Module Objectives

After completing this module, the participant will be able to:

1. Discuss the basic concepts of security.
2. Define the CIA security triad.
3. Discuss asset protection.
4. Explain the privacy requirements.
5. Explain non-repudiation and why we need it.
6. Discuss defense in depth.

Overview

One of the first questions we should ask is, what is information security? Information security can have completely different meanings for different people.

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 different contexts depending on the industry in which we work. We can agree that information security is something that is desirable or wanted; it is not just a hindrance or an obstacle, as some 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strategy of the organization; otherwise it is too easy to build an information security program that quickly becomes out of date.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.

Common Misunderstandings

One of the first questions we should ask is, what is information security? Information security can have completely different meanings for different people.

Too often, security falls to the IT department under the misguided assumption that security is achieved through the use of technology. It is true to say that your technology—your IT systems, communication systems, access controls systems etc.—are all vital assets. Indeed, so much so that without these various systems most organizations would not be able to function. But this is not the complete security picture: relying on or simply securing these technical systems will not fully create the security posture that you are aiming for. There is no way that a firewall or IDS system can truly be effective unless we remember that security is a jigsaw puzzle—a puzzle with thousands, tens of thousands of interlocking parts.

If an attacker can bypass your physical security, convince a member of staff that they are legitimate members of the organization or have a user click on an email link, then it really doesn't matter what technology you have in place. A single point of failure will cascade at an alarming rate.

It would also be true to say that we don't have to buy the most advanced system; sometimes a simple training session is more effective. Look at what you hope to achieve, and align it with your stakeholders and available resources. Sometimes less really is more.

Look at the types of problems and keep looking!

https://blog.barkly.com/biggest-data-breaches-2018-so-far

Focus

This course will 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 the 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. When we build security into the business processes, we ensure that the organization is stable and secure.

Bridging the Gap

One reality in information security that will probably never change is the fact that 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

How can you ensure that your limited resources (time and money) are used 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 valuable 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.

Classification and Asset Value

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 the end of their useful life, so even though at one point they were critically important, their importance has now diminished. This change in asset value complicates the process of asset management as some assets increase in value over time while others decrease.

Most organizations will develop a method of identifying the value of assets. As an example, 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 in order to protect it based on its value. When a person picks up a document 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 prescribing the necessary action is a waste of time.

The risk with classification lies in having too many levels of classification so that no one really knows the difference between one level of classification and another. This "overkill" 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 have 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 based on value.

a

Information Security Principles

We have already discussed the challenge of defining what information security is and we saw how people see information security differently. As security practitioners, 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 even an 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 the battle against 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 would-be 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. 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 when many 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 personally identifiable information (PII), protected health information (PHI), and classified or sensitive information. This last category includes trade secrets, research, business plans and 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 or sensitive 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 for which harm would befall an organization or individual if that information were to be improperly disclosed (confidentiality) or modified (integrity).

Consequences of a Breach

The consequences of a breach in confidentiality may include legal and regulatory fines and sanctions, loss of customer and investor confidence, loss of competitive advantage, and civil litigation. These consequences can have a damaging effect on the reputation and economic stability of an organization. Confidentiality supports the principle of "least privilege" by providing that only authorized individuals, processes, or systems should have access to information on a need-to-know basis. The level of access that an authorized individual should have is set at the level necessary for that individual to perform his/her job.

Ensuring Confidentiality

An important measure to ensure confidentiality of information is data classification. This helps to determine who should have access to the information (public, internal use only, or confidential). Identification, authentication, and authorization through access controls are practices that support maintaining the confidentiality of information. A sample control for protecting confidentiality is to encrypt information. Encryption of information limits the usability of the information in the event it is accessible to an unauthorized person.

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 of information whereby it is recorded, used, and maintained in a way that ensures its completeness.

Information must be accurate, internally consistent, and useful for a stated purpose. The internal consistency of information refers to the principle of ensuring that information is correct on all related systems so that it is displayed and stored in the same way on all systems.

Systems' integrity, on the other hand, refers to the maintenance of a known good configuration and expected operational function as the system processes the information. For example, the integrity of a transaction where a customer makes a deposit and the system ensures that the deposit is made to the correct account of the correct amount.. The key to ensuring integrity is knowledge of state. Specifically, the ability to document and understand the state of data or a system at a certain point, creating a "baseline." For example, a baseline can refer to the current state of the information – is it protected. Then to preserve that state, the information must continue to be protected at all times through a transaction.

Going forward from that baseline, the integrity of the data or the system can always be ascertained by comparing the baseline with the current state. If the two match, then the integrity of the data or the system is intact; if the two do not match, then the integrity of the data or the system has been compromised. Integrity is a key factor in the reliability of information and systems.

Integrity controls include system edits and data validation routines invoked during data entry and update; system, file, and data access permissions; change and commitment control procedures; and secure hashing algorithms. Detective controls include system and application audit trails, balancing reports and procedures, antivirus software, and file integrity checkers that could detect a potential problem with the integrity of the information.

The need to safeguard information integrity and system integrity may be dictated by laws and regulations, such as the Sarbanes–Oxley Act of 2002, which mandates certain controls over the integrity of financial reporting. More often, it is dictated by the needs of the organization to access and use reliable, accurate information. Integrity controls such as digital signatures used to guarantee the authenticity of messages, documents, and transactions play an important role in non-repudiation (in which a sending or signing party cannot deny his/her action) and verifying receipt of messages. Finally, the integrity of system logs and audit trails and other types of forensic data is essential to the legal interests of an organization.

Consequences of Integrity Failure

Consequences of integrity failure include an inability to read or access critical files, errors, and failures in information processing, calculation errors, and uninformed decision making by business leaders. Integrity failures may also result in inaccuracies in reporting, resulting in the levying of fines and sanctions, and in inadmissibility of evidence when making certain legal claims or prosecuting crimes.

Integrity also includes the reliability of the source of the information, a concept referred to as non-repudiation.

Non-Repudiation

Non-repudiation is a legal term and is defined as the 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, or 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.

Consequences of Availability Failures

Consequences of availability failures include interruption in services and revenue streams, fines and sanctions for failure to provide timely information to regulatory bodies or those to whom an organization is obliged under contract, and errors in transaction processing and decision making.

Privacy

Privacy can be defined as "the rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information." Personal information is a rather generic concept and encompasses any information that is about or on an identifiable individual.

Core Guidelines

Although international privacy laws are somewhat different in respect to their specific requirements, they all tend to be based on core principles or guidelines. The Organization for Economic Cooperation and Development (OECD) has broadly classified these principles into eight areas: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.

The guidelines are as follows:

- There should be limits to the collection of personal data, and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- Personal data should be relevant to the purposes for which it is to be used and, to the extent necessary for those purposes, should be accurate, complete, and kept up to date.
- The purposes for which personal data is collected should be specified not later than at the time of data collection, and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified above except:
    - With the consent of the data subject or
    - By the authority of law.
- Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure.
- There should be a general policy of openness about developments, practices, and policies concerning personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of its use, as well as the identity and usual residence of the data controller.

- Individuals should have the right:
    - To obtain from a data controller, or otherwise, confirmation of whether the data controller has data relating to them.
    - To have communicated to them, data relating to them:
        - Within a reasonable time
        - At a charge, if any, that is not excessive
        - In a reasonable manner
        - In a form that is readily intelligible to them.
    - To be given reasons if a request made is denied, and to be able to challenge such denial.
    - To challenge data relating to them and, if the challenge is successful, to have the data erased, rectified, completed, or amended.
- A data controller should be accountable for complying with measures that give effect to the principles stated above.

Information Classification

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.

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.

