Discussion: The Meaning of Information Security

So the question is simple...

"What is information security and what does it mean to you?"

Review: The Meaning of Information Security

When we look at information security, it can have a different context depending on the industry in which we work. We can agree that information security is something that is desirable or wanted and it's not just a hindrance or an obstacle—as many others in an organization may perceive it. We can also see that information security is only a subset of the security of the entire organization.

This is an important point.

An information security breach is measured by its impact on the organization, not just by its impact on the affected IT system. When we develop an information security strategy, it must be strategic not just operational or tactical.

The strategy must plan for the risks and environment of the future, not just the threats and challenges of today. The development of an information security strategy must be aligned with the direction and strategy of the organization. Otherwise it is too easy to build an information security program that quickly becomes out of date.

A common risk is that the information security strategy does not address the changes in business processes and technology that may completely change the way the business operates.

Focus

This course is going to focus on the many topics that make up the area of information security, but it's important to remember that information security is there to support business goals and objectives. We should never have a situation where our information security program hinders business mission. Instead, our security program must be woven into the processes of the organization.

Security is not a separate endeavor from the business. It is the way we do business—we build security into the business processes. This will ensure that the organization is stable and secure.

Classification

There is one reality in information security that will probably never change—you will never have enough time or money to do everything you need and want to do. For most organizations, the gap between where they are and where they want to be is quite large, and to reach their desired security objectives would take an incredible amount of time and budget. In reality, you will not get there this year . . .

Discussion: Assessing Resources and Priorities

So what do you do to ensure you use your limited resources (time and money) effectively?

How do we set priorities—addressing the most important issues but not ignoring other issues that may become important?

Review: Assessing Resources and Priorities

The first step in protecting our assets and establishing an effective information security program is to know what we are protecting. This includes identifying what assets are critical or sensitive and who is responsible for (owns) those assets.

Discussion: Identifying Assets of an Organization

How do we identify the assets of the organization that must be protected?

Protecting Assets

An information security program includes protecting all the assets of the organization, including equipment, data, personnel, facilities, systems, and physical infrastructure. For example, we cannot protect data if we do not have a lock on the server room door. Throughout this course, we will examine how to protect each of the assets listed above.

One area we will examine in more detail later is asset management. In the end, we cannot protect something we do not know about, and having an asset management database (or similar asset tracking system) is crucial to providing the correct level of protection for our assets.

Some assets require little or no protection, and we should not waste the limited resources we have protecting such assets. Some systems and equipment may be at end of life and even though at one point they were critically important, their importance has diminished. This change in asset value complicates the process of asset management as some assets increase in value, while others diminish.

Most organizations will develop a method of identifying the value of assets—data is often listed as business private, business confidential, secret, or top secret. The classification may also be based on laws or regulations that require a certain level of protection for sensitive data.

The benefit of classification is that it mandates the handling of the asset. When a person picks up a document, for example, that is marked as business confidential, they should know how to handle that document—can they discuss it with a co-worker, does it need to be shredded or just recycled? Classification without proscribing the necessary action is a waste of time.

The risk with classification is not to have too many levels of classification so that no one really knows the difference between one level of classification and another. This makes the classification meaningless or ineffective.

As asset values change, the classification should be reviewed, and perhaps a classified document can now be declassified or reclassified.

Important tips on what we covered so far:

Information security is a business-oriented activity. It must address the needs of the business and be built into business operations. An important part of an information security program is a clear understanding of the terminology used and the information security strategy. An important first step in protecting the assets of the organization is to identify all assets and ensure that they are properly classified and protected.

Information Security Principles

Earlier in the course, we discussed the challenge of defining what information security is and how people see information security differently. We tend to see information security as a positive factor that supports and stabilizes business operations, while managers may see security as a necessary cost or irritation that gets in the way of productivity.

We need to convince management and users of the value and benefits of information security and why it is a part of 'their' job and not just the responsibility of some 'other' department. To do this, we need to make security relevant and meaningful and avoid the perception that 'security is immeasurable or impossible'. Security is possible, and security professionals are winning over their adversaries every day. Every time a new flaw is found, an attentive security team patches the vulnerability and shuts down the attack. This causes frustration for the attackers who then constantly need to find new ways to attack.

To define security, therefore, it has become common to use the terms Confidentiality, Integrity, and Availability (sometimes called the CIA triad). The purpose of these terms is to describe security using words that are relevant and meaningful to management and users—to make security more understandable and define its purpose.

Throughout this course, we will use the definitions from CNSS Instruction (CNNSI) 4009, available at www.cnss.gov. The reason for this is simple—it is authoritative and open for use by everyone without cost. While there may be other, even better, definitions for words from other sources, the CNSS definitions are clear and accurate.

Confidentiality

Confidentiality is defined in CNSSI4009 as:

> Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

We can see that confidentiality relates to permitting authorized access to information, but at the same time protecting information from improper disclosure. This is a difficult balance to achieve—especially as a lot of the users on our systems are guests or customers that we have little or no control over. We do not know if they are accessing our systems from a compromised machine or vulnerable mobile application. So our obligation is to regulate access—protect the data that needs protection and yet permit access to authorized individuals.

Related to the area of confidentiality are the terms PII (Personally Identifiable Information), PHI (Protected Health Information), and Classified or Sensitive Information, such as trade secrets, research, business plans or Intellectual Property (IP).

- **PII:** NIST Special Publication 800-122 defines PII as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."
- **PHI:** Information regarding health status, the provision of health care or payment for health care as defined in HIPAA (Health Insurance Portability and Accountability Act)
- **Classified Information:** Information that has been determined to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Another useful definition is Sensitivity:

> A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection. Sensitive information is information that would harm an organization or individual if that information were to be improperly disclosed (confidentiality) or modified (integrity).

Integrity

Data Integrity can be defined as:

> The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.

Another definition is:

> Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Organizations depend on accurate and reliable information—information that can be trusted. This requires the protection of the data in our systems and during processing to ensure that we protect the data from improper modification, errors, or loss. This also includes the reliability of the source of the information—a concept referred to as non-repudiation.

Non-repudiation is defined as:

> Protection against an individual falsely denying having performed a particular action. Non-repudiation provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.

In today's world of e-commerce and electronic transactions, it is more difficult to establish trust. This leads to the threat of a person falsely impersonating someone else or a person denying they sent a message that they had sent. We need to ensure the reliability of the sources of messages and, thereby, have assurance of the integrity of our data.

