The Information Systems Audit

INFO 6008 NEW Week 6

FANSHAWE

Governance and Management of IT

- **We are covering the following topics:**
- **The IT Steering Committee:** This section defines the role and importance of the IT steering committee in corporate governance.
- **Corporate Structure:** This section defines the most common types of corporate structures in business today.
- **IT Governance Frameworks:** This section explains common IT governance frameworks and their roles in governance.
- **Enterprise Risk Management:** This section details common techniques for enterprise risk management.
-

Governance and Management of IT

- **We are covering the following topics:**
- **Policy Development:** This section provides an overview of policy development approaches and related implementation strategies.
- **Management Practices of Employees:** This section describes common policies and controls related to how people are hired, promoted, retained, and terminated.
- **Performance Management:** This section reviews methods to measure performance to ensure that the organization's goals are consistently being met in an effective and efficient manner.
-

Governance and Management of IT

- **Management and Control Frameworks:** This section reviews how a control framework categorizes and aligns an organization's internal controls to identify and manage risk in the most optimal manner.
- **Maturity Models:** This section reviews the basics of maturity models and how maturity levels are measured against controls and processes.
- **Management's Role in Compliance:** This section defines management's role in driving adoption of policies to ensure compliance.
-

Governance and Management of IT

- **Process Optimization Techniques:** This section describes various techniques and methods to optimize processes.
- **Management of IT Suppliers:** This section reviews key controls related to the support and management of an IT supplier, IT vendor, or IT third-party provider.

Governance and Management of IT

- IT governance is a subset of corporate governance that focuses on the belief that the managers, directors, and others in charge of an organization must establish key roles and responsibilities to control IT risks.
- Management must implement rules and policies to control the IT infrastructure and develop practices to distribute responsibilities. Not only does this prevent a single person or department from shouldering responsibility, it also sets up a framework of control.

Governance and Management of IT

- The growing need for IT governance tools and techniques was fueled by the following factors:
- Growing complexity of IT environments
- Fragmented or poorly performing IT infrastructures
- User frustration leading to ad hoc solutions
- IT costs perceived to be out of control
- IT managers operating in a reactive, rather than proactive, manner
- Communication gaps between business and IT managers
- Volatile organizational, political, or economic environment

Governance and Management of IT

- The growing need for IT governance tools and techniques was fueled by the following factors:
- Increasing pressure to leverage technology in business strategies
- Need to comply with increasing laws, standards, and regulations
- Scarcity of skilled staff
- Lack of application ownership
- Resource conflicts/shifting priorities
- Impaired organizational flexibility and nimbleness to change
- Concern for risk exposures

Governance and Management of IT

- IT governance is established by creating an IT strategy committee, developing policies and procedures, defining job roles, executing good HR practices, and performing risk assessments and periodic audits.

THE IT STEERING COMMITTEE

- IT governance is established by creating an IT strategy committee, developing policies and procedures, defining job roles, executing good HR practices, and performing risk assessments and periodic audits.
- An IT steering committee, which also may be referred to as an IT strategy committee, is tasked with ensuring that the IT department's goals are properly aligned with the goals of the business.
- This is accomplished by using the committee as a conduit to move information and objectives back and forth between senior business management and IT management.

THE IT STEERING COMMITTEE

- The exact makeup of the IT steering committee will vary by organization based on size, industry, regulatory mandates, and leadership strength. In general, the IT steering committee needs to be made up of senior leaders from IT, corporate functions, and lines of business. The following are typical IT steering committee members:

Take a Guess?

THE IT STEERING COMMITTEE

- **Business management**: The committee is managed by the chief executive officer (CEO) or by another person who is appointed, such as the chief information officer (CIO).
- **IT management**: IT management is represented by the CIO or a CIO representative.
- **Legal**: The legal group is represented by an executive from the legal department.
- **Finance**: A representative from finance is needed to provide financial guidance.

THE IT STEERING COMMITTEE

- **Marketing**: A representative from marketing should also be on the committee.
- **Sales**: A senior manager for sales should be on the committee to make sure the organization has the technology needed to convert shoppers into buyers.
- **Quality control**: Quality control ensures that consumers view products and services favorably and that products meet required standards. Therefore, quality control should be represented on the committee.

