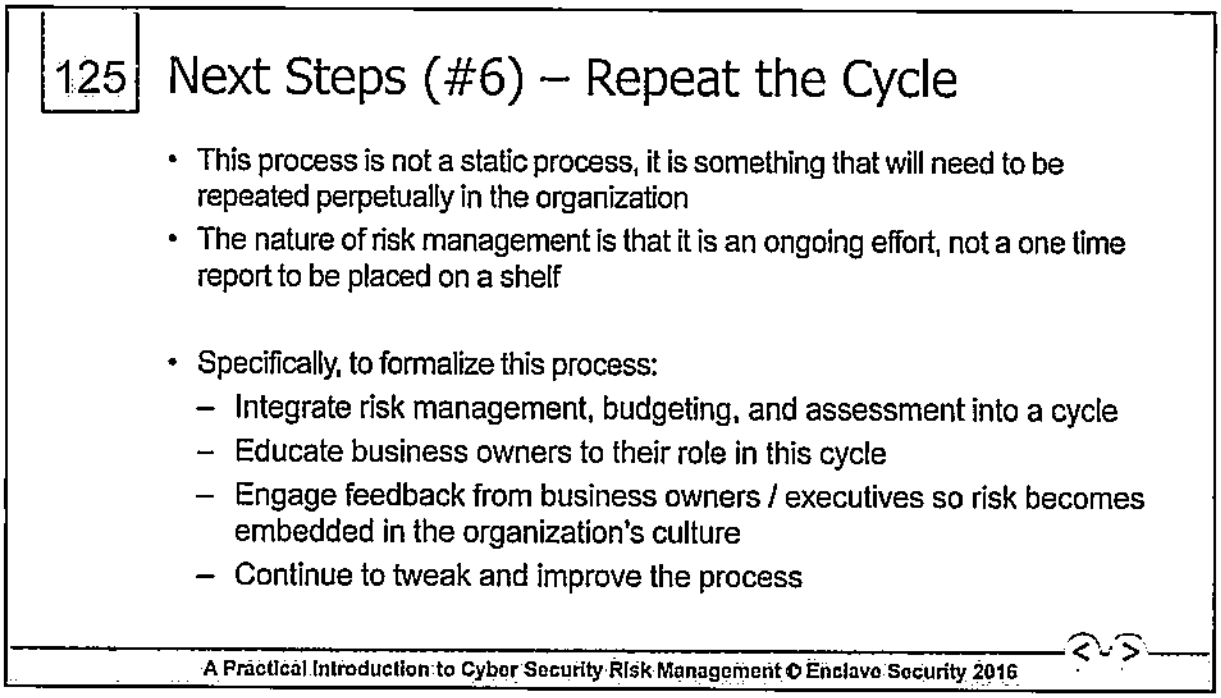
- Create an inventory of the organization's information assets
- Document threats / vulnerabilities / likelihoods in the organization's risk management tool
- Remember the 10 step process discussed earlier in the class



Once a risk assessment has been performed, and the data gathered, the next step is to analyze the identified risks and choose which risks to remediate in the short term. Risk treatment was discussed earlier in today's lesson, and there are a number of options to choose from once a risk has been identified. It is during this phase of the process that the organization will make and begin acting on that decision.

In this step of the process, specific steps and deliverables that the organization should consider are to:

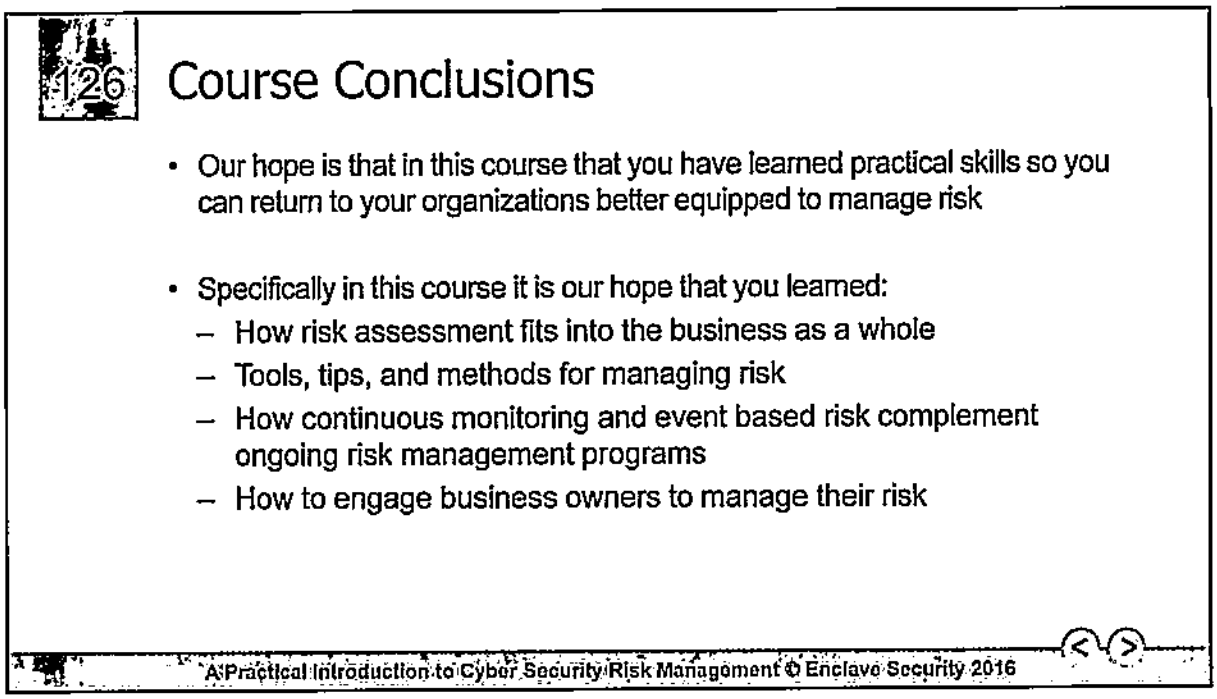
- Identify each of the risks documented by the risk assessment
- Make a decision on how to treat each of these risks
- Prioritize each of the risks in order of implementation
- Create a one, three, and five year plan for risk remediation



Finally the organization is ready to repeat the cycle and move constantly towards greater efficiencies. Risk management is not a static process or something with a defined end date. Said in project management terms, this is a program, not a project. It is ongoing and hopefully will continue as long as the organization is in existence. It is not a one time effort to be completed and put on a shelf for compliance, it is a method for strategically managing risk.