Availability

Availability can be defined as:

> Ensuring timely and reliable access to and use of information; and
>
> Timely, reliable access to data and information services for authorized users.

The core concept of availability is that data is accessible to authorized users when it is needed. This does not mean that data or systems are available 100% of the time. Instead we ensure that the systems and data meet the requirements of the business for timely and reliable access.

Some systems and data are far more critical than other systems and data, so the security practitioner must ensure that the appropriate levels of availability are provided. This requires consultation with the business to ensure that critical systems are identified and available.

Availability is often associated with the term 'criticality'.

Criticality is defined as:

> A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function.

Least Privilege

Least privilege is a subset of the three concepts of confidentiality, integrity, and availability.

Least privilege is defined as:

> The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

An essential requirement of data protection is to limit the level of access an entity (user or process, for example) has to the minimum level of access required to perform their job. For example, a user may be restricted to read-only access instead of a more privileged level of access, such as administrator access or the ability to modify the data.

The concept of least privilege ensures that controls are in place to prevent unauthorized access to data, improper modification, or destruction of data.

There are several ways to implement the concept of least privilege including mutual exclusivity, separation (or segregation) of duties, and dual control.

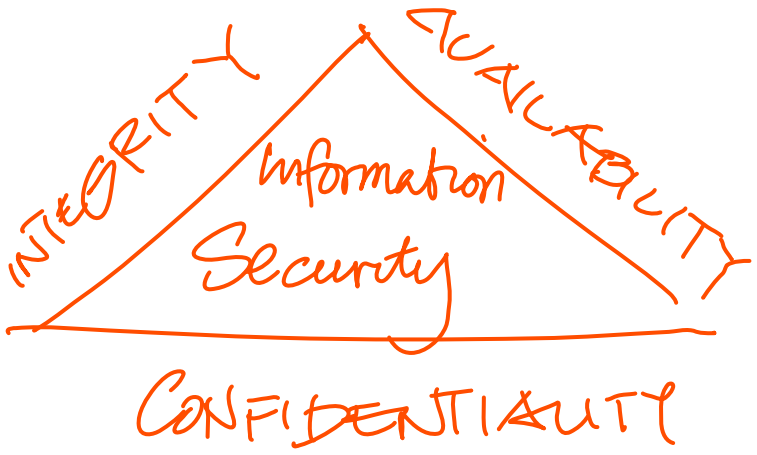
Summary

The concepts of confidentiality, integrity, and availability are effective ways to communicate the goals and objectives of an information security program to management, using language that management can understand and relate to. An effective security program must consider all three concepts and not just focus on one area at the expense of others.

In addition, an effective security program is...

One that understands the needs of the business and provides an appropriate level of security to support business objectives and maintain a stable IT infrastructure.

CIA Triad



Identification of Assets

The security practitioner plays an important role in protecting the assets of the organization. The first step in protecting assets is to identify the organization's assets—after all we cannot protect something we do not know about. We examined this earlier in the course, but now we will look into this important function of the security practitioner in more depth.

The ISO/IEC 27005 breaks the assets of the organization into two categories:

The primary assets:

- Business processes and activities
- Information

The supporting assets (on which the primary elements of the scope rely) of all types:

- Hardware
- Software
- Network
- Personnel
- Site
- Organization's structure

Assets to be examined in this course include:

- Personnel
- Facilities
- Hardware
- Software
- Information

Asset management topics include the systems development lifecycle (SDLC), hardware, software, and all aspects of data management including storage, transmission, destruction, and data loss prevention (DLP).

Discussion: Protecting Assets

What are critical steps in ensuring that all assets are properly protected?

Discussion: Determining Asset Value

How do we determine asset value? Why is it important to know the value of the asset?

Knowing asset value is crucial to ensure that the protection of each asset is appropriate. Appropriate or adequate levels of protection can be defined as a level of security that is commensurate with the risk associated with the asset. When we calculate risk, we use asset value to determine the level of impact that a risk event would have on the organization.

NIST SP800-39 states ". . .it is imperative that leaders and managers at all levels understand their responsibilities and are held accountable for managing information security risk—that is, the risk associated with the operation and use of information systems that support the missions and business functions of their organizations'.

Personnel

For many years it has been said that people are the most valuable asset that an organization has. Indeed, in the end, it is people who can make or break an organization, and security is primarily a people problem. It is important, therefore, to educate, develop and win the loyalty of staff.

Hiring

Hiring the right people to meet job requirements is the first step. This can require verification of education, experience, and knowledge. Unfortunately, there are too many examples of people who have not been truthful on employment applications, or did not have the level of knowledge that they claimed.

Development

Organizations make significant investments in technology, but they often lack in the development of the personnel who are responsible to manage the technology. This often leads to poor and ineffective use of the technology and a failure of the technology to deliver on its potential benefits. Organizations should ensure that the appropriate training is provided to staff. This can lead to a more engaged and loyal staff and more effective security. As will be seen later in the course, Security Awareness training is also an important part of employee development. As seen in the access control domain, it is also imperative to ensure that a person's access is maintained according to the principles of least privilege and that personnel with elevated privileges, such as system and network administrators, are subject to additional (compensating) controls to prevent errors or misuse.

Termination

When an employee leaves a department or leaves the organization altogether, the employee's access should be revoked and any assets that the employee has (such as ID cards, laptops, access tokens, etc.,) should be

recovered. In the case of an involuntary termination, the ex-employee may need to be escorted from the building.

Facilities

Physical security will be looked at in more detail later in the course, but it should be remembered that physical security is an integral part of information security. If a person has access to server or equipment rooms, cabling or electrical power plants, then they can bypass almost any other security measure that is in place. Proper protection of facilities may reduce the risk of theft or compromise of systems or data.

Hardware

Procurement

The first step in hardware asset protection (and also in software asset protection) is to ensure that there is an established process for procurement. The organization must ensure that the correct product is being purchased to meet the needs of the organization. The choice of the 'correct' product may not be simple. Comparing products may require the comparison of features, cost, training, compatibility or interoperability with other products, as well as the relationship with the vendor for ongoing support, upgrades, and maintenance. An important factor in procurement is to ensure that the security requirements are listed in the Request for Quote (RFQ) and also in the purchase contract.

Implementation

Once a product has been purchased, it should be listed in a configuration management database (CMDB) to track the asset. This CMDB should list all assets and their location and ownership. This will permit asset tracking and proper maintenance.