THE IT STEERING COMMITTEE

- **Research and development (R&D)**: Because R&D focuses on developing new products, this department should be represented on the committee. IT must meet the needs of new product development.
- **Human resources (HR)**: Managing employees is as complex as the technology needed to be successful. HR should be represented on the committee.

THE IT STEERING COMMITTEE

- **Research and development (R&D)**: Because R&D focuses on developing new products, this department should be represented on the committee. IT must meet the needs of new product development.
- **Human resources (HR)**: Managing employees is as complex as the technology needed to be successful. HR should be represented on the committee.

THE IT STEERING COMMITTEE

- The IT steering committee does not typically consist of technologists such as the chief technology officer (CTO) because this is primarily viewed as a business committee. The chief information officer (CIO) typically is a member and acts as the bridge between the IT steering committee and the technology department.
- The IT steering meeting provides an opportunity for exchange of views where the business communicates its business goals and IT discusses how it can align and enable the business' goals through the use of technology.
- Often this includes IT leadership educating the business on the limits and risks of technology.

THE IT STEERING COMMITTEE

- Once an understanding is reached between the business and IT leadership on goals, the CTO and other technologies engage in implementation planning.
- Although membership might vary, the goal of the committee should be consistent.
- The committee is also responsible for reviewing major IT projects, budgets, and plans.
- The duties and responsibilities of the IT steering committee should be defined in a **formal charter**.

THE IT STEERING COMMITTEE

- If an organization lacks a charter or doesn’t have a steering committee, this should be a clear warning that IT and the business may not be closely aligned.
- Although the charter gives the committee the power to provide strategic guidance, the IT steering committee should not be involved in the day-to-day activities of the IT department.

THE IT STEERING COMMITTEE

- If there is evidence that the IT steering committee is involved in day to day activities – this should alert the auditors that the committee has strayed from its charter or that the charter is not clear on the committee's responsibilities.
- A steering committee is one of three items needed to build a framework of success. The other two are:

1. performance measurement
2. risk management.

THE IT STEERING COMMITTEE

- If there is evidence that the IT steering committee is involved in day to day activities – this should alert the auditors that the committee has strayed from its charter or that the charter is not clear on the committee's responsibilities.
- A steering committee is one of three items needed to build a framework of success. The other two are:

1. performance measurement
2. risk management.

THE IT STEERING COMMITTEE

- The IT steering committee is a good place to start understanding the separation between governance and management.
- Senior management's role in the IT steering committee process is at a strategic level, not a tactical one.
- Consider eBay, for example. While eBay's senior management should be concerned about merchandise being listed for the duration of an auction and about bidding and closing occurring seamlessly, they should have little concern about the operating system and platform.

THE IT STEERING COMMITTEE

- As long as the technology can meet the stated business goal and budget constraints, the choice of Windows, Linux, or UNIX should be left up to the IT department.
- Senior management’s goal is to ensure that goals are aligned, IT is tasked with meeting those business needs, and the auditor is responsible for ensuring that controls are present and operating effectively.

CORPORATE STRUCTURE

- Senior management must select a strategy to determine who will pay for the information systems services.
- Funding is an important topic because departments must have adequate funds to operate. Each funding option has advantages and disadvantages. These are the three most common funding options:
- Shared Cost
- Chargeback
- Sponsor pays

CORPORATE STRUCTURE

- **Shared cost**: With this method, all departments in the organization share the cost. The advantage of this method is that it is relatively easy to implement and for accounting to handle. Its disadvantage is that some departments might feel that they are paying for something they do not use.
- **Chargeback**: With this method, individual departments are directly charged for the services they use. This is a type of pay-as-you-go system. Those opposing the chargeback system believe that it is not so clear-cut as end users don’t consume IT resources evenly.
-

CORPORATE STRUCTURE

- **Sponsor pays**: With this method, project sponsors pay all costs. Therefore, if sales asks for a new system to be implemented, sales is responsible for paying the bills. Although this gives the sponsor more control over the project, it might lead to the feeling that some departments are getting a free ride, which can cause conflicts.