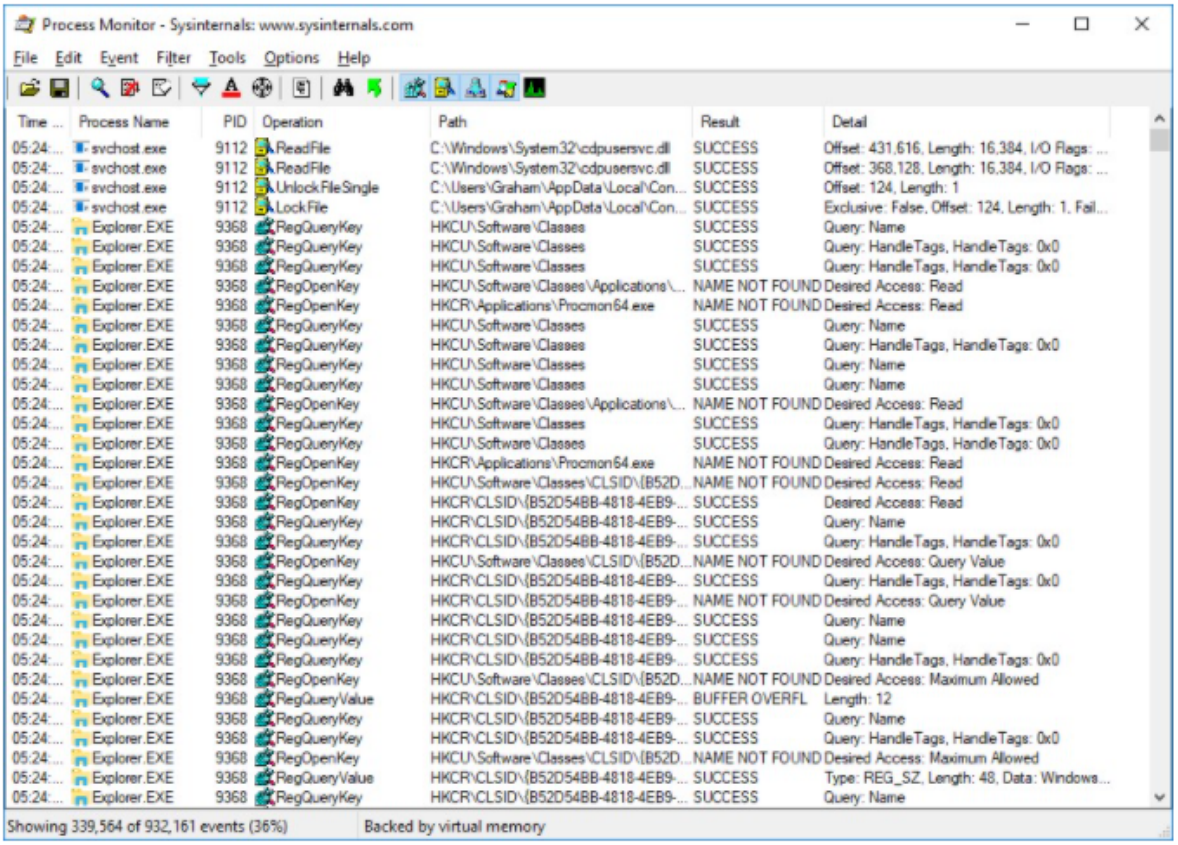
An essential requirement of data protection is to limit the level of access an entity (e.g., user or process) has to the minimum level of access required to perform their job. For example, a user may be restricted to read-only access instead of a more privileged level of access, such as administrator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

Least Privilege and Commercial Off-the-Shelf (COTS) Applications

Unfortunately, many commercial off-the-shelf (COTS) applications are developed in environments that have not adopted least privilege principles and, as a result, these products often require elevated privilege to run. For desktop applications, the use of Microsoft's Process Monitor and similar tools can identify system files, registry keys, and other protected resources accessed by the application so that policy configuration can be modified to provide specific permissions as needed.



The above figure shows an output from Microsoft's Process Monitor. What we clearly see here is a detailed output of the current system activities, even including which registry keys are being used. When we consider software, and how some software requires elevated credentials, the information in the output becomes a critical key to determining the exact access level being used.

However, this is time consuming and only useful in certain operating environments. When a full implementation of least privilege is not feasible or possible, adopting a defense in depth strategy using such things as audit logs, event monitoring, and periodic audits can be used as a compensating control strategy. In practice, privileges are typically set by associating specific roles or groups with an access control entry. Maintaining role or group-based privileges is much more efficient than granting these rights at an individual level, which requires frequent modifications across multiple access entries to accommodate changes in each individual's status and job function. The groups "Everyone," "Public," "Authenticated Users," and the like, which contain all authorized users of a system, should be associated with access control entries that grant only the minimum privileges needed to authenticate to the system.

Separation of Duties

Separation of duties is an operational security mechanism for preventing fraud and unauthorized use that requires two or more individuals to complete a task or perform a specific function. Note that separation of duties does not necessarily require two people to perform a single task, but requires that the person performing a task is not the same person that is checking on the task. Separation of duties is a key concept of internal control and is commonly seen in financial applications that assign separate individuals to the functions of approving, performing, and auditing or balancing a transaction. This ensures that no single person operating alone can perform a fraudulent act without detection.

Dual control is similar to a separation of duties in that it requires two or more people operating at the same time to perform a single function. Examples of dual control include use of two signatures for processing payments, supervisor overrides for transactions over a certain monetary value, and for the recovery of encryption keys.

Separation of duties does not prevent collusion. Collusion is where two or more people cooperate to bypass separation of duties and perpetuate a fraudulent act). Careful transaction balancing and review of suspicious activity and output captured in logs, transaction registers, and reports are the best methods of detecting collusion. In some organizations, additional operational security practices such as mandatory vacation periods or job rotations are enforced to provide management with an opportunity to prevent and detect collusion.

It is important to note that a true defense in depth strategy requires that safeguards not share a common mechanism or be dependent on one another for proper operation. This is because failure of a common mechanism causes failure of all safeguards that rely on that mechanism. A failure of a single-sign-on solution, for example, would interrupt access to all the systems it supports.

Network segmentation is also an effective way to achieve defense in depth for distributed or multi-tiered applications. The use of a demilitarized zone (DMZ), for example, is a common practice in security architecture. With a DMZ, host systems that are accessible through the firewall are physically separated from the internal network by means of secured switches or by using an additional firewall (or multi-homed firewall) to control traffic between the web server and the internal network. Application DMZs (or semi-trusted networks) are frequently used today to limit access to application servers to those networks or systems that have a legitimate need to connect.

Activity: Security Concepts

INSTRUCTIONS

Answer the following questions:

1. What is the principle of least privilege?
2. Why would separation of duties be a useful security measure?
3. What is meant by the term “privacy”?
4. What might be the consequences of a failure of:

    a. Confidentiality

    b. Integrity

    c. Availability

Activity Answers: Security Concepts

Answers

1. What is the principle of least privilege?

    Only allowing the minimal level of access for a person or program to carry out a specific and legitimate purpose.

2. Why would separation of duties be a useful security measure?

    Dividing a task so that more than one person is required to complete that task.

3. What is meant by the term “privacy”?

    The ability of an organization, group or person to seclude information.

4. What might be the consequences of a failure of:

    a. Confidentiality

        Dissemination of private or secret data that may result in harm.

    b. Integrity

        Inaccurate information causing loss or harm to an individual or organization.

    c. Availability

        The inability to carry out a process or function which is critical to the business.

Module 2: Participate in Asset Management

Module Objectives

After completing this module, the participant will be able to:

1. Understand how to identify assets.
2. Explain IT Asset Management (ITAM).
3. Create hardware and software inventories.
4. Explain the hardware and software lifecycle.
5. Describe a hardware/software inventory.
6. Evaluate the benefits of Continuous Diagnostic and Mitigation (CDM).
7. Compare techniques for secure data deletion.

Overview

Asset management deals with the protection of valuable assets to the organization as those assets progress through their lifecycle. Therefore, we need to address the security of assets all through the stages of their lifecycle including creation/collection, identification and classification, protection, storage, usage, maintenance, disposal, retention/archiving and defensible destruction of assets.

To properly protect valuable assets, such as information, an organization requires the careful and proper implementation of ownership and classification processes, which can ensure that assets receive the level of protection based on their value to the organization.

The enormous increase in the collection of personal information by organizations has resulted in a corresponding increase in the importance of privacy considerations. Therefore, privacy protection constitutes an important part of asset security.

Appropriate security controls must be chosen to protect the asset as it progresses through its lifecycle, bearing in mind the requirements of each phase and the handling requirements throughout.

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.

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 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."

IT Asset Management (ITAM)

IT asset management (ITAM) entails collecting inventory, and financial and contractual data to manage the IT asset throughout its life cycle. ITAM depends on robust processes, with tools to automate manual processes. Capturing and integrating auto discovery/inventory, and financial and contractual data in a central repository for all IT assets enables the functions to effectively manage vendors and a software and hardware asset portfolio from requisition through retirement, thus monitoring the asset's performance throughout its life cycle.