The product should be reviewed once it has been received to ensure that it meets contractual requirements and that the security and operational features are enabled. This would include removing any vendor default passwords or accounts that could be used to compromise the system.

Operations and Maintenance

Equipment needs maintenance and upkeep. This includes applying patches and upgrades and maintaining the correct configuration of the equipment. Equipment should be 'hardened' by disabling unnecessary services, ports, or features that are not required since these services may present an avenue of attack leading to system compromise. Staff turnover may result in inadequately trained staff supporting the system. Equipment that was

installed in a secure manner should remain secure throughout its operational life cycle.

Disposal

When hardware reaches end of life, a new threat emerges. Equipment may fail causing an outage of a critical system. This is a serious problem for many organizations that have a lot of older equipment still in service— some of which they are not even aware of. Equipment may also contain sensitive data that must be properly erased from the equipment prior to disposal. This can be done by overwriting the data, degaussing magnetic media, or physical destruction.

Software

Organizations may acquire (purchase) software, build their own software, or purchase commercially available software and customize it to meet their own requirements. The main challenge related to software is patching. Most software contains flaws that could be exploited by an attacker. This is especially true for web applications. All software should be rigorously tested to detect any vulnerabilities, both prior to implementation and on a regular basis once implemented. As vulnerabilities are detected, they should be fixed as quickly as possible depending on their severity. As a vendor issues patches, the work to roll out patches can be a daunting task for the administrators. This will be examined in more detail later in the course when we look at change management.

Whenever possible the organization should retain a copy of the source code used to write the software program. This is simple when the organization writes the software itself but more difficult when purchasing software from a vendor. The source code should be kept in a secure library that prohibits unauthorized access or modification. The software should also be documented and a copy of the documentation kept up to date and secure. When purchasing software from a vendor, the organization may negotiate with the vendor to keep a copy of the source code with a trusted third party —in escrow. This would allow the organization to obtain a copy of the source code if the vendor did not meet their contractual obligations, perhaps through bankruptcy.

Organizations also must be careful not to implement software that exceeds the number of licenses, or types of licenses, they have purchased. Software piracy can have serious financial consequences for the organization.

- patching
- source code
- licensing (privacy)

Information

Information may be one of the most valuable and also one of the most vulnerable assets of an organization. Business today runs on information and the loss, theft, or compromise of that information may have serious consequences on the organization. These consequences may include financial penalties, loss of customer confidence, loss of competitive advantage, failure of a business process or service, and reputational damage.

Information is protected through classification of the information. Classification ensures that the appropriate level of protection is mandated for the information. This protection may include protection of data in storage, in transit, when displayed, when on reports, or when discussed verbally. Each person that has access to information should know and follow the rules for handling that information. Each person is responsible for protecting the information they have access to.

Discussion: Protecting Information

How can we protect information? What steps should be taken to ensure that information is protected in all forms, at all times?

Information Ownership

The protection of information is the responsibility of everyone, but it still must be the responsibility of a named individual—the information owner. The information owner is ultimately responsible for the overseeing the classification and protection handling requirements of the information. The information owner must be a senior manager who can accept responsibility on behalf of the organization. The naming of an information owner is required by law in many jurisdictions today.

Privacy

The classification of information is often mandated through laws and regulations. These laws may pertain to all organizations within a country, or

they may be specific to one industry vertical (such as healthcare). The organization has a legal (and moral) obligation to protect the information listed in the laws or regulations. Earlier in the course, we examined the definitions of PII and PHI. When the information owner sets out the handling requirements of information, they must ensure that they are compliant with any applicable laws.

In addition to laws, an organization may also be bound by contractual or industry-specific requirements. An example of this is any organization that handles payment (debit or credit) cards (e.g., VISA, MasterCard, AMEX, JCB). These organizations are required to be compliant with the Payment Card Industry – Data Security Standard (PCI-DSS). This standard mandates how a merchant or card processor must protect sensitive payment card data. While this is not a law, it can still lead to significant financial penalties or the loss of card processing privileges if an organization is not compliant with the standard. For many organizations, the loss of permission to accept a payment card for a purchase would seriously impact revenue.

The Payment Card Industry also has standards for software and equipment that handles payment card transactions or PIN (Personal Identification Number) transactions.

Operations/Maintenance

As assets age, they require maintenance and replacement. It is important to ensure that equipment continues to operate in a secure and reliable manner. This requires careful review of the assets to identify old equipment that should be replaced and to review all changes to equipment to verify that they did not open new vulnerabilities or bypass security controls.

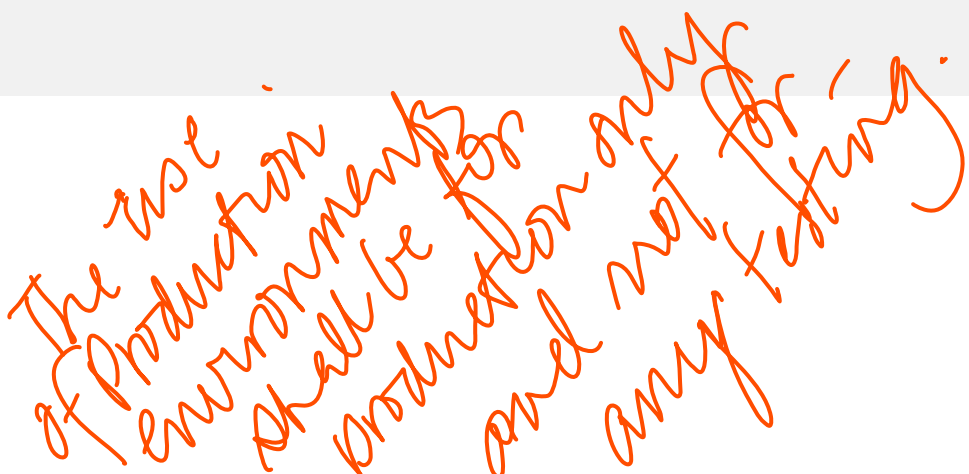
Assets also change in value as they age. A system may increase or decrease in importance, and this affects the risk calculations associated with the asset. A system that increases in value and becomes more critical to supporting business mission may require additional risk mitigation measures that were not justified using earlier calculations.

Third Party/Outsourcing Implications

An increasing number of organizations are outsourcing business processes, data storage, and processing. The availability of easily scalable and cost-effective solutions, such as cloud services and third-party providers, has made outsourcing an attractive and beneficial service.