IT GOVERNANCE FRAMEWORKS

- IT governance frameworks offer blueprints for achieving the key organizational objectives set by the IT steering committee, including meeting compliance and cybersecurity expectations.
- These frameworks represent best practices as techniques and approaches that have been proven to provide consistent desired outcomes. IT governance best practices require the organization to meet specific goals:

IT GOVERNANCE FRAMEWORKS

- **Align the goals of IT to the goals of the organization:** Both must be focused on and working for the common goal.
- **Establish accountability:** Accountability requires that individuals be held responsible for their actions. Accountability can be seen as a pyramid of responsibility that starts with the lowest level of employees and builds up to top management.
- **Define supporting policies and processes:** It is important to establish the rules of the road and expected behavior.

IT GOVERNANCE FRAMEWORKS

- Not all IT governance frameworks are created equal.
- Each IT governance framework was designed to meet a specific industry or regulatory guidance need.
- While many frameworks overlap to some degree, they are also often complementary, building on the strengths and weaknesses of others.
- Because of this natural synergy, many organizations adopt multiple governance frameworks.
- Let’s examine this synergy by examining COBIT and ITIL.

IT GOVERNANCE FRAMEWORKS: COBIT

- Control Objectives for Information and Related Technologies (COBIT) is used to ensure quality, control, and reliability of information systems by establishing IT governance and management structure and objectives.
- COBIT promotes goals alignment, better collaboration, and agility, and as a result, it reduces IT risks.
- COBIT essentially defines *what* is needed to achieve the organization's goals and defines the high-level organizational structure and control requirements needed to reduce IT risks.

IT GOVERNANCE FRAMEWORKS

- COBIT 5 is the newest version of COBIT, released in 2012. It outlines five core governance principles:
- **1.** Meeting stakeholder needs
- **2.** Covering the enterprise end to end
- **3.** Applying a single integrated framework
- **4.** Enabling a holistic approach
- **5.** Separating governance from management

IT GOVERNANCE FRAMEWORKS

- COBIT 5 describes these principles in terms of enabler requirements that support an enterprise in meeting stakeholder needs related to the use of IT assets and resources across the enterprise.
- There is a significant emphasis on governance, responsibilities, and accountability. COBIT requires management to understand and manage the business risk.

IT GOVERNANCE FRAMEWORKS

- There are two types of processes in COBIT 5:

1. governance processes (evaluate, direct, and monitor)
2. management processes (plan, build, run, and monitor).

- COBIT 5 is a broad framework that can be applied to any industry to organizations of all sizes.

IT GOVERNANCE FRAMEWORKS

- There are two types of processes in COBIT 5:

1. governance processes (evaluate, direct, and monitor)
2. management processes (plan, build, run, and monitor).

- COBIT 5 is a broad framework that can be applied to any industry to organizations of all sizes.

IT GOVERNANCE FRAMEWORKS - ITIL

- Information Technology Infrastructure Library (ITIL) is a series of documents that define how to execute IT service management (ITSM) processes.
- In short, ITSM is the alignment of enterprise IT services and information systems against the IT steering committee goals and broad organizational principles such as those set by COBIT.
- ITSM defines how to deliver value to the business and customer, and how to manage the underlying technology.

IT GOVERNANCE FRAMEWORKS - ITIL

- ITIL essentially defines *how* to achieve the organization's goals and defines the low-level organizational structure and process requirements needed to reduce IT risks.
- ITIL provides a set of interrelated best practices that provide detailed guidance for developing, delivering, and managing enterprise IT services. There are five stages in the ITIL service life cycle:

IT GOVERNANCE FRAMEWORKS - ITIL

- **1.** Service strategy
- **2.** Service design
- **3.** Service transition
- **4.** Service operation
- **5.** Continual service improvement

IT GOVERNANCE FRAMEWORKS – COBIT VS ITIL

- Broadly COBIT provides the “what” on governance objectives that must be achieved, and ITIL provides the detail on “how” to achieve the objectives. This is, of course, an oversimplification, but suffices for this stage.
- Think of COBIT as defining the coaching staff for an NFL team. In this analogy, COBIT would define the need for an offensive coordinator and a defensive coordinator. COBIT would define their roles and accountabilities, what type of records they should keep, how often the player health should be checked, and so on.
- What’s missing?