Hardware/Software Device Management

A successful attack on hardware/ software is usually based on the exploitation of a vulnerability in the hardware/ software. Unmanaged hardware/software assets are more likely to be vulnerable to attacks; successful attacks on these assets often go undetected because no one is attending to them. The device management capabilities are:

Hardware Asset Management (HWAM)	Software Inventory Management (SWAM)	Configuration Setting Management (CSM)	Vulnerability (Patch) Management (VUL)

- The Hardware Asset Management (HWAM) capability addresses whether someone is assigned to manage the machine and whether the machine is authorized; it does not address how well the machine is managed.
- Quality of management is covered by Software Asset Management (SWAM), Configuration Setting Management (CSM), and Vulnerability Management (VUL).

One reason unmanaged devices are more vulnerable is that no one is actively managing software installation, configuration settings, and vulnerabilities. This leaves the software on those devices with a higher risk of successful attack. If we do not know who is managing the device, we cannot send the responsible individual(s) data to identify problems with software installed (SWAM), configuration settings (CSM), and patching (VUL). In addition, we cannot hold anyone responsible for poor management of the device.

Continuous Diagnostics and Mitigation (CDM)

HWAM supports SWAM, CSM, and VUL. Since HWAM is the first step in proper execution of Continuous Diagnostics and Mitigation (CDM), HWAM must be implemented before the other capabilities can be executed. For example, it is impossible to determine which vulnerabilities exist in software if an organization does not know what software is installed, and it is impossible to manage installed software without knowing which devices the software is to be installed on.

Hardware

For the purposes of Hardware Asset Management, a device is:

- Any hardware asset that is addressable (i.e., has an IP address) and is connected to your organization's network(s). These devices and their peripherals are remotely attackable.
- Any USB device connected to a hardware asset that has an IP address. These devices are a vector to spread malware among devices.

This definition is used by FISMA (a US Government Reporting requirement) and is documented on page 23 of the annual FISMA reporting instructions. Thus, not every "device" in a property inventory is included in the Hardware Asset Management definition of devices. For example, a monitor (not addressable, thus not included) can be attacked only through an addressable computer.

Hardware Inventory

Detailed hardware inventories are necessary for recovery and integrity purposes. Having an inventory of each workstation, server, and networking device is necessary for replacement purposes in the event of facility destruction. All devices and systems connected to the network should be in the hardware list. At a minimum, configuration documentation should include the following information about each device and system:

- Make
- Model
- MAC addresses
- Serial number
- Operating system or firmware version
- Location
- BIOS and other hardware-related passwords
- Assigned IP address if applicable
- Organizational property management label or bar code
- Owner

Hardware Asset Management Data

The minimal Hardware Asset Management data recorded for desired state should include the following:

DATA ITEM	JUSTIFICATION
Expected CPE (customer provisioned equipment) including vendor, product, version, release level or equivalent)	• For reporting device types • For supply chain management • To know what CPEs may apply to these devices
Person or organization who is responsible for managing the hardware asset (note: such assignments should ensure that the designee is not assigned too many assets to effectively manage them)	• To know who should fix specific risk conditions • To assess the responsible individuals' risk management performance
Data necessary to link desired state inventory to actual state inventory	• To be able to identify unauthorized and unmanaged devices

Data necessary to physically locate hardware assets	• So that managers can find the device to fix it • To identify mobile devices so that extra controls can be assigned
The period of time the asset is authorized	• To allow previously authorized devices to remain in the inventory, while knowing they are no longer authorized
Expected status of the device (active, inactive, stolen, missing, transferred, etc)	• To know which authorized devices are not likely to be found in actual inventory
Data necessary to physically identify the asset (such as property number or serial number)	• To be able to validate that the remotely found device is actually this device and not an imposter

Hardware Procurement

The first step in hardware asset protection (and, for that matter, 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.

Hardware 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.

The SSCP's Challenge

There is no denying that Hardware Asset Management (HAM)/Software Asset Management (SAM) is an expense – one that many organizations are reluctant to incur because HAM is seen as directly benefiting the IT department and no other business units. As with any worthwhile IT project, HAM requires an investment of time and effort to put the right people in place, adjust processes, and implement the right technology. Yet, in the bigger picture, implementing HAM can prove to be invaluable for managing computer life cycle and software, new IT initiatives, and expanding the management and reporting functions for the service desk. The SSCP should be prepared to communicate this bigger picture to the business to justify implementing HAM.

Impacts and Results

- Align the organization's HAM strategy with operational goals.
- Identify best practices to maximize hardware asset ROI (Return on Investment) while offering adequate risk protection.
- Construct the supporting documents you need to make the business case to justify the cost of the strategy.

IT savings will start with hardware life cycle management—for instance, saving as much as 20% on hardware, then paving the way for 35% through software asset management, and gaining up to 25% efficiencies for the service desk.

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 lifecycle.

Data Retention and Disposal

A record retention policy and schedule (list of records, owners, retention periods, and destruction methods) is an important component of an organization's information handling procedures. Information owners are responsible for designating retention periods and assigning custodial duties, typically in IT, to ensure that record integrity is preserved for the specified retention period. Audits may be performed to ensure policy compliance. Many organizations use a commercial document management system to organize and automate aspects of their record retention policy.

Handling procedures for confidential information must include provisions for secure destruction of records containing sensitive information. For private industry in the United States, such procedures may be required by U.S. privacy regulations such as the Fair and Accurate Credit Transactions Act of 2003 (FACTA), HIPAA, and GLBA, in Europe these procedures are required under GDPR.

Additional mandates apply to government entities and contractors working with national interest information. Records destruction should be authorized, appropriate to the level of sensitivity of the record, secure, timely, and documented. The goal of secure destruction is to assure the appropriate sanitization of sensitive information so that it is no longer legible and so that insufficient data remains to be pieced together to derive protected data elements. Secure destruction methods are designed to combat the problem of data remanence, which is generally used to refer to the information left in a record or file after the original data has been deleted or moved to another location. Secure destruction methods include burning, shredding (including crypto-shredding), disk cleaning or reformatting, and tape degaussing.

Shredders

Due to environmental concerns, it is often considered inappropriate to burn paper records or CD/DVD media disks. Instead, paper documents and media disks should be shredded using special equipment designed for this purpose. Shredders typically cut paper and plastic items (e.g., disks) into thin strips or small fragments. They come in a variety of capacities, from personal shredders to industrial-strength models; the latter include multimedia shredders that can handle hard drives and other bulky items. Several types of shredders are available, such as:

- **Strip-cut shredders:** Cut material into long, thin strips
- **Cross-cut shredders:** Preferable to strip-cut, these cut material into small rectangular fragments
- **Particle-cut shredders:** Similar to cross-cut; creates tiny square or circular fragments
- **Hammermills:** Pound and grind material until it is fine enough to pass through a screen
- **Granulators (or disintegrators)**: Repeatedly cut material into fine, mesh-size particles

Security Levels

DIN 32757, a shredding standard developed by the German Institute for Standardization, is the de-facto standard used by the shredding industry to classify equipment into hierarchical security levels based on the residue produced by shredding. Government and certain private applications may require use of shredders certified and labeled at a specific maximum-security level for paper documents containing classified information.

Security levels (with general applicability) are:

- **Level 1:** Least secure, cuts material into 12-mm strips; not suitable for classified information
- **Level 2:** Cuts material into 6-mm strips; not suitable for classified information
- **Level 3:** Cuts material into 2-mm strips; limited suitability for confidential information
- **Level 4:** Cuts material into particles 2 x 15 mm particles; suitable for Sensitive but Unclassified or Business Proprietary information
- **Level 5:** Cuts material into 0.8 x 12 mm particles; suitable for Classified information
- **Level 6:** Cuts material into 0.8 x 4 mm particles; suitable for Top Secret information

Shredding services can be contracted to process large volumes of information, either onsite using mobile equipment, or at a specially designed facility. Depending on the application, such companies may require a security clearance and may only be suitable for some classification levels. For typical applications, such clearance may not be necessary, but it is wise to request a certificate of destruction, which most companies will supply on request.

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 physically destroying the equipment.

Destruction of Magnetic Media

Magnetic media, including diskettes, CD/DVDs, disk drives, and tapes, may be destroyed using a number of methods. Often, however, these methods are not environmentally friendly, require excessive manual effort, or are not suitable for high-volume enterprise application. CD/DVD shredders are available at nominal cost and are practical for small business units. Fixed disk shredders are also available, but they are mainly geared to the consumer market and may not produce consistent results with data in disparate formats. When disk shredders are used, they should produce fragments that contain less than one (512k) block of data. Many organizations may wish to preserve the media for reuse or redeployment to another location. For example, many organizations donate used PCs to schools or charitable organizations. Even when media is redeployed within an organization, care should be taken to remove sensitive information before the media is reused.