When an organization outsources a service (e.g., call center) or data hosting (e.g., Cloud), it must be recognized that the responsibility for protecting the assets of the organization remain primarily with the organization not the service provider. In some cases, the service provider may accept a limited liability for an incident, but it is the organization that must answer to its customers and regulators regarding the incident.

The interests of the organization must be protected through contractual agreements and monitoring. The contract with the third-party supplier should mandate the requirements for the protection of the assets of the organization (data, customer lists, research and development). This should include the jurisdiction in which the contract would be enforced and the requirements to protect data once the contract with the service provider ends—perhaps through secure deletion of data and backups. The contractual agreements should also address the need to dispose of old equipment that has been used to store sensitive data properly.



Understand the Risk Management Process Overview

In this section of the course, we are going to begin to look at Risk Management. Risk Management is a critical component of an information security program since it drives the selection of controls used to mitigate business and IT risk. The risk management program manages risk, but does not eliminate it. Risk is an essential part of business operations.

In the IT department, we tend to see risk from a negative viewpoint; it represents the problems and inconvenience associated with IT systems failure. Risk is when something goes wrong, and we have the pressure to fix the problem as quickly as possible. However, in the rest of the business, risk is seen as opportunity—the chance to take a risk and make a return on investment—and the larger the risk, the greater the possible reward (or loss).

First of all, a definition of risk:

> A measure of the extent to which an entity is threatened by a potential circumstance or event and typically a function of:
>
> (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

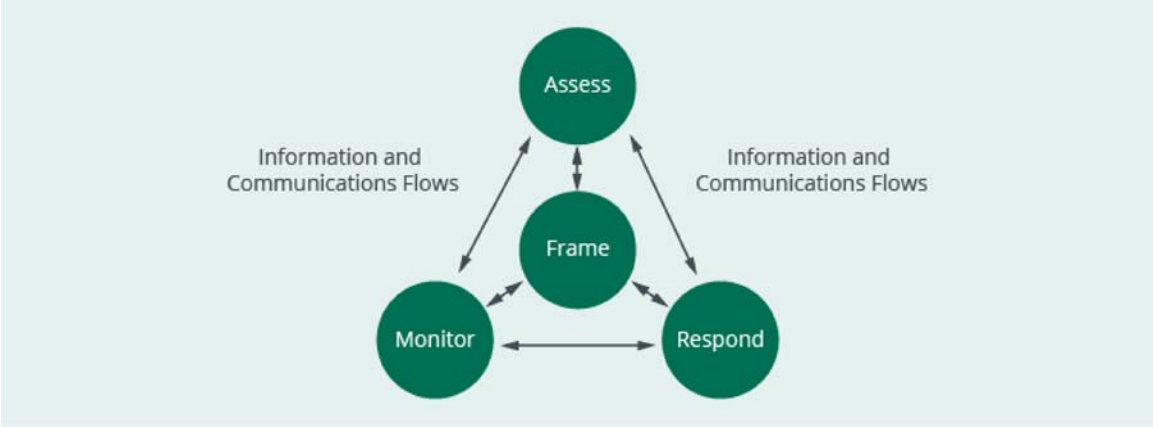
[Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.]

We see from this definition (which is first of all IT based) that risk is associated with threats, impact, and likelihood. But this definition also states that IT risk is a subset of business risk and must be measured by the impact of the risk event on organizational operations, assets, and other third parties.

Risk Management Framework

There are many different risk management approaches, but in this course, we are going to use the process from NIST because it is freely available to everyone and closely aligns with the international standards ISO/IEC 27005 and ISO/IEC 31000.

NIST SP800-39 describes the Risk Management Framework in four parts as seen in the diagram below:



The center of the process is to Frame Risk. This drives the other three components of the process and receives data from them. The next step would be to Assess Risk, then to Respond to the Risk, and finally to Monitor Risk.

While the SSCP security practitioner is not expected to be a risk practitioner, it is still helpful to understand the risk management process so that we can contribute to, and benefit from, the risk management effort.

We are going to take a high level look at Risk Management now and then look into the individual steps in the risk management process in the next few chapters of the course.

Frame Risk

Risk management must always be conducted in alignment with the goals, mission, and culture of the organization. This requires communication with senior management to understand the attitude of the organization toward risk. Some organizations are, by their very nature, averse to risk and try to avoid any risk that could pose a significant impact on the business. On the other hand, other organizations embrace risk and the opportunities that it provides. To further complicate issues, there can often be a wide difference in the attitude toward risk from different departments in the same organization—where sales is energetic and much more risk tolerant than finance, which may be very careful and risk averse.

The first step, therefore, in conducting a risk management effort is to understand the organization and the attitude of senior management toward risk. Does management welcome risk or want to avoid it? When we conduct a risk assessment, we must do it in consideration of management's attitude toward risk. It would be irresponsible to be overly careful and recommend strict risk response actions for an organization that embraces risk or vice versa.

Frame risk also considers both internal and external factors that can influence the risk management approach, such as laws or regulations that mandate how an organization must address risk or service level agreements (SLAs) that an organization must meet even in the event of a serious incident.

Risk management should also be aware of major projects or imminently pending changes that could change the risk environment.

Most organizations will not be able to conduct a single risk assessment for the entire organization and will instead break the risk management process into manageable sized pieces perhaps based on a single product or service, line of business, type of threat, or geographic location. This requires a careful definition of the scope of the risk management effort to ensure that the risk effort is focused on the area within the scope of the defined risk management effort.

Discussion: Today's Risks

What are some of the most serious risks we face today?