In this step of the process, specific steps and deliverables that the organization should consider are to:

- Integrate risk management, budgeting, and assessment into a cycle
- Educate business owners to their role in this cycle
- Engage feedback from business owners / executives so risk becomes embedded in the organization's culture
- Continue to tweak and improve the process



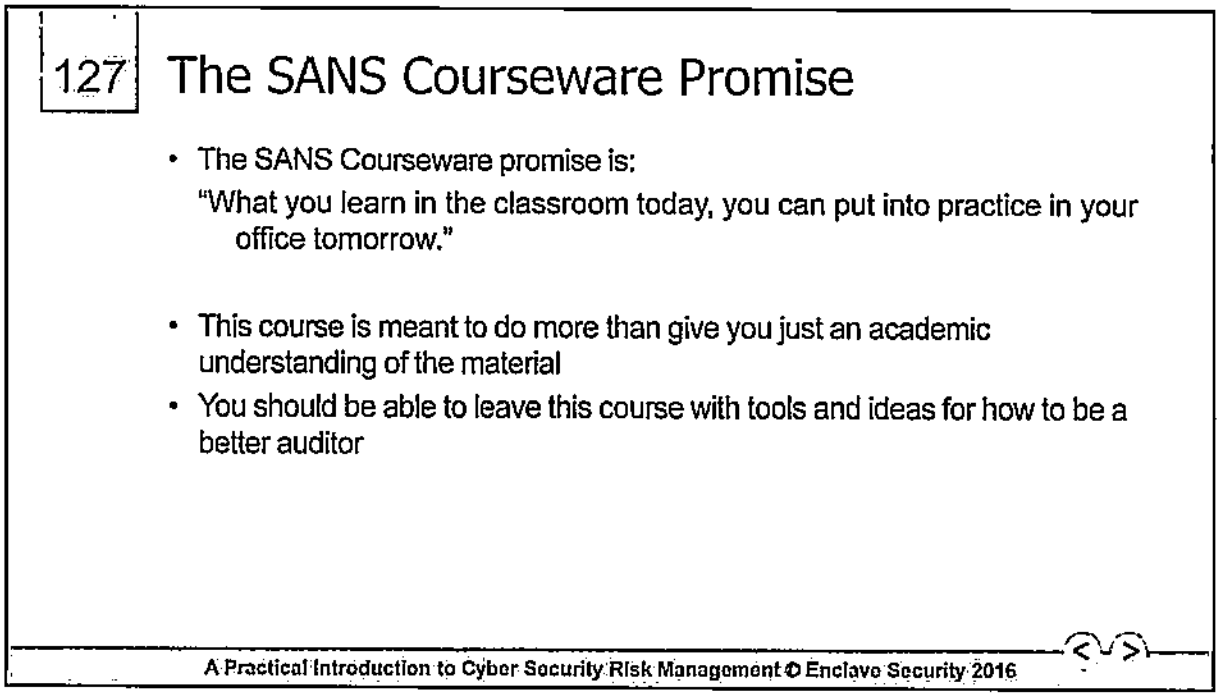
We are glad you had the opportunity to participate in this course with us this week. We really do hope that as a result of taking this course that you have learned practical skills for managing risk and frameworks for integrating risk management into your organization's business practices.

Risk assessment and risk management can be fuzzy concepts for many people and we hope that through this material we have made the issues surrounding risk more concrete and actionable. Certainly many of the concepts we have discussed will need to be integrated specifically into your organization's business practices. But our hope is that you have an idea now for the specific decisions and steps you will need to take to begin this journey.

Specifically over the past couple days we hope so far you have learned:

- How risk assessment fits into the business as a whole
- Tools, tips, and methods for managing risk
- How continuous monitoring and event based risk complement ongoing risk management programs
- How to engage business owners to manage their risk

If any of these concepts seem fuzzy to you still, and you still have brain cells left, please talk with your instructor after class to clarify.

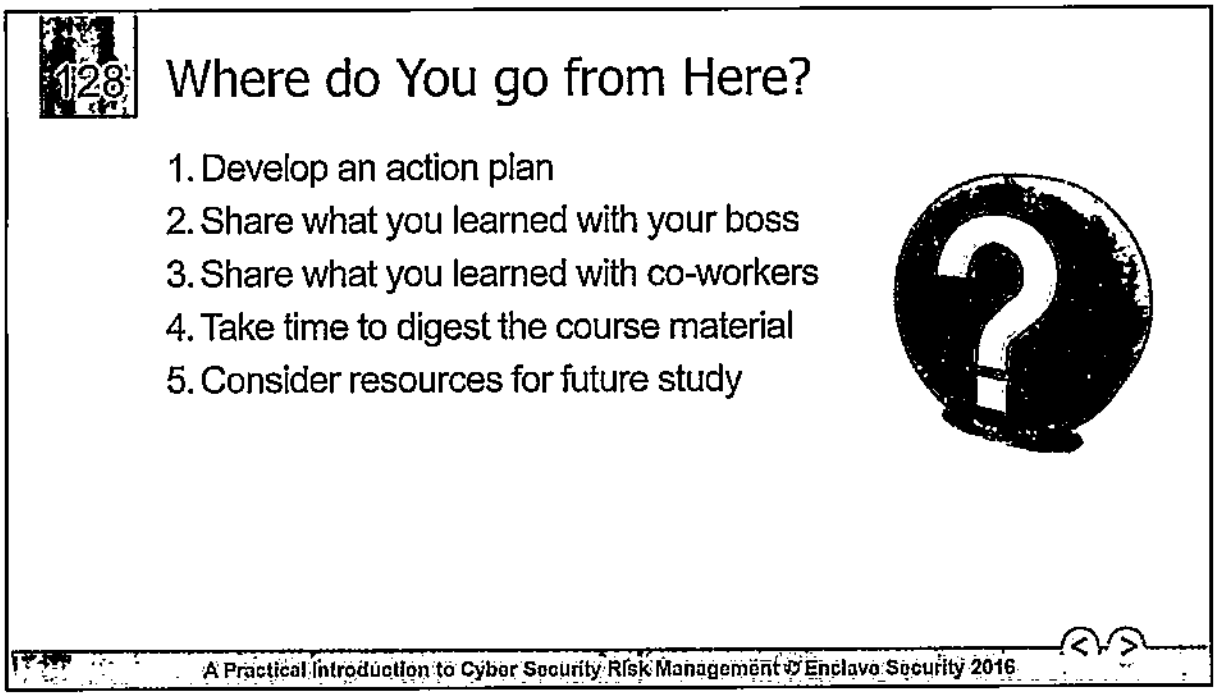


At this point in the class we're officially done filling your head with new information, but that doesn't mean that class is over. The last thing we need to do in class this week is take a few minutes to evaluate what you have learned, and think about what information you can take home with you.

SANS and its authors developed a saying through the years that over time officially became called the SANS Courseware Promise. It reflects our commitment to providing quality training that best serves individuals and their organizations. Our promise to our students is that:

"You will be able to apply our information security training the day you get back to the office."