Methods of destroying data contained on magnetic media include various techniques for clearing or sanitizing data. Clearing refers to any operation that removes or obscures stored data such that it cannot be reconstructed using operating system or third-party utilities. Sanitizing or purging removes data in such a way that it cannot be reconstructed at all. While disk clearing may be acceptable protection against accidental or random disclosure, it is not adequate to prevent someone with intent and commonly available tools from restoring the deleted data.

Cloud service providers should support eradication of data when deleted. Ensure when selecting a cloud provider that the provider can support overwriting and scrubbing information from the shared infrastructure when a deletion occurs.

Data Wiping

Disk wiping, or overwriting, is a method of writing over existing data — typically with a stream of zeroes, ones, or a random pattern of both. Special procedures may be required, such as using certain combinations of patterns or making a certain number of passes over the disk, each time writing a different pattern. Overwriting is acceptable for clearing media for reuse, but is not a sufficient method of sanitizing disk or tape. Overwriting before reformatting is a much more effective technique than reformatting alone and can be a suitable means of clearing less sensitive content from disk.

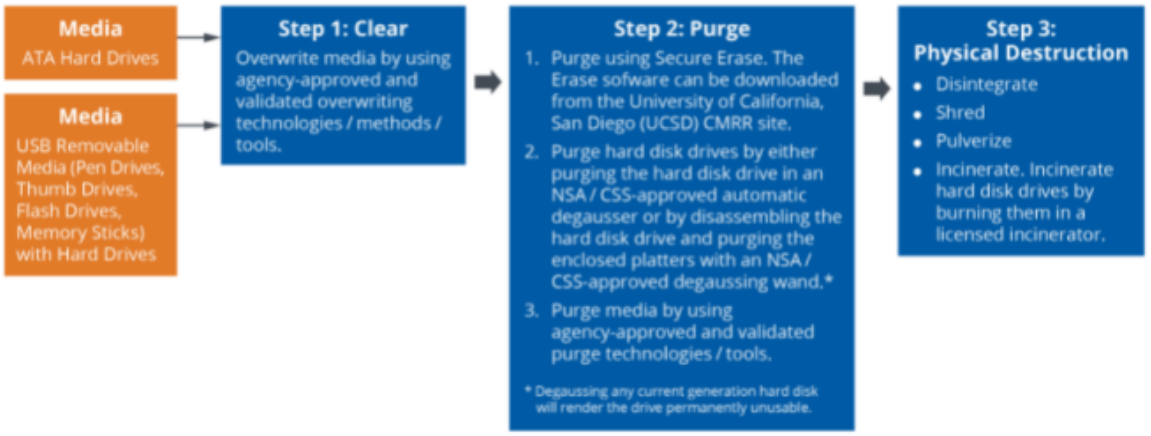
Degaussing

Degaussing is a technique of erasing data on disk or tape (including video tapes) that, when performed properly, ensures that there is insufficient magnetic remanence to reconstruct data. This is performed with a machine called a degausser, which applies a magnetic field to the media and then removes it, eliminating the residual magnetic signals on the media.

Media can be classified in terms of coercivity, or the intensity of the magnetic energy a disk or tape can store, measured in a unit called Oersteds. To perform properly, the degausser must be capable of creating a magnetic field with two to three times the intensity of the capacity of the media. Magnetic tape may be classified by coercivity as type I, II, or III and must be degaussed with a machine rated for the type of tape employed.

Degaussers may be operated manually or be automatic using a conveyor belt assembly. Because of the strength of the magnetic field generated, not all media can be successfully degaussed without destroying the information needed by the servomechanism used to read the disk or tape, which would render the media unusable. This is particularly true of some disk and tape cartridges used in midrange and mainframe systems. Therefore, manufacturer's specifications should be consulted before planning a degaussing strategy.

This matrix is provided by the U.S. NIST SP 800-88 for determining requirements for clearing and sanitizing media at various levels.



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 to support the software, 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.

Software Inventory

A software inventory should minimally include:

- Software name
- Software vendor (and reseller if appropriate)
- Keys or activation codes (note if there are hardware keys)
- Type of license and for what version
- Number of licenses
- License expiration
- License portability
- Organizational software librarian or asset manager
- Organizational contact for installed software
- Upgrade, full or limited license

Benefits of Assets Inventory

The inventory is also helpful for integrity purposes when attempting to validate systems, software, and devices on the network. Knowing the hardware versions of network components is valuable from two perspectives. First, the security professional will be able to quickly find and mitigate vulnerabilities related to the hardware type and version.

Most hardware vulnerabilities are associated with a particular brand and model of hardware. Knowing the type of hardware and its location within the network can substantially reduce the effort necessary to identify the affected devices. Additionally, the list is invaluable when performing a network scan to discover unauthorized devices connected to the network. A new device appearing on a previously documented network segment may indicate an unauthorized connection to the network.

Configuration Lists

A configuration list for each device should also be maintained. Devices such as firewalls, routers, and switches can have hundreds or thousands of configuration possibilities. It is necessary to properly record and track the changes to these configurations to provide assurance for network integrity and availability. These configurations should also be periodically checked to make sure that unauthorized changes have not occurred.

Configuration Management for Operating Systems

Operating systems and applications also require configuration management. Organizations should have configuration guides and standards for each operating system and application implementation.

System and application configuration should be standardized to the greatest extent possible to reduce the number of issues that may be encountered during integration testing.

Software configurations and their changes should be documented and tracked with the assistance of the security practitioner. It is possible that server and workstation configuration guides will change frequently due to changes in the software baseline.

Identification

Identification captures and maintains information about the structure of the system, usually in a configuration management database (CMDB). Each component of the system configuration should be separately identified and maintained as a configuration item (CI) within the CMDB using a unique identifier (name), number (such as a software or hardware serial number), and version identifier. The CMDB may be a series of spreadsheets or documents, or may be maintained within a structured database management system (DBMS). Use of structured databases is preferred to enforce consistency and maintain the integrity of information (such as preventing duplicate entries and preserving associations between CIs) and to safeguard against unauthorized modifications and deletions.

Within the CMDB, changes are tracked by comparing the differences between a CI before and after the change in a change set or delta. The CMDB thus is capable of storing the baseline configuration plus a sequence of deltas showing a history of changes. In addition, the system must maintain a consistent mapping among components so that changes are appropriately propagated through the system. Dependencies between components are identified so that the impacts of logical changes to any one component are known.

Automated Configuration Management Tools

Many in-house software development teams use automated tools for software version change control and other aspects of configuration management. Most development platforms include features such as source code comparators, comment generators, and version checkers. When linked to a central repository, these tools use check in/check out functions to copy code from the repository into a development library or desktop environment, make and test modifications, and place the modified code back into the repository.

Branching and merging tools help resolve concurrency conflicts when two or more individuals modify the same [software] component. Stand-alone or add-on tools are available commercially or as open source and typically contain more robust functionality suited to teams of developers.

Tool vendors do not always distinguish between features that manage the CM process and those that manage actual configurations. Datacenter CM tools, for example, range from stand-alone CMDBs to full suites that include workflow engines, access control, policy enforcement, and reporting capabilities.

Control

All configuration changes and releases must be controlled throughout the life cycle. Control mechanisms are implemented to govern change requests, approvals, change propagation, impact analysis, bug tracking, and propagation of changes.

Control begins early in systems design and continues throughout the system life cycle. Before changes are implemented, they should be carefully planned and subjected to peer review. Implementation and rollback plans (in case of a failure of the change) should accompany the change request. Technical controls to enforce this aspect of CM include access control for development, test and production environments, as well as to the CMDB itself.

Activity: Asset Management

INSTRUCTIONS

Answer the following questions:

1. Why would you degauss?
2. Why is a configuration list important?
3. What are the benefits of having an ITAM policy?
4. Why is it important to consider remanence when disposing of assets?
5. What are some key concerns about software licensing?

Activity Answers: Asset Management

Answers

1. Why would you degauss?

   To completely destroy data on magnetic media.

2. Why is a configuration list important?

   Configuration data becomes important when trying to recover (rebuild) systems after adverse events.