Assess Risk

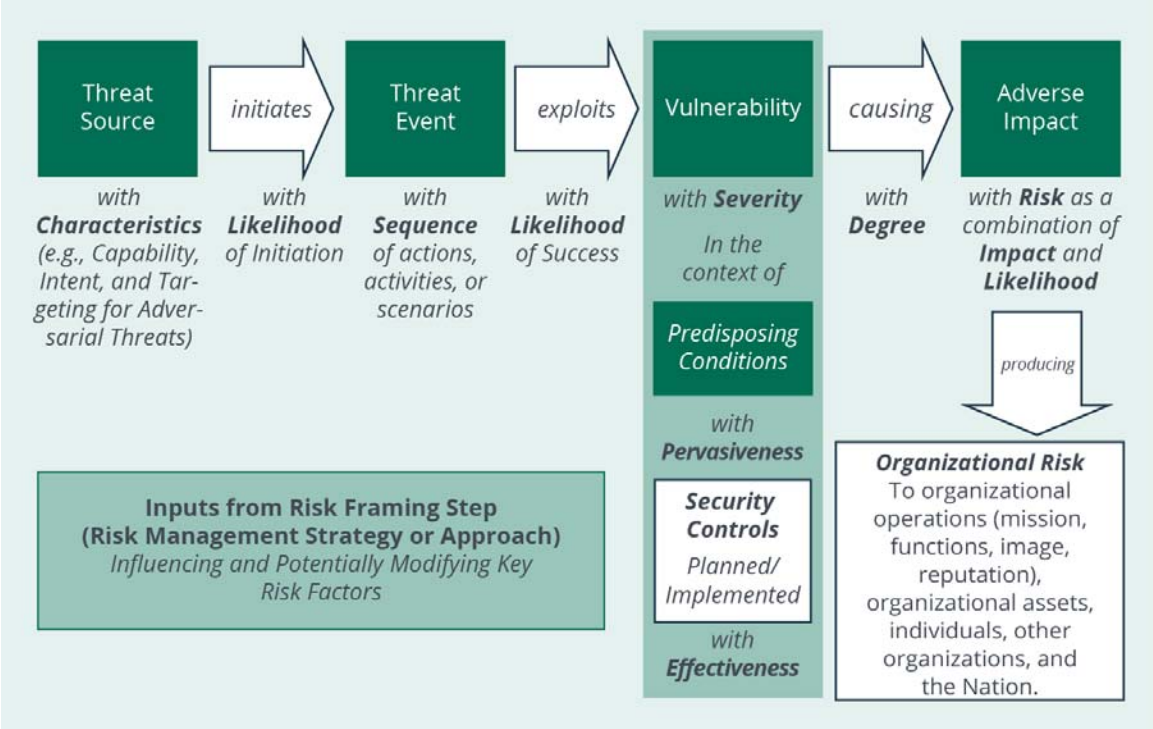
Some risk methodologies break risk assessment into two separate areas—risk identification and risk assessment; however, we will follow the NIST approach and combine the two into the process of risk assessment. Based on the information provided through the Frame Risk process, the process of risk assessment attempts to identify and prioritize risk.

Risk assessment is defined as:

> The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system.

Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

This diagram from NIST SP800-30 Rev1 outlines the risk assessment process:



This diagram shows the process of a risk event and the relationship between the various elements of a risk event. For example, a threat source (hacker) uses a piece of malware (threat event) to exploit a vulnerability in a software product (unpatched system) that is unpatched because of a poor patch management process (predisposing condition), causing damage (an adverse impact) on the organization.

Here are some of the definitions commonly used in risk management:

Threat:

> Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

Vulnerability:

> Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Impact:

> The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Likelihood of Occurrence:

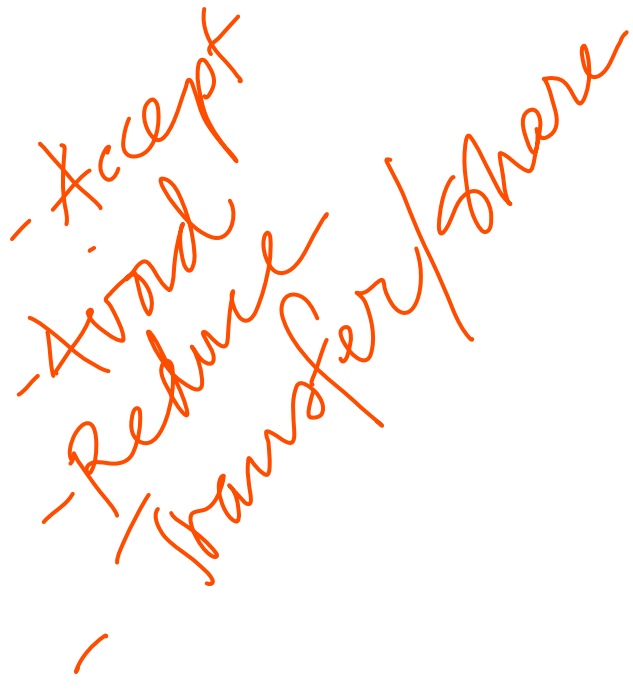
> A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.

Respond—Risk Response

Some documents call this phase Risk Treatment. This is the phase of the risk management process where decisions are made on what is the best action to take in regard to the risk identified in and prioritized through the risk assessment process. The decisions made are dependent on the attitude of management toward risk and the availability—and cost—of risk mitigation. The options commonly used to respond to risk are:

- Accept the risk
- Avoid the risk
- Reduce (mitigate) the risk
- Transfer/share the risk

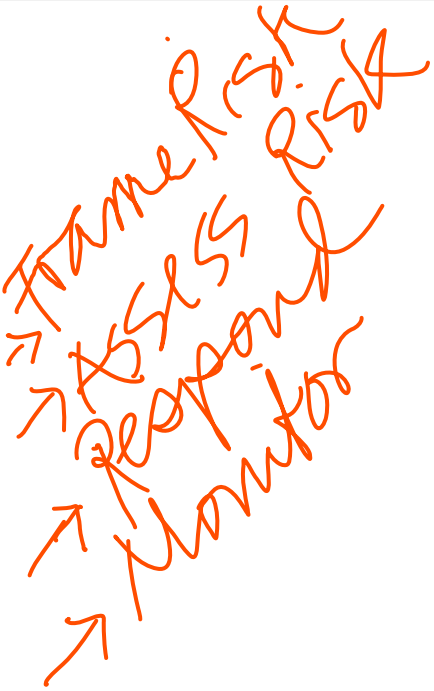
Each of the options for risk response will be examined in more detail later in the course.



Monitor

The fourth step in the risk management process is to monitor risk. Risk changes as new vulnerabilities are discovered, new threats emerge, asset values change, laws or regulations change, and management's attitude toward risk changes. What was an acceptable level of risk previously may not be acceptable in the future.

When the risk respond effort implements controls to reduce risk, it is also necessary to put in place the ability to monitor the controls to ensure they are working. As the controls are monitored, the results are communicated to management. If the controls are found to be inadequate or ineffective, they may need to be replaced, reconfigured, or otherwise supported.



Data Sources for Risk Management

It is important that the results of each step of the risk management process are accurate and complete since those results are needed by the next step in the process and to communicate the current risk profile to management. Performing a risk assessment is both a methodical science as well as a creative endeavor that must imaginatively think of all possible risk events and even forecast the possibility of new risk events not even thought of previously.

Discussion: Identifying Risk

What sources can be used to identify risk?