IT GOVERNANCE FRAMEWORKS – COBIT VS ITIL

- The plays - the specific drill routines and much more.
- COBIT talks about the running of the team, ITIL talks about all the details of how to win each game.
- The NFL team analogy illustrates the synergy between the frameworks; without both a well-run team and effective execution on the field, the team cannot win games.

IT GOVERNANCE FRAMEWORKS – COBIT VS ITIL

- Governance frameworks can and do overlap. Typically, they overlap in how they define certain functions or placement of those functions within an organization.
- For example, ITIL calls out IT risk management as a unique topic and chooses to integrate the practice across its services.
- COBIT calls out both IT risk management as a topic with separate and unique process requirements for its management.
- While accommodation may be needed so they coexist, in the end they are complementary.

IT GOVERNANCE FRAMEWORKS – COBIT VS ITIL

- Ultimately, IT governance frameworks are often adjusted to accommodate the organizational, industry, and technology environment in which they are to be implemented. These accommodations make each IT governance framework implementation unique.
- While auditors may have a firm grasp on any framework at an academic level, they need to understand the accommodations made before they can effectively audit the environment.
- The following is a high-level list of what an auditor needs to consider as part of an IT governance framework audit:

NIST CYBER SECURITY FRAMEWORK

- In February 2013, President Obama issued Presidential Executive Order 13636, “Improving Critical Infrastructure Cybersecurity.” The goal was to develop a new framework to reduce cyber risks to critical infrastructure.
- For a year, the NIST conducted workshops to gather inputs from experts across the country. Through this collaborative approach between government, industry, and academia, NIST published the Cyber Security Framework (CSF) in February 2014.
- NIST continued to gather feedback and recommendations for improvement on the framework and published an updated version of the CSF in April 2018.

NIST CYBER SECURITY FRAMEWORK

- CSF 800-53 Version 1.1 is completely compatible with the original version.
- Most of the changes were refinements and clarifications to the existing information, although one new category focused on supply chain risk was introduced and ten additional subcategories were added.
- The NIST CSF is a voluntary framework that incorporates existing standards, guidelines, and industry practices.
- The framework is industry agnostic. By leveraging existing approaches and solutions, the CSF is flexible enough to be used by any company looking to develop a cost-effective approach to manage and reduce cybersecurity-related risks. One of the key strengths of the framework is that it shifts the primary focus to risk-based outcomes rather than simply focusing on a list of controls.

NIST CYBER SECURITY FRAMEWORK

- The NIST CSF is composed of three main components: the core, implementation tiers, and profiles.
- The core represents a cybersecurity life cycle that describes a list of desired outcomes with a comprehensive list of cybersecurity activities that includes multiple references.
- Implementation tiers provide insight into how well the organization is managing their overall cyber risk in the context of the framework. The profile captures the organization’s desired outcome based upon their current state, specific business needs, and risk posture.
- The core makes up the bulk of the NIST CSF and is composed of functions, categories, subcategories, and references.

NIST CYBER SECURITY FRAMEWORK

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

NIST CYBER SECURITY FRAMEWORK

At the top level, the core is broken down into the following five major functions:

- Identify
- Identify and prioritize risks to key assets, information, and processes.
- Protect
- Implement appropriate safeguards to protect those assets, information, and processes, thereby limiting the impact of cybersecurity events.
- Detect
- Deploy measures to detect suspicious and malicious activities.
- Respond
- Develop capabilities to properly respond to events.
- Recover
- Ensure you can recover operations and services after an event.
- .

NIST CYBER SECURITY FRAMEWORK

- In order to get a sense of how well you are embodying the characteristics of the framework, you need to determine which tier best describes your organizational risk management posture.
- The NIST CSF tiers provide insight into how the organization is managing risk along a four-level, hierarchical scale:
- Tier 1 – Partial

The organization is managing risk in an informal, ad hoc, and reactive manner. There is limited awareness of cybersecurity risk.

- Tier 2 – Risk Informed

Risk management practices exist in silos across the organization. Cybersecurity activities are prioritized, leveraging threat information and business needs, but the approach is more tactical in nature.•

NIST CYBER SECURITY FRAMEWORK

- Tier 3 – Repeatable

A formal, comprehensive risk management program exists with well-defined cybersecurity policies, procedures, and metrics, along with routine reviews to adjust where necessary.