3. What are the benefits of having an ITAM policy?

   Unlike simply asset management ITAM also tracks the financials associated with assets (purchase costs, service contracts etc.) as these are also part or the organization's assets.

4. Why is it important to consider remanence when disposing of assets?

   An asset, a disk, thumb drive or even a paper document, may contain information which is critical to the business or to individuals. If this is released it may have serious impact and therefore must be correctly handled. Often this is overlooked when disposing of old IT equipment.

5. What are some key concerns about software licensing?

   Software purchased outside of the normal procurement process may present an organization with licensing issues together with problems pertaining to patch testing and release. Software also needs to go through a functionality and security testing process, too often it is evaluated based only on form and function with little or no consideration of the security functions, or lack thereof.

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 for 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.

Disclosure Controls: Data Leakage Prevention (DLP)

Various implementations of data leakage prevention (DLP) systems exist; the two most common are those that protect transfer of sensitive data to mobile storage devices such as USB keys and smartphones, and those that prevent data leakage via web and e-mail at an organization's Internet gateway. Less prevalent are those solutions that tackle confidentiality of data at rest in files, databases, and mass storage facilities. An effective data leakage prevention strategy includes use of both host- and network- based components that perform the following functions:

- **Data discovery:** The process of "crawling" distributed files and databases to locate sensitive data is the first step in implementing data leakage prevention tools. The discovery process has intrinsic value, even without implementing loss prevention tools, in that organizations can use it to pinpoint exactly where their sensitive data are stored and design additional safeguards, such as policies and access control mechanisms, to protect the data. One may, for example, uncover cases where users run queries over sensitive data that are stored in a secured database and then save the results to their desktops or to an unsecured public file, where access control safeguards may be weaker. (Note that this violates the "*" property of the Bell–LaPadula Confidentiality model!)
- **Labeling:** Data may be labeled or "tagged" with an identifier that can be used to subsequently monitor movement of that data across the network. This is particularly useful in identifying documents and files containing sensitive information. Labels used may correspond to the sensitivity levels defined in the organization's information classification policy or may identify specific types of data such as Protected Health Information (PHI).

- **Policy creation:** Content monitoring and usage policies specify which data are sensitive and define rules for copying or transmitting that data, typically using a combination of predefined labels, keywords, and regular expressions (e.g., nnn-nn-nnnn to identify a Social Security Number) to identify unique data elements.
- **Content detection/monitoring:** Data communications over local and wide-area networks, data traversing perimeter gateway devices, and data leaving host computers via USB or serial connections are monitored by inspecting the contents of the communication at the file, document, and packet level. At the network layer, packet-level monitoring can be used to identify and intercept transmission of sensitive data through FTP, SSL, and posting to blogs and chat rooms among other things. Documents transferred as attachments to email and instant messages can also be monitored and blocked at gateways if they contain sensitive content. To identify data transferred to removable storage, software agents are typically employed on target machines to monitor traffic over USB, wireless, and Firewire ports.
- **Prevention or blocking:** When policy violations are detected, user actions may be prevented or network traffic may be dropped, depending on the location of the violation. Alternatively, encryption may be enforced before a write operation to CD, USB, or other removable media.
- **Reporting:** Violations of data disclosure policies are reported, typically showing the policy that was violated, the source IP address, and the login account under which the violation occurred.

Regardless of the method used to detect and prevent data leakage, it should be supplemented with traditional safeguards such as physical and logical access controls, encryption, and auditing. It must also be kept current to accommodate changes in applications, business processes and relationships, and infrastructure.

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. The PCI-DSS is not a law, but 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 Personal Identification Number (PIN) 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 the change 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.

Risk and Asset Value

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."

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 (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.

Summary

In this module we focused on the identification of assets. As we saw, the assets to an organization are many and varied, but what we have to bear in mind is that most organizations will have multiple business units. In turn, each business unit will have multiple and potentially different assets. Before we can move on to a risk management phase, and then to a control phase, we must identify several elements:

1. What are our business units?
2. What assets—hardware, software, people, and more—are necessary to support those business units?

Having identified, classified, and recorded our assets we are ready to move forward.

Module 3: Understand the Risk Management Process

Module 3 Objectives

After completing this module, the participant will be able to:

1. Describe the risk management process.
2. Understand risk frameworks.
3. Define risk concepts (e.g., threats, vulnerabilities).
4. Describe Common Vulnerability Scoring Systems (CVSS).
5. Identify source systems.
6. Interpret report findings from monitoring results.

Overview

In this module we begin to look at the risk management process. 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. We see risk as what happens when something goes wrong, and we are under 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 is a measure of the extent to which an entity is threatened by a potential circumstance or event and typically a function of (1) the adverse impacts that would arise if the circumstance or event occurs; and (2) the likelihood of occurrence.

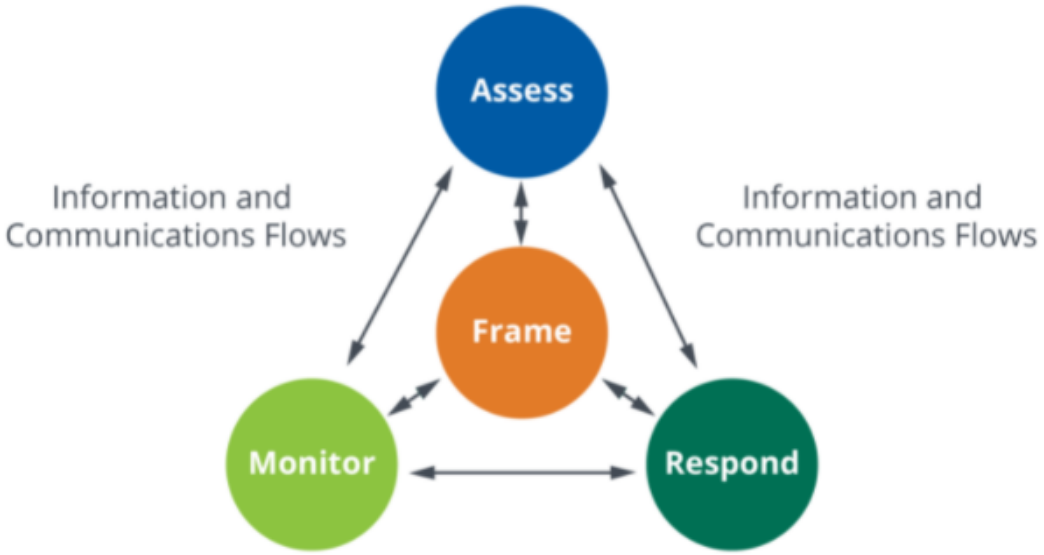
[Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational 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 the central function, which is to Frame the Risk. Framing 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 will 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—for example 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 (appetite) toward risk. It would be irresponsible to be overly careful and recommend strict risk response actions for an organization that embraces risk, while the reverse is true in an organization that is highly risk averse.

To frame risk we also need to consider 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, and service level agreements (SLAs) that an organization must meet even in the event of a serious incident.

Risk management should also be aware of imminent major projects and pending changes that could affect the risk environment.

Most organizations will not be able to conduct a single risk assessment for the entire organization and will instead break the 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?

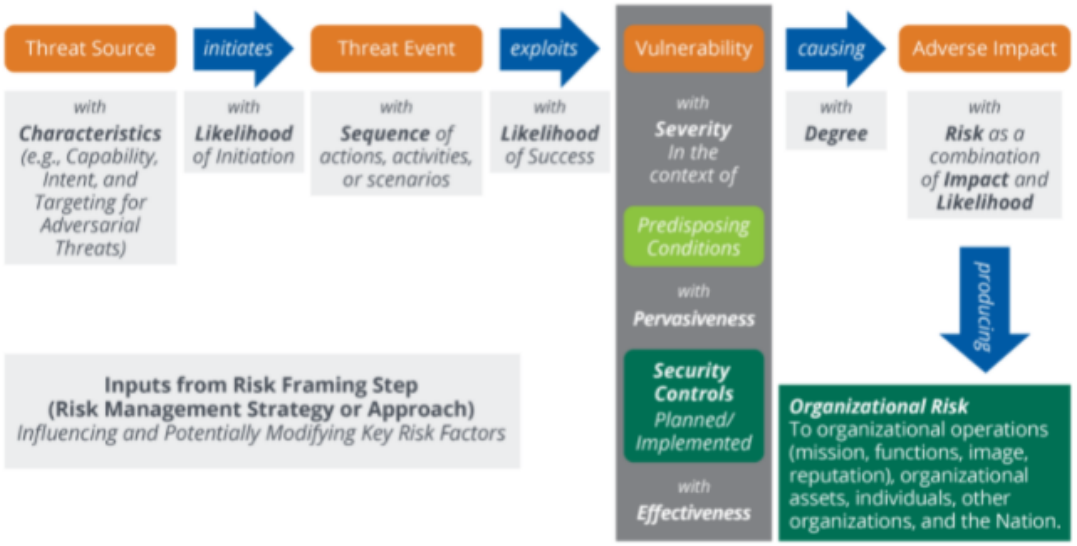
Assess Risk

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. It is 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.