Vulnerability Identification

As defined earlier, a vulnerability is a weakness that could be exploited by a threat source. A vulnerability is the "hole in the fence," the missing step in the process or the untrained employee that allowed the attack to succeed.

The identification of vulnerabilities is critical to the process of risk management. It would not be possible for an organization to protect itself if it did not recognize and address the vulnerabilities or gaps that could be exploited by a risk event. We recognize the importance of "knowing the enemy" and understanding the threat sources that may attack us, but it is equally important to know whether our organization has the weaknesses or conditions that could be exploited by that enemy.

The process of vulnerability identification is often referred to as vulnerability assessment. Vulnerability assessment is much more than just a technical review of network security. It is the methodical and scientific process of careful examination of the entire organizational environment to find any possible points of compromise. Vulnerability assessment should examine all the areas that comprise the security fabric of the organization—the technical, procedural, physical, and managerial elements of organizational operations that are woven into the overall operations of the business. It must be remembered that even a small hole in a fabric can lead to a major tear or compromise. The vulnerability assessment is successful only when it has identified any possible point of compromise.

If a soldier is appointed to guard a city against an attack, the soldier should examine the defenses of the city to discover where the likelihood of attack would be and where the defenses are inadequate to protect against the motivation and skills of the enemy. Then the soldier can deploy the limited resources available to increase the defenses and monitor against an attack.

Linked to vulnerabilities are "predisposing conditions." Predisposing conditions are environmental factors that could affect the effectiveness of the organization's risk management process. For example, if an organization has an excellent, well-trained and enthusiastic staff that is security aware, the chances of a security breach are much less than for an organization that has

a poorly trained and unhappy staff that are not really interested in putting in extra effort to protect their organization from attack. These are predisposing conditions. Even an organization with outdated but well-managed equipment may be more effective in mitigating risk than an organization with newer but poorly managed systems.

When conducting a vulnerability assessment, the assessor should examine the morale of the staff, whether the staff are compliant with policies and procedures, the effectiveness of monitoring, the openness of communications, the management of assets, and other factors that could represent predisposing conditions that could either increase or decrease risk to the organization.

Discussion: Vulnerabilities

There are many sources of information about vulnerabilities. Which are some of the ones you use?

Summary

We have introduced the risk management framework, and we will continue to look at the framework in more detail in the next few sections of the course. It is important to remember that risk management is an ongoing effort that needs to be revisited on a regular basis as risk factors and control effectiveness may change over time.

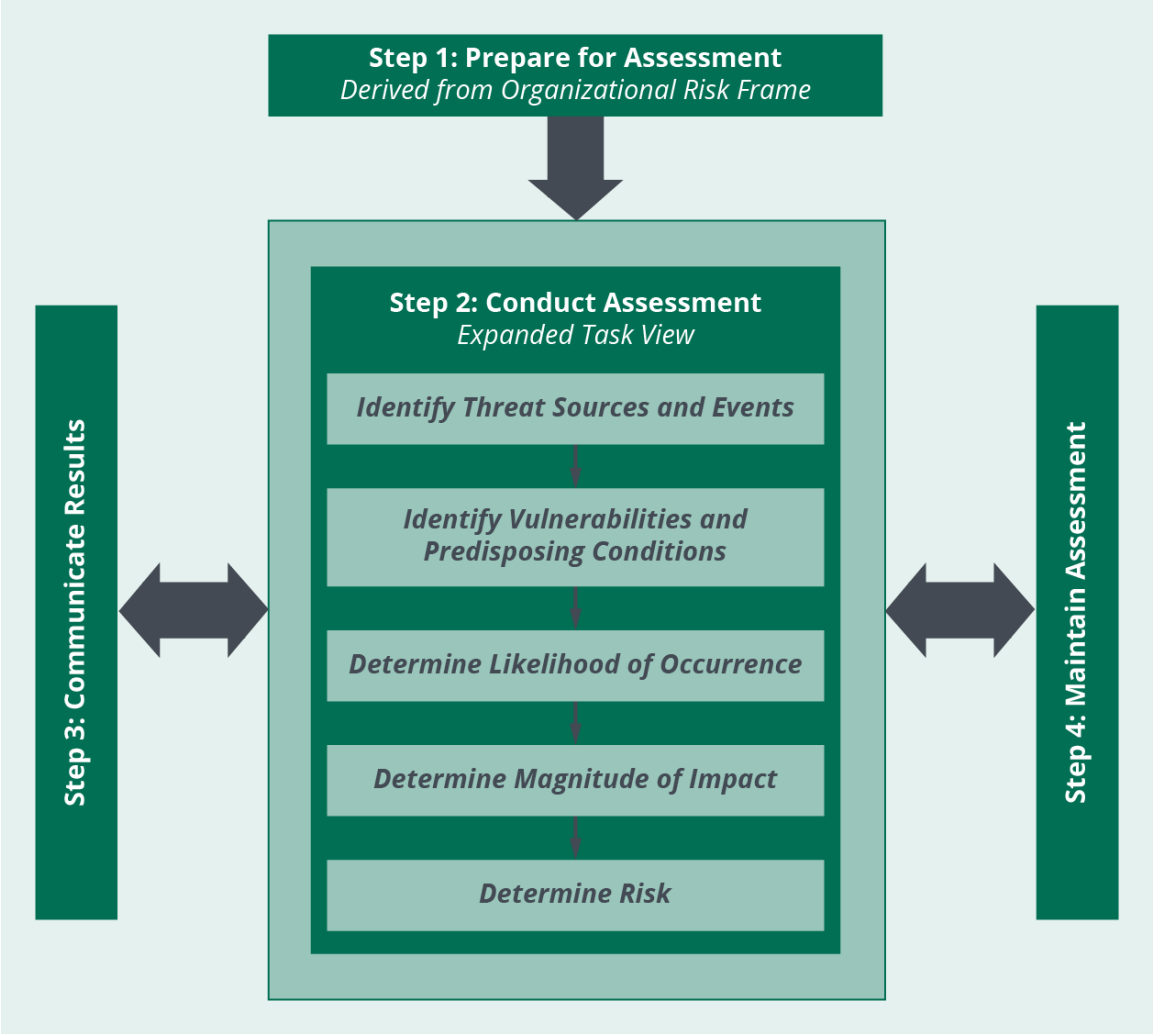
Risk Assessment Overview

The next step after gaining an understanding of the context for the risk management effort (through the Risk Frame process) is to perform the risk assessment.