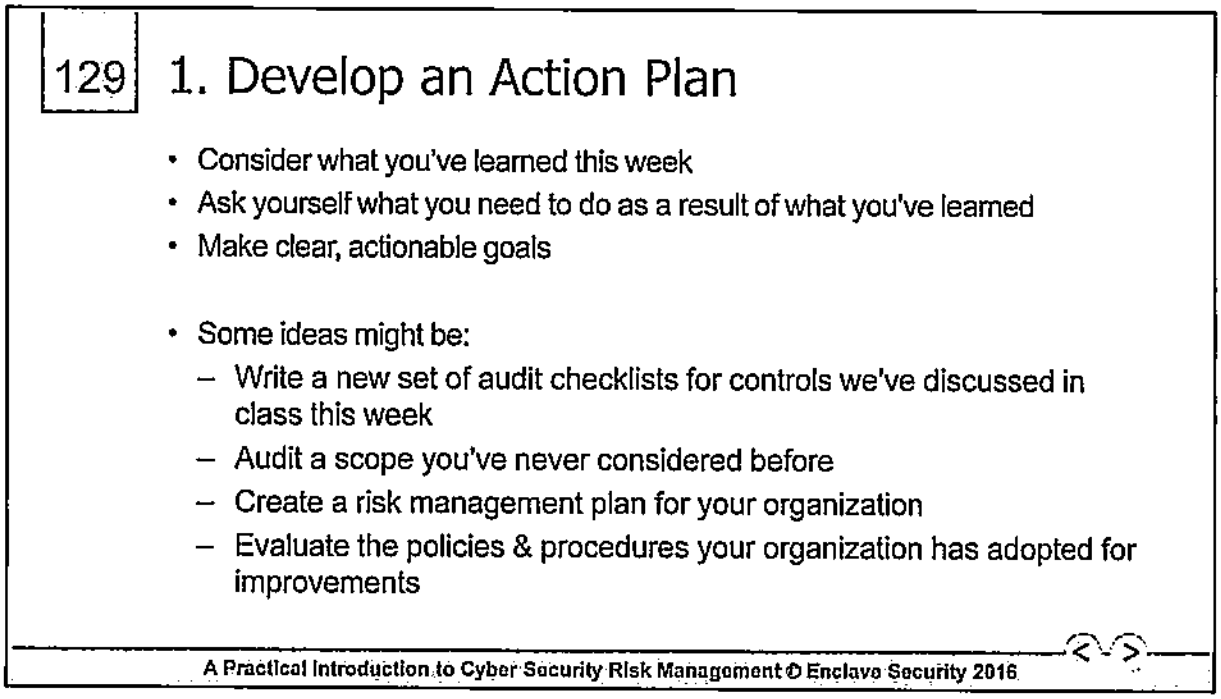
If we cannot meet this goal, then we need to reconsider what we are doing and how we can make this true again. This course is meant to do more than simply give you an academic understanding of the material. You should be able to leave this course with tools and ideas for how to be a better auditor and how practically to be better at your job.



The question then becomes, where do you go from here? If the goal is to make this information practical, we would like you to take a minute to consider how you may specifically be able to take the information from this class back to your office.. So we have a simple five-step program for you to think about for the remainder of our time together and while you drive or fly back to your office this week.

Specifically our next steps for you are to:

1. Develop an action plan
2. Share what you learned with your boss
3. Share what you learned with co-workers
4. Take time to digest the course material
5. Consider resources for future study

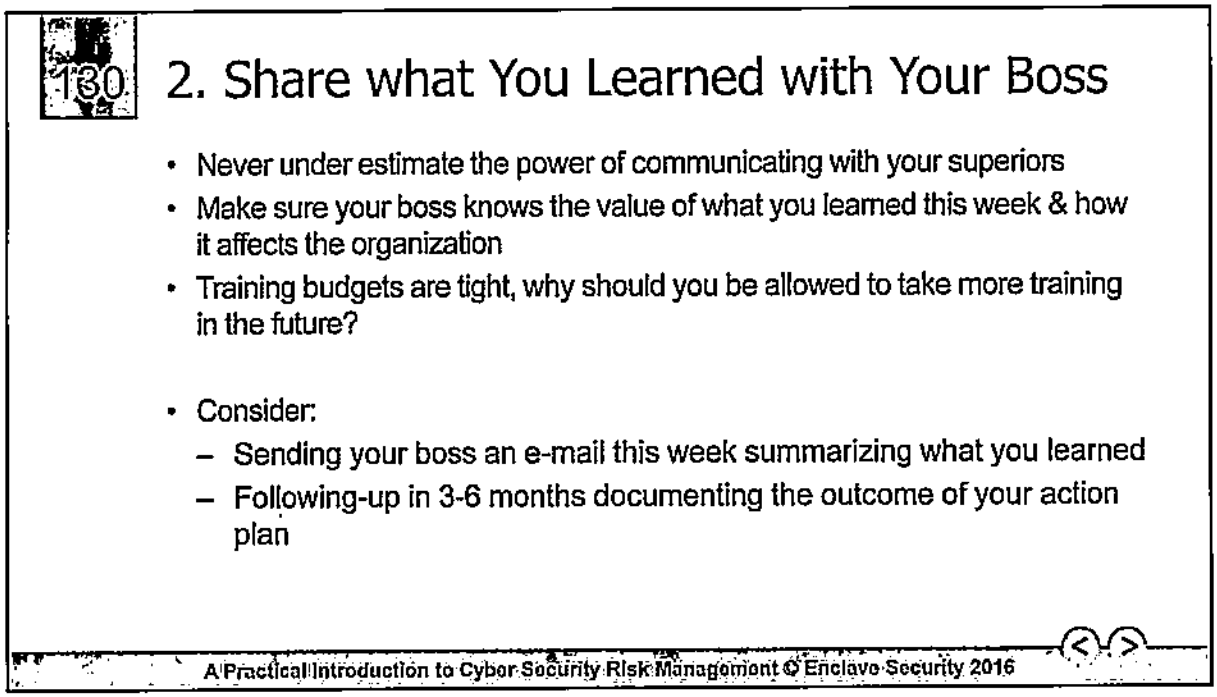


First, develop an action plan.

Consider what you've learned this week. It's now time to ask yourself what you need to do as a result of what you have learned. We hope you have learned tricks for doing your job better, frameworks for understanding information, and strategies for being more efficient at how you work. But we also want to make sure you have clear and actionable goals as you go home. That is what will make you more effective for your next steps.

Every person in the class will most definitely have different goals, but here are a few examples of the types of things you might need to consider going back to your offices:

- Write a new set of audit checklists for controls we've discussed in class this week
- Audit a scope you've never considered before
- Create a risk management plan for your organization
- Evaluate the policies & procedures your organization has adopted for improvements