The result of the risk assessment phase is a report on risk that documents and prioritizes the identified risk. This report is provided to management for review and approval. In some cases, management may indicate a need for a more in-depth or detailed risk assessment. This report will be used in the next phase of Risk Response.

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 Risk

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 previously an acceptable level of risk may not be acceptable in the future. When the risk response 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.

Continuous/Compliance Monitoring

Monitoring is the ongoing, near-time analysis of traditional and non-traditional data sources, related to targeted business activities and controls, to proactively identify, trend, and respond to potential compliance "signals" and to be predictive of user behavior. Monitoring is considered distinct from auditing, which is typically retrospective and often limited by time, frequency, and scope. Monitoring results inform corrective action plans, including full-scale compliance investigations, policy changes, enhanced training and communications, additional monitoring, focused audits, and other programmatic responses.

Continuous monitoring represents the desire to have real-time risk information available at any time to make organizational decisions. Continuous monitoring systems are comprised of sensor networks, input from assessments, logging, and risk management. When implemented correctly, continuous monitoring systems can provide organizations with a sense of information security risk; when not configured correctly, they can lead an organization to false panic or a false sense of security.

The Need to Monitor

The risk response was based on management's direction and acceptance of risk. As a result, we now should see that the level of risk has been reduced to an acceptable level, and any other areas of risk that still need mitigation are listed in the risk register with an action plan to address those areas according to the agreed-upon schedule.

The reality is that risk management is a cycle—a never-ending effort—and even though the best steps have been taken to respond to risk, there are many risk factors that change. This means that we need the next step in the framework, monitoring.

In the monitoring phase, we will:

- Evaluate the effectiveness of the controls
- Watch for changes in risk
    - Asset value
    - New threats
    - New vulnerabilities
    - New legislation
- Report (Communicate) risk levels to management
- Comply with legal reporting requirements
- Support audit
- Trigger a new risk assessment when necessary

Data Sources for Risk Management

It is important for the results of each step of the risk management process to be 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 and 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.

Sources System or System of Record (SOR)

These are terms which we would generally apply to the management of data, perhaps a data warehouse. When we are talking about risk however, we are talking about an ability to collate and normalize data from different monitoring systems, then feed that information into a risk assessment process or a CVSS system.

Information can be supplied from external sensors and systems or from your operational database. Event logs, IDS/IPS logs and compliance monitoring systems all provide information to the central repository.

We will look more deeply at these devices as we progress through the course.

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 make up 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 effectiveness of the defenses and monitor against an attack.

Linked to vulnerabilities are "predisposing conditions." Predisposing conditions are environmental factors that could diminish 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, the extent to which 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?

Common Vulnerability Scoring System (CVSS)

Understanding vulnerabilities can sometimes be problematic. To attempt to address this problem, an open source standard exists to assist help assess the issues. It helps to identify the severity and to prioritize the response by assigning severity scores.

The current version is CVSSv3.0; it was released in 2015.

Common Vulnerability Scoring System (CVSS) uses three measurement factors:

1. **Base metrics:** access, attack and authentication
2. **Temporal:** how the characteristics evolve over time
3. **Environmental metrics**

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.

Module 4: Understand the Risk Management Process - Risk Treatment

Module Objectives

After completing this module, the participant will be able to:

1. Understand a risk profile.
2. Describe a risk profile.
3. Evaluate the organization's risk appetite/tolerance.
4. Differentiate between quantitative and qualitative risk assessments.
5. Understand risk terms.
6. Identify risk visibility.

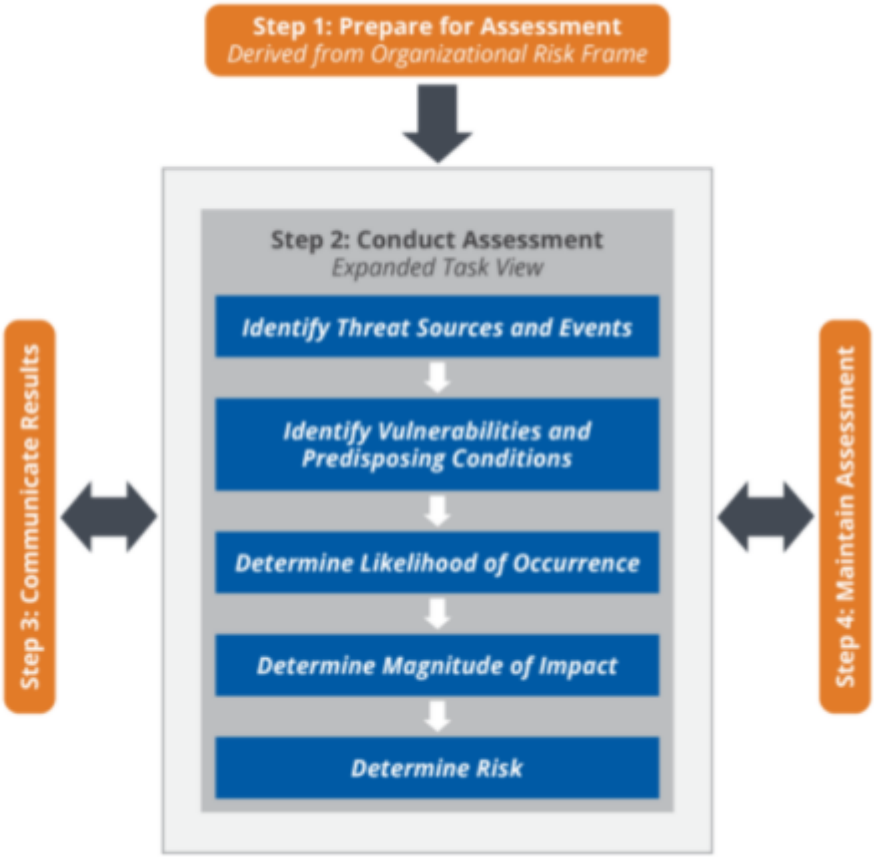
Overview

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 ways. 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 but at other times requiring costly repairs. This unpredictability can raise questions about the validity and value of risk assessment and even 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, intentional adversaries come in many different guises. 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 unintentionally 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. Certain external 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 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, and sets out risk priorities. This requires assessment of what a risk event would cost (impact), and how often we could expect a risk event to happen (likelihood). The problem with the latter is that statistics express likelihood, not predictions. A certain event may have a twenty-year statistical probability (i.e., overall it is likely to happen only 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. For this reason it is extremely difficult to provide management with accurate and trustworthy predictions about risk.

Discussion: Gathering Accurate Data

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

Risk Profile

Determine Risk

The final step in the NIST SP800-30 Rev1 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 semiquantitative approach.

Quantitative Risk Assessment

Quantitative risk is based on money, the financial cost of a risk event. For example in the snow-during-rush-hour scenario above, what it would cost me to slide off the road? That would be 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 in need of replacement.

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

Single Loss Expectancy (SLE)

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.

Annual Rate of Occurrence (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, newly licensed 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.

Annual Loss Expectancy (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 (ALE). 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 = $9,000 * 1/3

ALE = $3,000

This tells us that the driver could expect to incur a cost of $3,000 per year for sliding into the ditch. This would mean that the driver now needs to calculate the costs of reducing this risk—the cost of new tires, the cost of not going to work on slippery days, the cost of insurance, and other risk-reduction measures—against the expected loss (cost) of $3,000 per year.

This calculation of risk should be documented in the Risk Assessment Report to notify the organization's managers and decision makers of the risk.

The next step of the risk management process is to engage in Risk Response, where the organization's managers 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

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. The NIST evaluation may not be able to calculate the actual financial costs, but the business can translate this into 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 presenting risk assessment results 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, and similar processes.