Risk assessment is the process of identifying risk and then evaluating and prioritizing risk based on the level of importance (severity) of the risk. The final deliverable from the risk assessment process is to communicate risk to management often through a Risk Assessment Report (RAR) and by updating the risk register.

Risk Assessment requires the identification of risk through the identification of threats, vulnerabilities, likelihood, impact, and asset value. Together these are the factors that are used in risk determination.

NIST SP800-30 Rev1 uses the following diagram to describe the risk assessment process:



The determination of risk is not a precise and altogether accurate process because risk calculations work in a general sense but not in any one particular instance. How can a person calculate likelihood, for example? Two processes with identical equipment may experience risk in vastly different manners. One process has frequent failures while the other remains stable and reliable. Even the impact of each failure may vary greatly, sometimes causing negligible damage while other times requiring costly repairs. This unpredictability can raise questions about the validity and value of risk assessment and in fact about the relevance of risk management overall. In performing a risk assessment, care must be taken to gather data that is authoritative and relevant to the assessment being performed. This can be especially difficult when assessing the risk associated with new technology or a new business process, where there is no historical data available to base the assessment on.

Discussion: Improving the Risk Assessment Process

What are some ways we can improve the quality of the risk assessment process, and what sources can be used to gather the data required for the assessment?

Know Your Enemy

A critical step in understanding risk is to know as much as we can about the factors that create risk events. These include both intentional and unintentional threat agents—hackers, employees, users, natural events, equipment malfunctions, and physical problems (power failure, etc.).

Intentional Threat Agents

Intentional threat agents, such as hackers and thieves, attract a lot of attention from the media, and the risk associated with such threat agents is often substantial; however, not all adversaries are the same. When evaluating the risk associated with a hacker, we must also consider the motivation and skill of the attacker. A poorly motivated hacker just looking for an easy way to do damage or gain notoriety may be deterred through fairly simple controls, whereas an Advanced Persistent Threat (APT) will have the motivation, skills, and resources necessary to continue the attack and possibly overcome simple controls. Knowing the capabilities and objectives of the attacker can ensure that the risk controls are appropriate to the threat.

Unintentional Threat Agents

While hackers get most of the media attention, there are far more security breaches and risk events caused by employees and other factors than there are by hackers. A security practitioner must not focus so exclusively on external threats that they overlook the many internal issues that may lead to system compromise or failure. Many threats, such as malware, will be examined later in the course.

Threats related to power failure, flooding, theft, and fire must also be considered in the risk assessment process.

The NIST SP800-30 Rev1 and ISO/IEC27005 both contain lists of threats that should be considered in conducting a risk assessment.

Vulnerabilities

The next step in risk assessment is to know the vulnerabilities and predisposing conditions that may allow a threat to launch a successful attack. Previously, many risk models used threat and vulnerability pairings to identify risk, but this has fallen somewhat out of favor now since a threat may exploit one of many vulnerabilities, and a vulnerability may be exploited by a wide range of different threats.

Vulnerabilities are often seen as the gaps that the threat could exploit—the "hole in the fence." The challenge for the security practitioner is that the hacker may often find and exploit a small vulnerability even though the systems were 99% secure. The slightest gap is often all that a threat agent requires. This requires the security practitioner to diligently look for any gaps or weaknesses and not be content with a security framework that is nearly perfect.

Many times, a vulnerability is related to an existing control such as a security device that is not properly maintained, configured, or monitored. The presence of a security control does not guarantee the effectiveness of risk management. In fact in some cases, the presence of a security control that is not functioning correctly may cause a false sense of security. As will be seen later in the course, when performing a review of a technical security control, it is necessary to verify both the correct operation of the control as well as to review the supporting elements of the control—proper training of staff, change control, monitoring, and incident response. A control that is not being monitored is not going to provide effective protection for the organization.

The Hard Parts of Risk Assessment

Risk assessment relies heavily on the calculations of likelihood and impact. Risk assessment attempts to evaluate risk and set out risk priorities. This requires assessment of what a risk event would cost (impact), and how often could we expect a risk event to happen (likelihood). The problem is that statistics are not exact and dependable. In the big picture, a certain event may happen once in twenty years, but in individual cases the risk event may happen to one person several times in twenty years and yet never happen at all to the person sitting next to them. So to provide accurate and trustworthy predictions to management about risk is often difficult.

Discussion: Gathering Accurate Data

How can a security practitioner attempt to gather accurate data on likelihood and impact of risk?

Likelihood (Probability)

The determination of likelihood of a risk event is often based on what has happened before—which makes the calculation of likelihood very hard for a new process, new technology, or risk event that has not happened previously. There are other factors as well, such as the likelihood of an risk event may be low with a trained and skilled staff, but as that staff moves on and is replaced by staff with less training or experience, the likelihood and impact of the event may change. The likelihood is also based on the factors mentioned previously—skill and motivation of the attacker. The more motivated the attacker, the more likely a successful attack.

Impact (Consequence)

Driving into work this morning, there was new snow on the roads—the first snowfall of the year. As a result, there were numerous vehicles that had slid off the road into the ditch. Of the dozen cars I saw, the impact for most was negligible. The drivers may be late for work, their pride may be damaged, and their confidence of driving may be affected (all qualitative factors), but their cars were undamaged. The drivers were stuck in the snow, but once they had their car towed out of the ditch, they could drive off and continue their journey. However, for one car, which slid off the road like everyone else, running into a tree seriously damaged that car. Here we can see the problem with calculating impact. For ten drivers the quantitative (financial) impact was low, but for one driver it was high. If a risk event happens to our organization, are we one of the ten people with no damage or the one unfortunate one with extensive damage? If I report to management based on a worst-case scenario, does that undermine the credibility of our report if the impact is not as severe as we predicted?

Risk Profile

Determine Risk

The final step in the risk assessment diagram above is to determine risk. This determination sets out the prioritization of risk—which risk events are more serious and should be addressed immediately as compared to less serious events that we can address when time and resources permit.

Determination of risk is based on the value of the asset being protected. What is the importance of that asset to business mission, as well as the threats, vulnerabilities, predisposing conditions, likelihood, and impact of a risk event? When all of these factors are considered, an evaluation of the risk is possible.

The determination of risk provides the data needed to create the risk assessment report and update the risk register. These documents are key resources used by management to gain insight into the risk profile of the organization. The risk profile is simply the description of the risk environment and insight into the maturity and effectiveness of the risk management program. Glancing at the risk register, management can see all known risk facing the organization and whether progress is being made in addressing known risk.