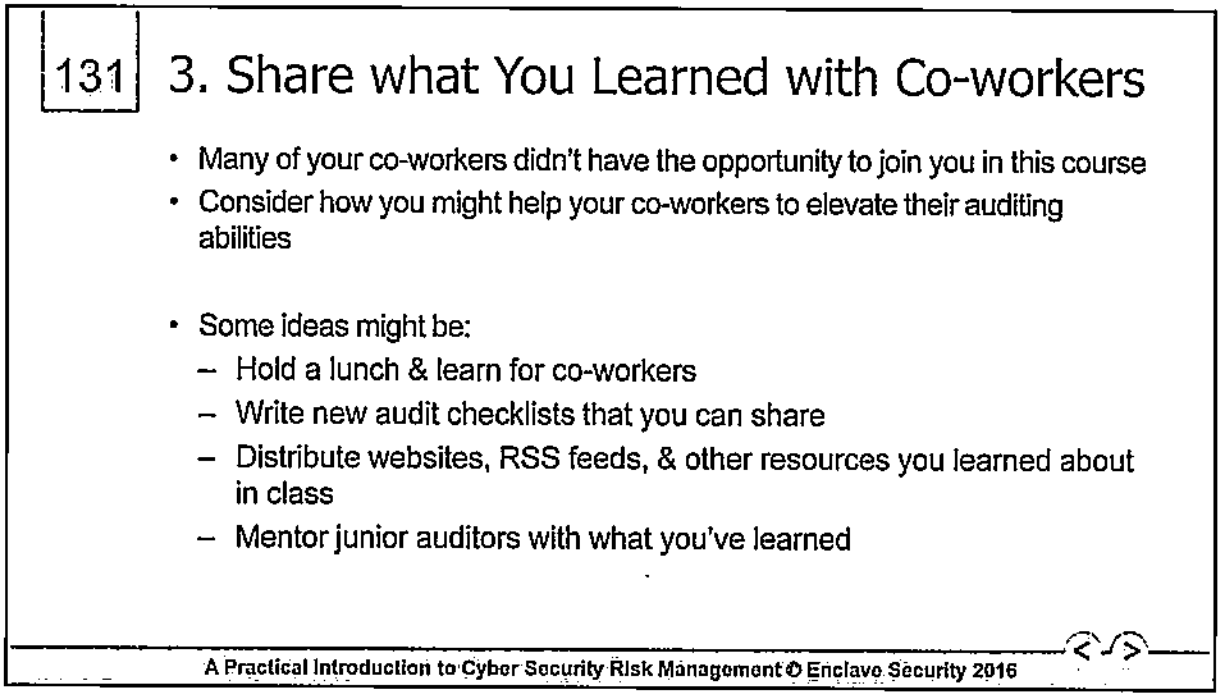
Next, share what you learned with your boss.

Never under estimate the power of communicating with your superiors. Make sure your boss knows the value of what you learned this week & how it affects the organization. The reality is that training budgets for organizations are always tight and resources are always limited. There is never enough time or money to send people to all the training they really should be receiving.

But, you can stand out from your peers and the crowd around you if you follow a couple of simple steps. The goal here is to distinguish yourself from your co-workers and to better compete for those training dollars.

First, send your boss an e-mail this week summarizing what you learned (and don't forget to say thank you for sending you to the event – bosses love that). Make sure this e-mail is specific and outlines what you think you can accomplish as a result of the training. Second, follow-up in 3-6 months, documenting the outcome of your action plan.

If you simply follow these two steps, you will be helping to educate your boss about the topics you learned this week, and you will be putting yourself in a better position to be the one to receive the training dollars next year. If a boss has a choice of who to fund, who is more likely – the person who documented and followed-up with the training, or the one who did not?

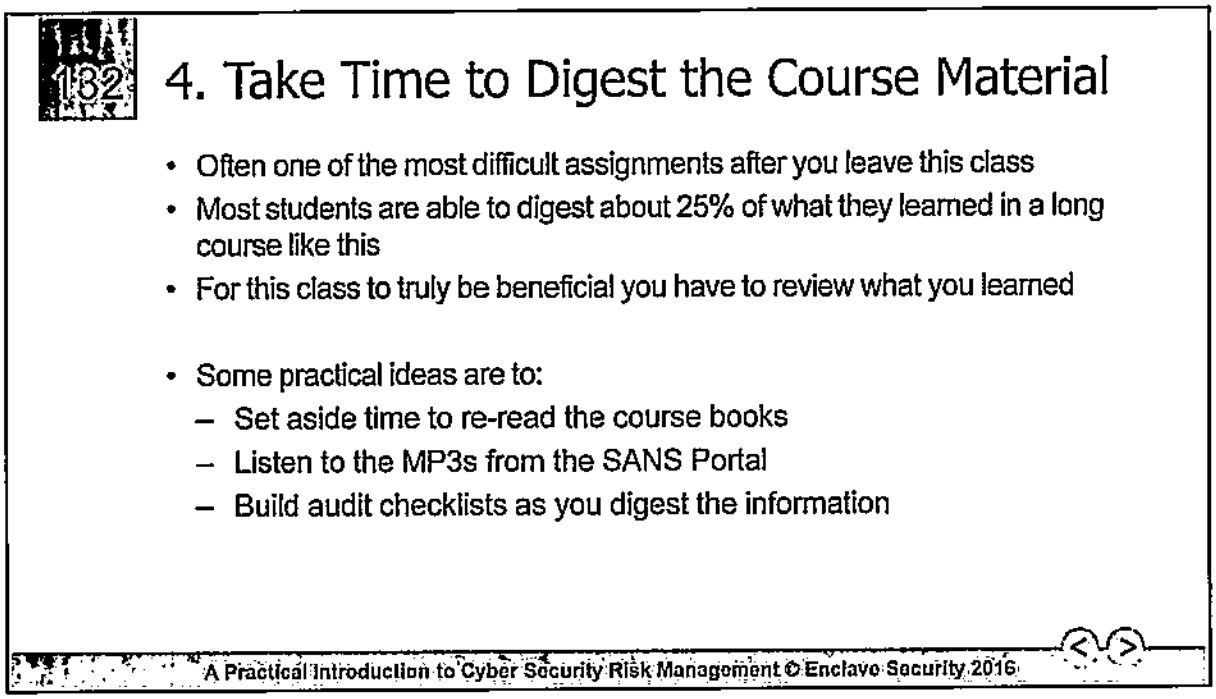


After you take the time to share what you have learned with your boss, the next step is to share what you have learned with your co-workers too. Don't try to keep all that good knowledge bottled up inside – let it out!

Many times your co-workers do not have the same opportunities you have to go out to training, so take the time to share with them some of the tidbits you have been able to take away from class. Think about, and even write down, what things you can do to pass along information to others, and especially how you can help them with their auditing skills.

Here are a few ideas you might try if you are looking for ways to share what you have learned:

- Hold a lunch & learn for co-workers
- Write new audit checklists that you can share
- Distribute websites, RSS feeds, & other resources you learned about in class
- Mentor junior auditors with what you've learned



In the midst of all this sharing though, do not forget to take the time to digest what you have learned for yourself too. One of the most difficult things after a long course, such as this, is how to translate the information you have learned into something useful back at work. Most students we see are able to retain maybe 25% of that they learn in class after hearing it the first time. If you really want to benefit from what you have learned, take the time to re-read the courseware and do whatever you can to make sure the information sinks in.