- Tier 4 – Adaptable

The risk management program is regularly updated based on lessons learned and other analytics to optimize organizational performance, reduce risk, and lessen the impact of incidents. Information is routinely shared with outside entities. Cybersecurity and risk management are part of the organizational culture.

NIST CYBER SECURITY FRAMEWORK

- Progression to higher tiers is encouraged and desirable commensurate with the business needs, risk appetite, and availability of resources of the organization.
- Every organization does not need to achieve a tier 4 status. While this tier structure sounds very similar to the Capability Maturity Model (CMM), it does not represent an actual maturity score.
- This qualification is understandable, since the categories and subcategories are not control-based objectives.
- Plus, organizations must tailor their adoption of the framework to their specific business needs, resources, risk tolerance, and regulatory commitments.
- There is no one-size-fits-all or ideal implementation of the framework.

NIST CYBER SECURITY FRAMEWORK

- Still, the tier levels sound very similar to a maturity model or similar scoring mechanism, so this often leads to confusion and frustration. It is understandable that organizations want a way to systematically and concretely measure their conformance to the standard, but for now, the tier designation is the closest solution available today. Some security vendors have created their own method for generating a maturity score aligned to the framework, but they are not officially part of the standard itself.
- Profiles are a way to optimize and fit the framework to your organization. This step is crucial to align the categories and subcategories of each function to the unique business requirements and goals of the organization. Go through each category and subcategory of the framework to assess your cybersecurity posture, and determine which tier best represents your current state.

NIST CYBER SECURITY FRAMEWORK

- Once you have a solid understanding of your current NIST CSF profile, you can conduct a similar exercise to determine your desired future state both in the short term (6 to 18 months) or long term (18 to 36 months). The cybersecurity industry and threat landscape are too dynamic to realistically predict accurate roadmaps longer than three years.
- This sets the stage for developing an action plan to prioritize cybersecurity activities and investments. Your goal is to achieve your desired profile, not necessarily a specific tier-level determination.
- Another use for profiles is to provide a benchmark with other organizations and use this comparison data to further justify your cybersecurity strategy.
- A word of advice: Document your assumptions and evaluation criteria so you can articulate how you arrived at your conclusions.

NIST CYBER SECURITY FRAMEWORK

- It will be difficult to remember all the conversations and decisions made during the assessment process months after the effort is complete. This will be helpful to ensure consistency when conducting future framework alignment assessments.
- It will also be necessary to explain your approach should you wish to benchmark your profiles with other organizations.
- The beauty of the framework lies in its simplicity and use of common terminology that is easier for non-security professionals to comprehend. The informative reference feature makes the NIST CSF powerful and flexible.

NIST CYBER SECURITY FRAMEWORK

- If a company has already adopted the COBIT 5 framework, for example, it is simple to map what they have done to the various elements of the NIST CSF. The NIST CSF provides many benefits:
- Offers a repeatable, measurable, risk-based approach to developing and managing a cybersecurity program.
- Contains a comprehensive list of cybersecurity activities that can be performed to meet the unique needs of an organization. It is an excellent reference of cybersecurity standards, frameworks, and guidelines.
- Simplifies the prioritization of investments to maximize the return on cybersecurity investments.
- Provides a common language using an easy-to-understand taxonomy for communicating cybersecurity risk management to nonsecurity professionals.

NIST CYBER SECURITY FRAMEWORK

- Lends itself to benchmarking the current and desired cybersecurity posture between peers.
- Complements current regulations and standards like NIST 800-53, HIPAA, and PCI.
- The flexible nature of the framework and its shift away from a control-focused viewpoint also make it more difficult to adopt. The NIST CSF is not without a few challenges:
- First, it is voluntary. Therefore, organizations may not feel the need to adopt a new framework, especially if they already have a methodology in place.
- Due to its broad, comprehensive nature, many decisions are open to interpretation, which can lead organizations to overestimate the effectiveness of their controls.