Date of Risk Review _____
Compiled By _____ Date _____
Function/Activity _____ Reviewed By _____ Date _____

Ref	The Risk: What Can Happen and How It Can Happen	The Consequences of an Event Happening		Adequacy of Existing Controls	Consequence Rating	Likelihood Rating	Level of Risk	Risk Priority
		Consequences	Likelihood					

To compile 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 o 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 regarding 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 follows.

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 follows.

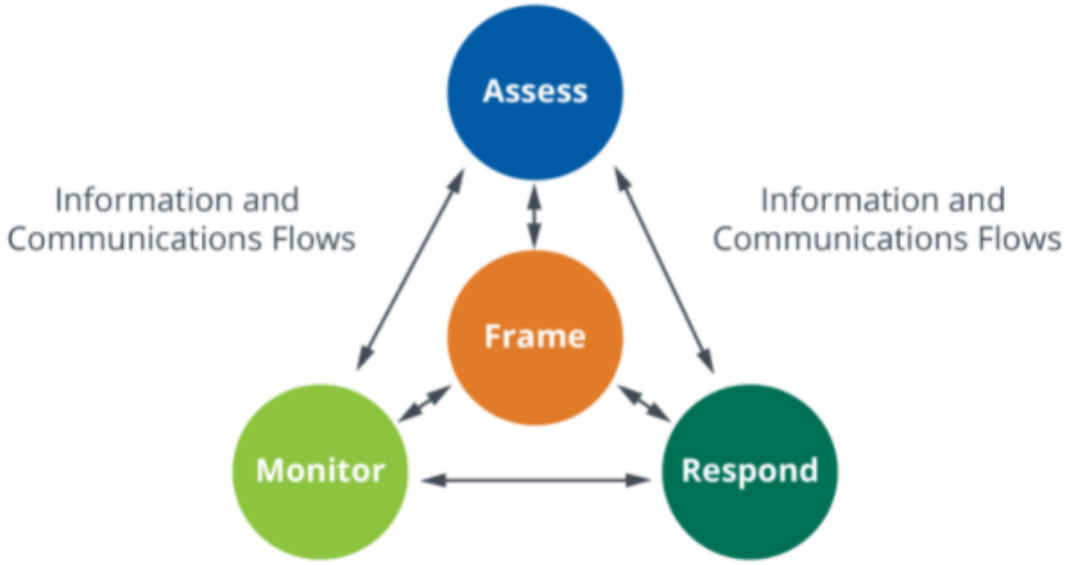
Security Controls: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

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

Residual Risk: Portion of risk remaining after security measures have been applied.

Risk Treatment Options

We have now completed the first two steps of the Risk Management Framework. We saw this diagram earlier from NIST SP800-39:



The first step was to frame the risk (or, as ISO/IEC 27005 calls it, to establish the Context) of the risk management effort. This set out the scope and identified internal and external factors that could influence the risk management effort. Then we performed the process of Risk Assessment where we identified and evaluated risk based on threats, vulnerabilities, likelihood, and impact of risk events. The final result of the Assessment step was a Risk Assessment Report (RAR) that was provided to management. The RAR documented the identified risks and also may have included some ideas or recommendations for how management might respond to the risk listed in the report.

Now we come to the Respond step, where management must decide how to respond to risk. Management's response to risk is based on management's attitude toward risk. What is management's risk appetite or tolerance? People have different appetites—some people enjoy spicy foods while others do not. It is the same with risk, as some people enjoy the thrill and challenge of taking a larger risk in hope of gaining a larger reward, while others are more cautious and will give up a larger reward in exchange for "playing it safe" with a lower level of risk and a more stable operational environment. The challenge for the security practitioner is to gain an understanding of management's appetite for risk and set out a risk response strategy aligned with that appetite.

There are four usual responses to risk, referred to in ISO/IEC27005.

- **Avoid risk:** cease the risk-laden activity
- **Accept risk:** take no action to reduce risk and instead accept the consequences of a risk event
- **Mitigate (reduce) risk:** implement or enhance controls
- **Share/transfer risk:** pass some of the risk to another party, such as purchasing insurance

The decision of the "best" risk response option can be difficult since there may be many possible alternate solutions and each alternative may have advantages over the other solutions in one way or another.

Discussion: Risk Factors

What are some of the factors that need to be considered when deciding on the best way to respond to risk?

Cost-Benefit Analysis

The general rule is not to pay more to protect an asset than the asset is worth. Spending $10,000 on a $5,000 problem is probably not wise.

One of the harsh realities faced by information security teams is that there will never be enough time or money to do everything that needs to be done. Therefore, the risk analyst and security practitioner have to investigate which risk treatment options are available and then perform a cost-benefit analysis on the various available solutions. Is it better to drive an expensive car or a cheaper one? Does quality save money in the end? These are hard questions that plague the risk analyst who has to determine whether to recommend a more expensive control that may have additional features over a cheaper option that may meet basic requirements.

This creates conflict related to priorities and tasks to find the correct balance between what has to be done, what to spend money and time on, and whether the resources are available to do everything to the best possible standards.

The justification for many projects is return on investment (ROI): what will be the return or benefit from an investment in a new technology or a modification to a business process? Calculating ROI for investment in security can be a challenge because if the investment is successful then ideally nothing will happen! This is the same with risk management—how can we justify the cost of a control? We try to use cost-benefit analysis where we compare the cost of the control with the benefit obtained through the control. In some physical cases this can be easy. For example, a company installs a new fire detection and suppression system that will reduce their insurance premiums, reduce the damage caused by a fire, and allow for faster resumption of operations following a fire. The benefits can be fairly easy to quantify and then they can be compared with the cost of the new system. If the benefits outweigh the cost of the system, it is probably a good investment. (But, again, this does not factor in the problem of likelihood. One organization can spend a lot of money on fire suppression and never have a fire—never need the system—while their neighboring company spends nothing on fire suppression and also does not have a fire. One company spent money on a system they did not use and the other saved the money and made additional profit from saving the money.) Who said risk management was easy?

One of the key requirements for a security program today is the need to make security accountable for its budget. Management may see security as a "black hole" where money sinks into darkness from which nothing ever seems to emerge. Instead management needs to see the benefit of a security program—how security is utilizing its resources and supporting and benefiting the business.

If a risk assessment report indicates that the organization should invest in new equipment, for example, a new firewall, then management wants to see the cost/benefit analysis of this recommendation: the cost of the firewall compared to the way the firewall will benefit the organization. This is one reason why a quantitative risk assessment (where the risk was measured in monetary values) was so important. Management will rarely be convinced to spend money because a qualitative risk assessment categorized a risk as a "Level 5 Risk." Management may say that if you want to spend money on a firewall, then it is important to show the monetary benefits from that firewall, which can be difficult to do.

Calculation of Cost

There is an old story of a customer walking into a car dealership and asking what the fuel efficiency was on a high-end car, to which the sales agent replied, "If you have to ask that, then this is not the car for you." This is recognition of the complexity of calculation of cost. The calculation of the cost of a control, such as a firewall, is based on much more than just the initial price of acquisition. In some cases, a vendor may even give away the initial product (e.g., a printer) for free, because they know that their real profit will come from the ongoing support for the product (toner cartridges, licensing, maintenance agreements, etc.). The security practitioner should include these ongoing costs in the cost-benefit analysis. After all, no one wants to be given money to purchase a firewall only to find there is no operating budget for training, support, licensing, or repair.

Discussion: Benefits of Security Investment

How can we calculate benefits—what are some of the ways to convince management of the benefits of investment in security?

Action Plan

The selection or choice of the risk response strategy drives the development of an action plan to roll out the chosen controls and enhancements. In many cases, a risk may be addressed through the enhancement of existing controls. It is often the case that an organization already has everything it needs to improve its security; it is just that many of the controls are not configured correctly or properly managed. The owner of the risk is also responsible to ensure that the controls implemented to mitigate the risk are also working correctly.

An action plan is important; it needs to have allocated resources, delivery dates, milestones, and reporting requirements. Without such details, it is questionable whether the project will ever reach completion.

A single control may not be adequate to mitigate a risk, In this case, more than one control may be required. If there are no cost-effective controls available to reduce the risk to an acceptable level, the organization may choose to purchase insurance to cover the remaining risk.

In the next phase of the risk management framework, the security practitioner may be required to support the monitoring of, and reporting on, risk. This may require that a control is configured to support the gathering of audit data and create suitable logs.