Again, some tips we would recommend to get started would be to:

- Set aside time to re-read the course books
- Listen to the MP3s from the SANS Portal
- Build audit checklists as you digest the information

133

5. Consider Resources for Further Study

- Courses like this are just meant to lay a foundation and introduce you to the world of IS Auditing
- This field especially requires continuous education & learning about available controls

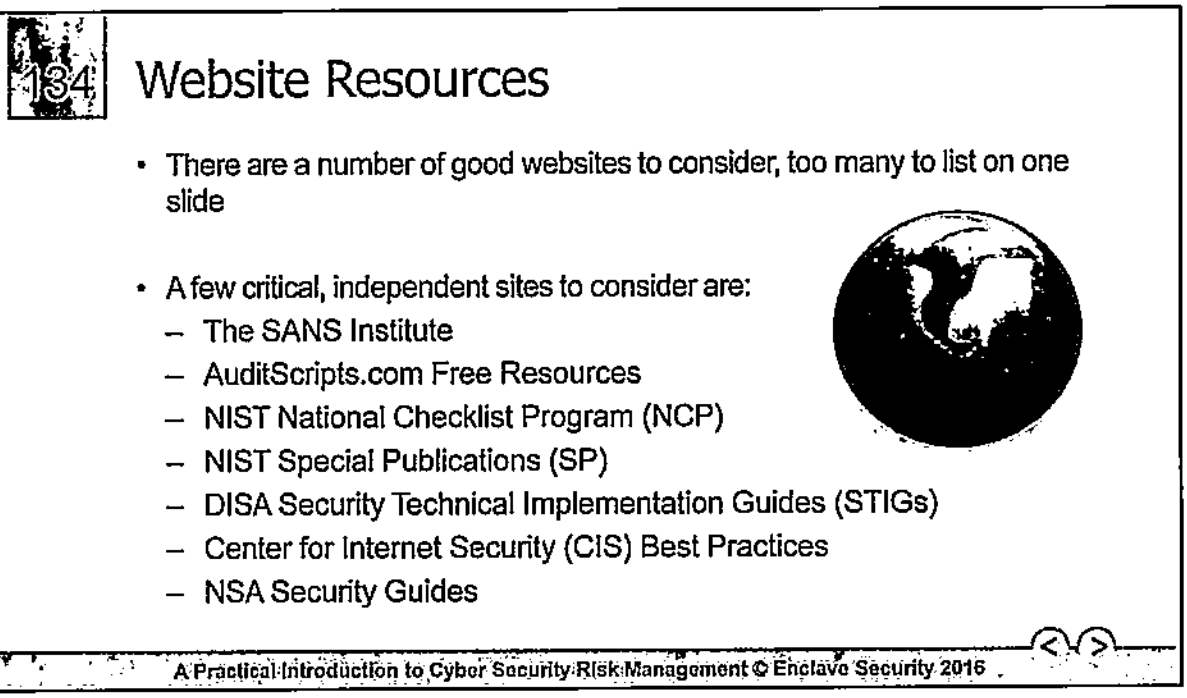
- Top 5 Resources to Consider:
  - Association Membership
  - Additional Certifications
  - Websites
  - Blogs & RSS
  - Social Media

A Practical Introduction to Cyber Security Risk Management © Enclave Security 2016

Courses like this are meant to lay a foundation and introduce you to the world of IS Auditing. There's no question that this course is meant to be a starter for you. It is certainly not the end of your education. Courses like this lay a foundation for a lifetime of learning about this field. There are always new technologies, new threats, new vulnerabilities, and new controls to learn about. Take advantage of resources such as these to continue learning even after the class is over.

We have a few parting resources for you over the next few slides to inspire you with your next efforts. A few resources to start with that we will cover here are:

- Association Membership
- Audit Certifications
- Websites
- Blogs & RSS
- Social Media



Of course one of the better resources to consider is websites. There are a number of great websites that you might consider checking out to help you with your career and continuing education. There are a number of great websites that will provide you free resources for learning and making your job easier. Why create an audit checklist from scratch when you can start with a template someone else has written? Why try to discover appropriate controls on your own when there are others out there who have already figured it out?

As a starting point, consider keeping an eye on the following websites as a way to stay on top of the industry:

- The SANS Institute
- NIST National Checklist Program (NCP)
- NIST Special Publications (SP)
- DISA Security Technical Implementation Guides (STIGs)
- Center for Internet Security (CIS) Best Practices
- NSA Security Guides

135 Blogs & RSS Feeds

- A full starter list of blogs and Real Simple Syndication (RSS) feeds is on the course USB (OPML File)
- If you're new to RSS, consider Feedly or another free RSS reader

- Don't miss the blogs at:
  - http://blogs.sans.org/
  - http://www.auditscripts.com/free-resources/blogs/

One of the best tools that we think is available to you in your continuing education efforts are Real Simply Syndication (RSS) feeds. RSS is a content aggregation service, which allows users to avail new content that is published from a given source – such as a news feed. [1]

"What is RSS?
RSS is an acronym for Really Simple Syndication.

How Can I Benefit From RSS?
RSS feeds save time, allowing users to receive notification only when new content is available.

How Do I Subscribe to RSS Feeds?
First you will need an RSS feed reader (also called a news aggregator). There are a number of RSS readers available. A short list is available at http://www.rss-specifications.com/rss-software.htm

Once you have an RSS reader you simply click the icon or a link to the RSS feed and paste it into your RSS reader. To make life easier for you, we have included a starter OPML / XML file that you can import into your favorite RSS reader. Hopefully this will be a good way for you to try things out.

1 RSS Subscriptions Explained. (n.d.). RSS Specifications and RSS Feeds. Retrieved February 1, 2011, from http://www.rss-specifications.com/rss-subscriptions.htm

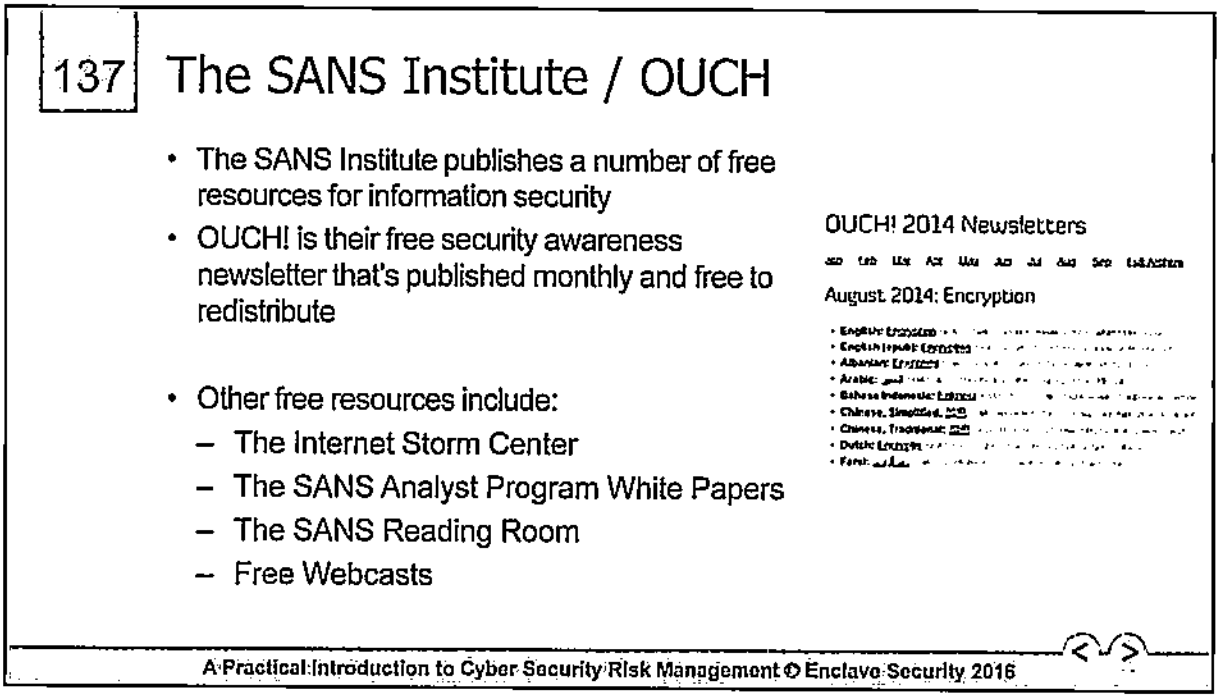
Social Media Sites

- Every day more and more security professionals are joining social media sites and contributing resources there