NIST CYBER SECURITY FRAMEWORK

- The downside to its flexibility is that it is not as prescriptive as some organizations need to get started. It can be challenging to determine “how do I get there from here?”
- The tiers (partial, risk informed, repeatable, adaptive) provide insight into the level of control contained within the organization, but it is not a true maturity assessment.
- The NIST CSF, like many other frameworks, does a nice job of laying out and grouping the foundational elements of a cybersecurity program into an easy-to-consume format.
- The structure of the core provides an organized collection of business-focused outcomes. The tiers provide risk management context around the adoption of the framework.

NIST CYBER SECURITY FRAMEWORK

- The profiles offer a way to capture current state and future state, which promotes better prioritization of cybersecurity recommendations.
- These recommendations are not a random selection of control objectives. Instead, they are aligned with business needs, sized according to the available resources, tailored to the organizational risk appetite, and customized to meet legal and industry obligations.
- By mapping informative references to existing standards, guidelines, and industry practices, companies can leverage past investments and adopt the NIST CSF with little rework.

IT GOVERNANCE FRAMEWORKS – COBIT VS ITIL

- Familiarize yourself with the implemented frameworks.
- Understand the business goals and objectives from the IT steering committee.
- Focus on the strengths and weaknesses of each of the applicable frameworks to ensure coverage of goals and business objectives.
- Ensure that accommodations between frameworks have not resulted in conflicting definition or redundant processes.
- Ensure that measurement systems are complementary.

ENTERPRISE RISK MANAGEMENT

- The goal of enterprise risk management (ERM) is to provide key stakeholders with a substantiated and consistent opinion of risk across the enterprise.
- ERM provides leadership with confidence that both individual risk events and the enterprise's aggregated risk are being effectively managed.
- The first step in the risk management process is to identify and classify the organization's assets.
- Information and systems must be assessed to determine their worth.

ENTERPRISE RISK MANAGEMENT

- When asset identification and valuation are complete, the organization can start the risk-identification process to identify potential risks and threats to the organization's assets.
- A risk management team is tasked with identifying these threats. The team can then examine the impact of the identified threats. This process can be based on real monetary amounts or a reasonable estimate based on experience.
- We have discussed types of threats and how to manage the associated risks in week 3 and we covered the different types of risk: inherent, control, detection, and residual.

ENTERPRISE RISK MANAGEMENT

- We also looked at the fact that, how the risk management team can move on to the risk mitigation or risk disposition phase.

Recall risk can be disposed of in the following ways:

- Avoiding risk
- Reducing risk
- Accepting risk
- Transferring risk

ENTERPRISE RISK MANAGEMENT

- The same tools and methods discussed in week 3 also apply to ERM.
- The difference is that ERM applies these tools to the entire end-to-end population of risk.
- For example, consider weather forecasting. Every day we can use tools to measure the weather. But there is also value in looking at the pattern of weather for the month, year, decade, and century.
- ERM is the processes that take the aggregate view of risk.

The Risk Management Team

- The risk management team is tasked with identifying and analyzing risks.
- Its members should be assembled from across the company and most likely will include managers, IT employees, auditors, programmers, and security professionals.
- Having a cross-section of employees from across the company ensures that the team can address the many threats it must examine.

The Risk Management Team

- Teams of specialists may be formed to address emerging or high-profile risks.
- These teams are not created in a void but are developed within a risk management program with a purpose.
- For example, a program might be developed to look at ways to decrease insurance costs, reduce attacks against the company's website, or verify compliance with privacy laws.

The Risk Management Team

- After the purpose of the team is established, the team can be assigned responsibility for developing, modifying, and/or implementing a more comprehensive risk management program.
- This is a huge responsibility because it requires not only identification of risk but also implementation of the team's recommendations.

Asset Identification

- At the center of most ERM processes is a comprehensive list of assets.
- Asset identification is the task of identifying all the organization's assets, which can be both tangible and intangible. The following assets are commonly examined:
- Hardware
- Software
- Employees
- Services
- Reputation
- Documentation

Asset Identification

When looking at an asset, the team must first think about the replacement cost of the item before assigning its value.

The team should consider the value brought by an asset more than just the cost to create or purchase it. These considerations are key:

- What did the asset cost to acquire or create?
- What is the liability if the asset is compromised?
- What is the production cost if the asset is made unavailable?
- What is the value of the asset to competitors and foreign governments?
- How critical is the asset, and how would its loss affect the company?