Risk Acceptance Levels

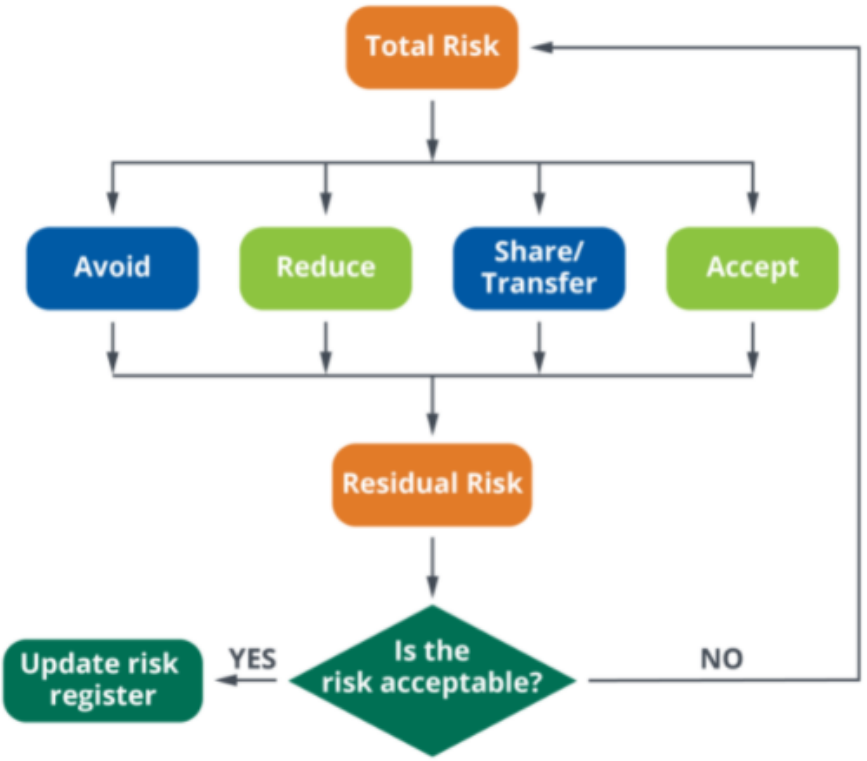
The goal of risk management is to ensure that all risk is within the risk acceptance levels set by management. We have already discussed how management may determine what is an acceptable level of risk and, in the end, only management can accept risk on behalf of the organization.

As per the risk assessment report, some identified risk may already be acceptable, but other risk may still remain that requires some form of risk response. This is where the decisions have to be made of what is the best response to the identified risk. Each of the risk response options is examined in more detail below.

Risk Response

Risk may be shared, avoided, reduced, or accepted. Which is the best solution? In some cases, more than one risk response may be required: to implement technology and, in addition, to purchase insurance. In the end, the implementation of controls will determine residual risk, the level of risk that remains after a control is implemented.

For example, a person purchases car insurance. This response shares or transfers (most of) the risk to the insurance company in exchange for an annual insurance premium that must be paid by the owner of the car. The insurance company ensures that they charge each insured person a premium for the insurance that would be enough to pay for any claims made against the insurance company, but even the insurance company shares the risk. They often purchase re-insurance so that if there are excessive claims, their re-insurance will pay for the amount of the claims above a certain limit.



For the owner of the car, insurance provides protection from total loss of the asset—the car. However, the owner of the car is still liable for the first part of a claim, often called the deductible, or excess. If the owner makes a claim, they know they have to pay for the first $500 of the claim, and the insurance only covers the amount in excess of $500. This deductible is the residual risk—it is the amount of risk the owner of the car still faces even after the implementation of the control (insurance).

Risk Avoidance

Risk avoidance is to cease the risk-laden activity. For example, an organization may close a branch office in a region that it considers unsafe. The choice to avoid risk protects the assets of the organization from a level of risk that cannot be effectively mitigated (based on cost or available solutions). This also means that the organization would also lose any potential benefit from continuing that business operation.

Risk Reduction/Mitigation Process

The fourth option to consider in responding to risk is to reduce the risk through the use of new or enhanced controls. The controls should reduce the risk to an acceptable level.

Once management has been provided with the Risk Assessment Report, then they need to initiate the process to respond to the identified risks in the manner they feel is appropriate, depending on their tolerance for risk.

The first step in risk response is to determine the owner of the risk. Is this a risk in a business process? A risk in IT operations? The owner of the risk will be responsible for ensuring that the appropriate risk response decision is made and, if necessary, overseeing the deployment of the risk mitigation activities.

The risks in the Risk Assessment Report should be prioritized according to their severity. Some risks may need immediate attention whereas others may be able to wait to be addressed in the future. The organization's decision makers may wish to review the justification for the recommendations made in the Risk Assessment Report. They may also want to confirm the effectiveness of the existing controls and review ongoing projects or major changes that may be pending in business operations. It may be that existing controls are adequate, or that there are compensating controls in place that would effectively stop an attack. A major change in business practices or the pending deployment of a new business process or technology may make it infeasible to address a risk to a process that is about to be replaced anyway. In this case, the business will usually accept the risk and increase the monitoring of the risk, pending the rollout of the new business process.

Risk Acceptance

Risk acceptance is the decision by the business to take no (further) action in regard to an identified risk. This decision may be based on cost—the cost of further controls would outweigh the benefits of the controls—or on the calculation that the level of risk is within acceptable limits, and the business is willing to accept the cost of the event should it occur.

The challenge with risk acceptance is whether the calculations of cost are accurate. It could be that the organization has accepted a risk of a certain declared value, but if that event ever happened, it is discovered that the real cost is far in excess of the original expectation.

The end goal of risk management is to reach the point where all risk to the organization is at a level that is communicated and accepted by its decision makers.

Residual risk can also be accepted by an organization. A risk acceptance strategy indicates that an organization is willing to accept the risk associated with the potential occurrence of a specific event.

It is important that when an organization chooses risk acceptance, it clearly understands the risk that is present, the probability that the loss related to the risk will occur, and the cost that would be incurred if the loss were realized. Organizations may determine that risk acceptance is appropriate when the cost of implementing controls exceeds the anticipated losses.

Share/Transfer Risk

If the level of risk to the organization exceeds an acceptable level, managers may decide to transfer the risk to another organization—for example, through the purchase of insurance. Another situation is where a business is working on a large project that may exceed the capabilities of the organization. In that case, the business may partner with other organizations that can provide the necessary skills or support to meet the project requirements. This means that both the risk and the profit are shared by the partnering organizations.

Residual Risk

Total Risk – Control Effectiveness = Residual Risk

The challenge with calculating residual risk lies in determining how effective a control will be. Some controls are 100% effective, such as applying a patch to a vulnerability. If the patch works, it will stop an exploit of that vulnerability (but of course we all know that some patches don't work). Other controls, such as a firewall, are partially effective. They will block some attacks but may miss others. A fire extinguisher is also partially effective in that it puts the fire out, but undoubtedly there is still some damage from both the fire and the residual suppressant from the extinguisher.

As we saw before, a control will usually reduce either the likelihood of an adverse incident or the impact of the incident. This leaves us with a level of residual risk. Our objective is to ensure that all organizational IT-related risk is within the limits accepted by the organization's decision makers. Therefore, our risk remediation objective is to reduce risk that is unacceptably high to a level that is equal to, or less than, the level of acceptable risk.

Residual risk is the measure of the level of risk that remains after the implementation of the controls (the risk response). Residual risk may not be exactly the same as acceptable risk since residual is the level of risk that does remain and acceptable is the theoretical level that would be accepted by management.

Activity: Risk Treatment

INSTRUCTIONS

Answer each of the following questions.

1. What risk treatment strategies are available?
2. What is risk mitigation?
3. How do we avoid risk?
4. If we transfer risk, who is responsible if something goes wrong?

Activity Answers: Risk Treatment

Answers

1. What risk treatment strategies are available?

   Remove, reduce, transfer, accept.

2. What is risk mitigation?

   The introduction of safeguards or countermeasures to reduce the exposure to or effect of an identified risk.

3. How do we avoid risk?

   Stop doing whatever it is that you are doing. For example, if doing business in the UK exposes the organization to an unacceptable level of risk, then don't do business in the UK

4. If we transfer risk, who is responsible if something goes wrong?

   Whoever transferred the risk. You can transfer the role but never the responsibility. You (the business) decided on the action therefore you are responsible for the action.