- LinkedIn
  - Numerous groups you can join
- Twitter
  - Consider following auditing handles
  - For example, @isaudit, @enclavesecurity, @sansinstitute
- Facebook
  - Fan pages exist for associations & security groups

Finally, in addition to RSS, it might be worth investigating some of the more popular social media sites for information security professionals and auditors that are publishing free content via the social media networks. Every day more and more auditors are joining social media sites and contributing resources there. There are discussion groups, postings, resources on upcoming events – everyone seems to want to get into the social media game.

But be careful, not only can these sites be a huge time drain (trust us, we know), but they are not always secure services by default. Make sure you take your time to perform due care and due diligence on any of the tools you are thinking about using. There's nothing worse than trying to learn about information assurance and getting hacked in the process.

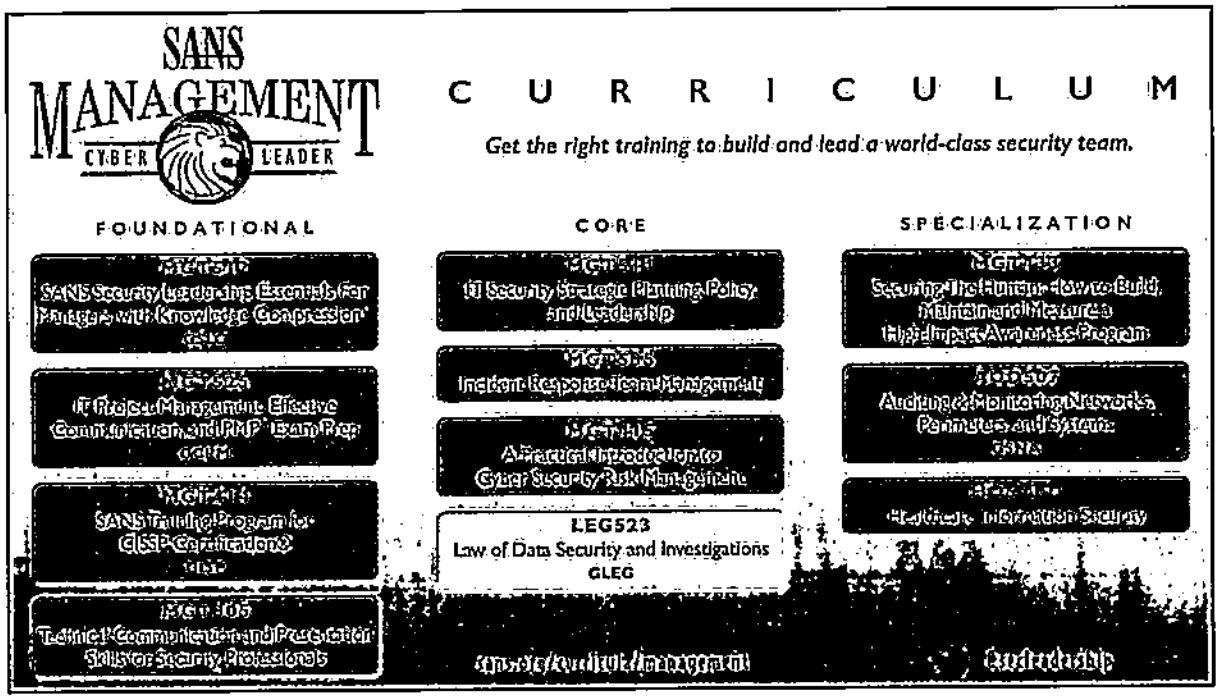


The SANS Institute also has a number of excellent resources that you can take advantage of on their website. The benefit of many of these resources is that they are free for anyone to access and use. Many of these resources can also be re-used within your organization at no cost. There are a number of people from the information assurance community who have published resources here on the SANS website in order to help the community as a whole promote good information assurance practices.

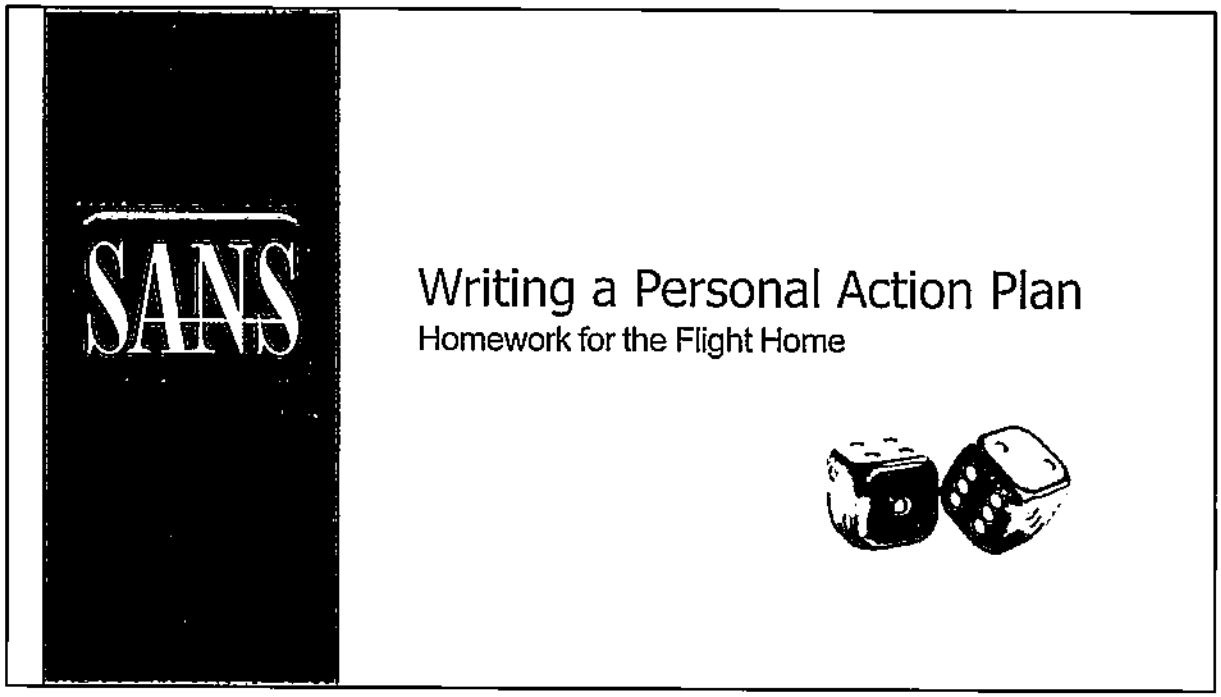
One of the more popular resources is the SANS OUCH newsletter that is released once per month. This is a free resource that the SANS Security the Human program produces through the help of volunteers to create security awareness content that can be used free of charge for OUCH subscribers.