The risk profile of the organization is the description of the current state of risk in the organization. It should be accurate and up to date to ensure that management is aware of the organization's actual levels of risk.

Qualitative and Quantitative Risk Assessment Methodologies

There are two primary methods that have been used to assess risk over the years, quantitative and qualitative. Each one has advantages and disadvantages and neither is perfect on its own. We often, therefore, see a hybrid model of risk assessment used that combines the two methodologies into a semi quantitative approach.

Quantitative Risk Assessment

Quantitative risk is based on money, the financial cost of a risk event, for example in the scenario above, what it would cost me to slide off the road—a risk event caused by the threat of reduced traction due to snow, mixed with the vulnerabilities that 1) I am not a good driver, and 2) the tires on my car were not changed over to winter tires

Those vulnerabilities allowed the threat event to successfully affect business mission (getting to work). This led to an increased likelihood of hitting the ditch and the resulting impact (cost of a tow truck).

SLE – Single Loss Expectancy

We can calculate the quantitative cost of this event as follows:

Single Loss Expectancy = Asset Value * Exposure Factor

SLE = AV * EF

Therefore;

The cost of a single event (hitting the ditch) is equal to the value of the asset (the car) multiplied by the loss in asset value due to the event (exposure factor).

For the person that hit the tree the calculation would be:

SLE = $36,000 * 25%, if the car was worth $36,000 and it suffered 25% asset loss.

SLE = $9,000

So the cost of the single event was $9,000. This is the calculation of impact.

Note: You understand how incomplete such calculations are since there are many other factors to this event we did not include—the cost of loss of use (having to rent a car), loss of income (not getting to work), and the potential cost of injury to the passengers in the car—but we are just looking at a simple example here.

ARO

The next factor to consider is likelihood, how often would this driver expect to have a similar accident.

This is the calculation of Annual Rate of Occurrence.

Annual Rate of Occurrence = Number of Incidents per year

ARO = Incidents/Year

If this is a young driver, the number of incidents may be much higher than for an older, more experienced driver.

Let's say, for example, that this driver could expect to have a similar accident (sliding off the road) once every three years. The calculation then would be:

ARO = 1/3

Note: The reason to calculate ARO as an annual value is to be able to compare events that happen frequently with events that happen rarely. By using a common denominator of "annual," we can compare these events simply. The reason to use an annual calculation is also because most of our security budgets are based on annual periods, and this allows the comparison of the annual cost of risk to the resources available in the budget.

ALE

Now that we have calculated to cost of a single event (SLE) and the frequency of such events (ARO), we can combine those two into the calculation of Annual Loss Expectancy. This calculates the annual value of the risk:

Annual Loss Expectancy = Single Loss Expectancy * Annual Rate of Occurrence

ALE = SLE * ARO

For our calculations above, the calculation of ALE now becomes:

ALE = $9000 * 1/3

ALE = $3000

This tells us that the driver could expect to incur a cost of $3000 per year for sliding into the ditch. This would mean that the driver now needs to calculate the cost of new tires, the cost of not going to work on slippery days, the cost of insurance, etc., against the expected cost of $3000 per year.

This calculation of risk should be documented in the Risk Assessment Report to notify management of the risk.

The next step of the risk management process is to engage in Risk Response, where management will decide what is the appropriate way to address this identified risk.

Qualitative Risk Assessment

Qualitative risk assessment does not rely on monetary values but instead uses scenarios and workshops to identify and evaluate risk. Risk is usually based on a range of values such as seen below:

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very high
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Source: NIST SP800-30 Rev1

We can see that the risk calculation is based on the factors of likelihood and impact using values from very low to very high.

This format works well when talking to the business. It may not know how to calculate cost of an event, but the business can tell us the relative cost and frequency of an event. By talking to people throughout the organization, we then get input on the relative levels of risk to all departments and systems.

Qualitative risk assessment often starts with the development of scenarios. When going to the business, we describe various types of scenarios that could happen and get feedback on the relative impact of each scenario.

Definitions:

Here are definitions of these risk assessment methodologies:

Qualitative Assessment:

> Use of a set of methods, principles, or rules for assessing risk based on nonnumerical categories or levels.

Quantitative Assessment:

> Use of a set of methods, principles, or rules for assessing risks based on the use of numbers where the meanings and proportionality of values are maintained inside and outside the context of the assessment.

Risk Visibility

The results of the risk assessment are documented and communicated to management. This ensures that management is aware of the real risk profile of the organization. This documentation is primarily through a Risk Assessment Report (RAR) that outlines the methodologies used in the risk assessment, the data gathered, and the interpretation of that data into a risk evaluation and prioritization. The RAR may also contain some suggestions for management to consider when addressing the identified risk in the next phase of the risk management framework—Risk Response.

Risk Register

Throughout this module, we have been examining risk gathered through risk assessment; however, there are many other sources of risk that are available within the organization. These include the results of Audits, Incident Management Reports, Penetration Tests, Vulnerability Assessments, Trouble Tickets, etc.

To collate all risk into one place, it is recommended to use a risk register. A risk register may be a simple spreadsheet that lists each identified risk, how that risk was discovered (source), the status of the risk (outstanding, resolved, etc.), and the ranking of the risk. This allows management to see all known risk in one place instead of having to check multiple sources to gain an understanding of the organization's current risk profile.

As risks are addressed and controls implemented, the risk register should be updated to indicate the resolution of the risk.

Risk Tolerance

Just as senior management "owns" and is responsible for the assets of the organization, so does management also "own" the risk to those assets. Senior management determines what is an acceptable level of risk for the organization. As security practitioners, we must aim to maintain the levels of risk within the limits of risk tolerance of management. This is where many organizations can have different levels of risk tolerance, and even within an organization, different departments may have a different attitude to what is an acceptable or unacceptable risk.

The security practitioner seeks to provide an adequate level of security to meet the expectations of management. This is defined as:

Adequate Security:

> Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

Adequate security is provided through the use of security controls. These are selected, or enhanced, in the next phase of risk management based on the results of this risk assessment as documented in the risk assessment report. Controls are justified by risk and should be traceable back to the risk they are designed to mitigate. Controls are defined as:

Security Controls:

> The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

The implementation of controls should reduce risk, hopefully to an acceptable level. The implementation of controls leads to residual risk, which is defined as:

Residual Risk:

> Portion of risk remaining after security measures have been applied.