Threat Identification

- The risk management team can gather input from a range of sources to help identify threats. These individuals or sources should be consulted or considered to help identify current and emerging threats:
- Business owners and senior managers
- Legal counsel
- HR representatives
- IS auditors
- Network administrators
- Security administrators
- Operations
- Facility records
- Government records and watchdog groups, such as CERT

Threat Identification

- A *threat* is any circumstance or event that has the potential to negatively impact an asset by means of unauthorized access, destruction, disclosure, or modification.
- Identifying all potential threats is a huge responsibility.
- A somewhat easier approach is to categorize the common types of threats:
- Physical threat/theft
- Human error
- Application error/buffer overflow
- Equipment malfunction
- Environmental hazards
- Malicious software/covert channels

Threat Identification

- A threat coupled with a vulnerability can lead to **a loss.**
- *Vulnerabilities* are flaws or weaknesses in security systems, software, or procedures.
- An example of a vulnerability is human error. This vulnerability might lead an improperly trained help desk employee to unknowingly give a password to a potential hacker, resulting in a loss.
- Examples of losses or impacts include the following:
- Financial loss
- Loss of reputation
- Danger or injury to staff, clients, or customers
- Loss of business opportunity
- Breach of confidence or violation of law

Threat Identification

- Losses can be immediate or delayed. A delayed loss is not immediate; it has a negative effect on the organization after some period of time—in a few days, months, or years.
- For example, an organization could have its website hacked and thus suffer an immediate loss. No e-commerce transactions occur, technical support has to be brought in to rebuild the web server, and normal processing halts. All these are immediate losses.
- Later, when the local news channel reports that the company was hacked and that personal information was lost, the company loses the goodwill of its customers. Some might remember this event for years to come and choose to use a competitor. This is a delayed loss.
- Thus far, we have discussed building a risk management team that has the support of senior management, identifying tangible and nontangible assets, and performing threat identification.

Quantitative Risk Assessment

- Performing a quantitative risk assessment involves quantifying all elements of the process: including asset value, impact, threat frequency, safeguard effectiveness, safeguard costs, uncertainty, and probability. This involves six basic steps:

1. Determine the asset value (AV) for each information asset.

2. Identify threats to the asset.

3. Determine the exposure factor (EF) for each information asset in relation to each threat.

4. Calculate the single loss expectancy (SLE).

5. Calculate the annualized rate of occurrence (ARO).

6. Calculate the annualized loss expectancy (ALE).

Quantitative Risk Assessment

- The **advantage** of a quantitative risk assessment is that it assigns monetary values, which are easy for management to work with and understand.
- **A disadvantage** of a quantitative risk assessment is that it is also based on monetary amounts.
- Consider that it's difficult, if not impossible, to assign monetary values to all elements. Therefore, some qualitative measures must be applied to quantitative elements.
- Even then, this is a huge responsibility; therefore, a quantitative assessment is usually performed with the help of automated software tools.

Quantitative Risk Assessment

- If asset values have been determined as previously discussed and threats have been identified, the next steps in the process for quantitative risk assessment are as follows:

1. Determine the exposure factor:

This is a subjective potential percentage of loss to a specific asset if a specific threat is realized.

This is usually in the form of a percentage, similar to how weather reports predict the likelihood of rainy conditions.

Quantitative Risk Assessment

2. Calculate the single loss expectancy (SLE):

The SLE value is a monetary figure that represents the organization's loss from a single loss or the loss of this particular information asset. SLE is calculated as follows:

- Single loss expectancy = Asset value × Exposure factor
- Items to consider when calculating SLE include:
- the physical destruction or theft of assets, loss of data, theft of information, and threats that might delay processing.

Quantitative Risk Assessment

- **3. Assign a value for the annualized rate of occurrence (ARO):**
- The ARO represents the estimated frequency at which a given threat is expected to occur.
- Simply stated, how many times is this expected to happen in one year?

Quantitative Risk Assessment

- **4. Assign a value for the annualized loss expectancy (ALE):**
- The ALE is an annual expected financial loss to an organization's information asset because of a particular threat occurring within that same calendar year. ALE is calculated as follows:

Annualized loss expectancy (ALE) =

Single loss expectancy (SLE) × Annualized rate of occurrence (ARO)

ALE = SLE * ARO

The ALE is typically the value that senior management needs to assess to prioritize resources and determine what threats should receive the most attention.