Other popular free resources include:

- The Internet Storm Center
- The SANS Analyst Program White Papers
- The SANS Reading Room
- Free Webcasts



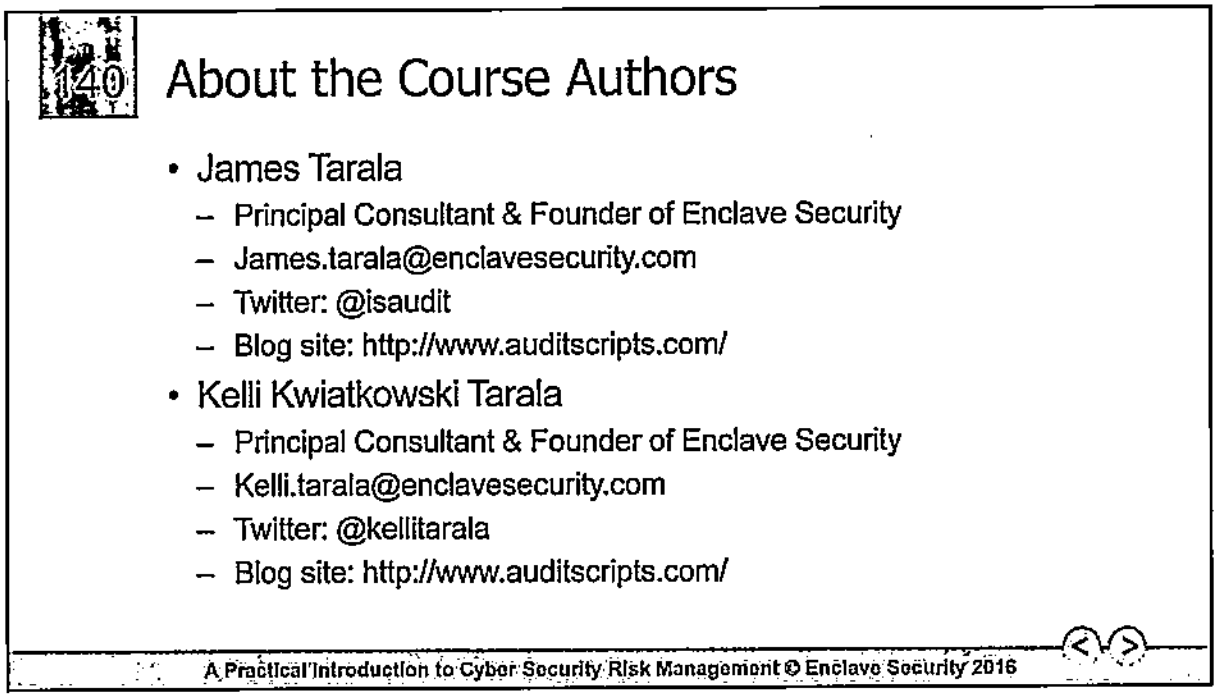
This course, SANS MGT415: A Practical Introduction to Cyber Security Risk Management, is a part of the SANS Institute's management and leadership curriculum as a part of it's core curriculum. In this course students will learn the practical skills necessary to perform regular risk assessments for their organizations. The ability to perform a risk assessment is crucial for organizations hoping to defend their systems. There are simply too many threats, too many potential vulnerabilities that could exist, and simply not enough resources to create an impregnable security infrastructure. Therefore every organization, whether they do so in an organized manner or not, will make priority decision on how best to defend their valuable data assets. Risk assessment should be the foundational tool used to facilitate thoughtful and purposeful defense strategies.



Now it's time to put what we've learned into practice. The purpose of the lab activities that we are engaging in during this class is to give the student an opportunity to put into practice what we have been learning about from the instructor. The hope is that by working through the exercises in this lab that you will be better prepared to take this information back to your company in order to put it into practice.

Some of these lab exercises specifically call on students to work as teams. Even if the lab specifically does not call for you to work as a team, in a conference setting you will likely get the most from this activity if you do work as a group with friendly students sitting around you. Not only will you be networking and building relationships with smart students sitting around you, but you will also be able to benefit from their ideas and experiences as well. Every student brings a wealth of information to class, and participating as a group is one of the better ways to be able to take advantage of those experiences.

At this point, it's time to turn to the section of the book where this lab is described in more detail. Listen to the specific instructions given by your instructor and follow the instructions in the lab exercises step by step. If you have any technical challenges or questions, don't hesitate to ask, the instructor and/or teaching assistants are here to help.



Course Lead Authors

James Tarala

James Tarala is a principal consultant with Enclave Security and is based out of Venice, FL. He is a regular speaker and senior instructor with the SANS Institute, as well as a courseware author and editor for many of their auditing and security courses. As a consultant, he has spent the past few years architecting large enterprise IT security and infrastructure architectures, specifically working with many Microsoft based directory services, e-mail, terminal services, and wireless technologies. He has also spent a large amount of time consulting with organizations to assist them in their security management, operational practices, and regulatory compliance issues, and often times performs independent security audits and assists internal audit groups to develop their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University, his graduate work at the University of Maryland, and holds numerous professional certifications.

Kelli Kwiatkowski Tarala

Kelli Tarala is a principal consultant with Enclave Security. Her career began in 1994 as a system administrator and technical editor at a pharmaceutical research organization. As a security architect and project manager, she specializes in IT security operations, information assurance strategies, and DIACAP certification & accreditation. As a consultant, she has assisted banks, DoD contractors, health insurance companies, law firms, and local, state, and tribal governments with information security initiatives. She holds numerous professional certifications including GIAC, CGEIT, and PMP. She is a courseware author editor for the CISA auditing course and regularly contributes to an information security column.

Risk Management Case Study

In this next exercise we will be performing a simple risk assessment of information assets using Microsoft Excel as the primary tool for performing the assessment. The purpose of this case study is to take the principles we have learned in class and apply them in our groups. Whereas in the previous exercise the instructor guided your groups through this exercise, in this case study you will be provided the necessary data to perform a simple risk assessment, and you will perform that assessment on your own (with your group) and report your findings to the class.

As we discussed in the previous lab exercise today, often times when organizations first perform risk assessments they discover that they do not have the time or the resources to use lengthy processes for performing risk assessment. Their goal instead is simply to begin the process of risk assessment using basic tools to start prioritizing where additional controls may be necessary to protect their information systems. In addition, you may find yourself in situations where you need to recommend to organizations a simple process of performing risk assessment if they have never performed this type of activity before. This exercise will help students to perform this type of assessment and get an initial picture of how to perform such assessments.

Part One: Break Up into Small Groups

To start this lab the first thing you will need to do is break up into groups of 4-5 people per group. For this exercise, as with a few others in the class, we will be performing the exercise as a group, so you will need to find some people sitting around you that you can work with for the course. If you have not already introduce yourself to the people around you and pick a small team to work with for the course. You will be sharing ideas and hopefully getting to know everyone quite well.

Eventually you will need to determine which roles everyone will play in the group. Each group should have a spokesperson who can report findings to the class, a timekeeper to watch the clock and keep everyone on task, and a secretary who can take notes on your group decisions. Since we will be performing multiple group exercises during the course, plan on switching these roles during each of the exercises.

PART TWO: COMPLETE THE RISK ASSESSMENT WORKSHEET

Next, as a group it is now time to complete your risk assessment worksheet and start to discuss as a group how you would rate each of the systems in your inventory. On your course USB you will find a template for risk assessment in the Security Tools directory in a folder labeled Enclave Risk Assessment. Open the Microsoft Excel file (Day 2 - Enclave_Event_Based_Risk_Partially_Blank) you find in that directory and we will use it as a template for this exercise.

Please Note: As we indicated in the course laptop setup requirements, you should have a copy of Microsoft Office 2010 or later already installed on your system to open this file. You will have the most functionality (including conditional formatting) if you use Microsoft Excel to open the file. However if you have an earlier version of Microsoft Office installed on your computer, many of the drop down choices in the tool will not work properly. You may need to work with a partner to complete the exercises.

Although we have performed a similar lab exercise already in class under the direction of the instructor, this is your opportunity to perform the assessment on your own (as a group). Your primary goal for this portion of the case study is to:

1. Complete the risk assessment spreadsheet from your course USB.
2. Answer the follow up questions from Part Three of this assignment.

All of the information you need to complete the assignment can be found in the case study section of the course from today's materials. This includes a full background on the company you will be analyzing as a part of this assessment. If you have any questions about the background or assumptions going into this assessment, please feel free to ask your instructor for feedback and clarification.

In the course notes you have been provided the following:

- The results from a vulnerability scan
- Alerts from an Intrusion Detection System (IDS)
- Alerts from a File Integrity Assessment (FIA) system of unauthorized file system changes
- A report of security related help desk tickets from the help desk system

To keep your group on task, consider completing the following tasks in order in order to complete this exercise:

1. Examine the partially complete risk assessment spreadsheet.
2. Examine the 'Data Systems' worksheet.
3. Enter the scores from your vulnerability scan report.
4. Examine the 'Event Scores' worksheet.
5. Enter the event scores for each column in the spreadsheet from the notes in the book.
6. Examine the aggregate scores from the 'Data Systems' worksheet.
7. Analyze your findings as a group.

PART THREE: ANALYZE YOUR RISK CALCULATIONS

In light of the scores that were calculated for you in the previous section, it is now time to make sure we understand how these scores were calculated and what our response to these numbers should be. In light of the individual findings that your group determined, please answer the following questions regarding your findings:

Which systems do you believe are subject to the greatest amount of risk? Explain to your group why you believe this to be true.

In light of your answer to the previous question, what can you do as an organization that will most effectively lower your risk scores? Can you prove that with numeric from the spreadsheet? If so, how?

For your individual risk assessment calculations that your group determined, which assets should be the focus of your risk remediation efforts? Can you give examples of what you think might best lower the scores in your assessment to acceptable levels?

Part Four: Reporting Group Consensus

Now that your group has answered the questions, be prepared to share your decisions with the rest of the class. Remember we need to be able to be good information security analysts that can analyze complex data sets on behalf of the business, but we also have to be effective communicators who have the ability to share our ideas with others and be persuasive in the process. So for the final portion of this exercise, and for a few exercises that we are going to complete during this course, be prepared to share your ideas with the class.

We will be performing multiple small group exercises during class, so as you break into small groups, make sure you pick a spokesperson for your group, but make sure it is a different spokesperson for each exercise we perform. That will give everyone a chance to practice their skills of oral persuasion. For this exercise though, pick one person who will be the primary reporter for these results.

After each of the groups has had enough time to come up with appropriate answers to the earlier questions we will reconvene as a class to discuss the results. The instructor will announce when it is time to get back together as a class to report the findings.

This page intentionally left blank.

Writing a Personal Action Plan

Now that you have had the opportunity to spend time in class this week learning about auditing and methods for running an audit program and individual audits, it is now time to think about next steps and what you can do to implement what you have learned into your daily practice. Going away to an event, such as a SANS conference, is a great way to increase your exposure to information, network with your peers, and get ideas for how to improve what you are doing in your job responsibilities. However unless we put those ideas into practice, the time you have spent in class will simply not have the same value it potentially could have.

This exercise does not have to be completed immediately at the end of the last day of class, but it should be completed between now and before you get home from the conference. If you wait until you get back to your office to perform this lab you will find that emails, voicemails, and meetings take over your free time and you will never actually accomplish the lab. So do it now before you leave or at least make sure you take the time to finish this exercise before you return home from this event.

PartOne: Action Items

First it is appropriate to think about what action items you personally want to take back to your office. The items you choose do not have to be items you learned directly from the courseware or the instructor. Maybe something that was said in class or you talked about with another student inspired you to think about something you need to do when you get back to your office. That's certainly fine. Just make sure you document whatever your ideas are so you do not forget.

So the first step is to document at least five action items that you want to remember to take home with you. Remember like we said in class too, there is value in sharing this information with your boss as well. It holds you accountable to the idea and may inspire your boss into action as well. So right now, it is now time to document your ideas.

Write down at least five action items that you want to consider as a result of your time in this class at SANS this week (be specific):

Action Item #1:

Action Item #2:

Action Item #3:

Action Item #4:

Action Item #5:

Excellent, now it is time to move to the next phase.

Step Two: Resources for Further Research

In this next section, the goal is similar to the first section, except now instead of writing action items, we would like you to consider areas of further study and research you want to learn more about. You do not need to choose too many areas, but enough to continue to inspire you to learn more as a result of this week. Education never stops, and we want to make sure you do not stop learning.

Next, write down three areas of further education you want to continue to pursue. Maybe these are topical areas, maybe they are resources (such as RSS feeds) that you want to read on a regular basis, maybe they are even additional SANS courses. Whatever they are, document at least three things you would like to learn more about or pursue as a result of what you have learned here this week.

Take the time now to document those three areas of learning for further education:

Idea #1 for Further Study:

Idea #2 for Further Study:

Idea #3 for Further Study:

Conclusion:

We are certainly glad you had the opportunity to join us in class this week. It was a pleasure to have you in class and from experience we can say that the instructor almost always learns from the class every week we teach and it is a privilege to be able to work with you this week.

If you have additional comments that you think would make this course better, please do not hesitate to write those comments on the course evaluation or email any of the authors with your feedback and they will most definitely respond to your feedback.

We hope you have learned new information this week and we hope you will be able to take this information home with you and be more effective at your job as a result of what you have learned this week. Good luck as you pursue your goals!