Quantitative Risk Assessment

- **4. Assign a value for the annualized loss expectancy (ALE):**
- The ALE is an annual expected financial loss to an organization's information asset because of a particular threat occurring within that same calendar year. ALE is calculated as follows:

Annualized loss expectancy (ALE) =

Single loss expectancy (SLE) × Annualized rate of occurrence (ARO)

ALE = SLE * ARO

The ALE is typically the value that senior management needs to assess to prioritize resources and determine what threats should receive the most attention.

Quantitative Risk Assessment

- **5. Analyze the risk to the organization:**
- The final step is to evaluate the data and decide whether to accept, reduce, or transfer the risk.
- Much of the process of quantitative risk assessment is built on determining the exposure factor and the annualized loss expectancy, which rely heavily on probability and expectancy.

Quantitative Risk Assessment

- When looking at events such as storms or other natural phenomena, it can be difficult to predict their actual behavior. Yet over time, a trend can be established.
- These events can be considered stochastic. A *stochastic* event is based on random behavior because the occurrence of individual events cannot be predicted, yet measuring the distribution of all observations usually follows a predictable pattern.
- In the end, however, quantitative risk management faces challenges when estimating risk, and it must therefore rely on some elements of the qualitative approach.

Quantitative Risk Assessment

- Another item that is sometimes overlooked in quantitative risk assessment is the total cost of a loss. The team should review these items as it's assessing costs:
- Lost productivity
- Cost of repair
- Value of the damaged equipment or lost data
- Cost to replace the equipment or reload the data
- When these costs are accumulated and specific threats are determined, the true picture of annualized loss expectancy can be assessed. Now the team can build a complete picture of the organization's risks. The following table shows sample results.
-

Quantitative Risk Assessment

Asset	Risk	Asset Value	EF	SLE	Annualized Frequency	ALE
Customer database	Loss of consumer data due to lack of a backup	$126,000	78.06%	$93,355	.25	$24,588
E-commerce website	Hacked	$35,500	35.50%	$12,603	.45	$5,671
Domain controller	Power supply failure	$18,000	27.27%	$4,907	.25	$1,227

Quantitative Risk Assessment

- Although automated tools are available to minimize the effort of the manual process, these programs should not become a crutch to prevent businesses from using common sense or practicing due diligence.
- Care should also be taken when examining high-impact events, even for the probability. Many of us witnessed the 100-year storm that would supposedly never occur in our lifetime and that hit the Gulf coast and severely damaged the city of New Orleans.
- Organizations must be realistic when examining such potential events and must openly discuss how such a situation should be dealt with. Just because an event is rated as a one-in-100-year probability does not mean that it can’t happen again next year.
- .

Qualitative Risk Assessment

- A qualitative assessment is scenario driven and does not attempt to assign monetary values to components of the risk analysis.
- A qualitative assessment ranks the seriousness of threats and sensitivity of assets by grade or class, such as low, medium, or high. You can see an example of this in NIST 800-26, a document that uses confidentiality, integrity, and availability as categories for a loss.
- It then rates each loss according to a scale of low, medium, or high. The example table shows an example of how this process is performed. A rating of low, medium, or high is subjective. In this example, the following categories are defined:
-

Qualitative Risk Assessment

- **Low**: Minor inconvenience; can be tolerated for a short period of time but will not result in financial loss
- **Medium**: Can result in damage to the organization, cost a moderate amount of money to repair, and result in negative publicity
- **High**: Will result in a loss of goodwill between the company and a client or an employee; may result in a large legal action or fine; and may cause the company to significantly lose revenue or earnings

Qualitative Risk Assessment

Asset	Loss of Confidentiality	Loss of Integrity	Loss of Availability
Customer credit card and billing information	High	High	Medium
Production documentation	Medium	Medium	Low
Advertising and marketing literature	Low	Low	Low
HR (employee) records	High	High	Medium

Qualitative Risk Assessment

- The disadvantage of performing a qualitative assessment is that you are not working with monetary values. This type of assessment lacks the rigor that accounting teams and management typically prefer.

Other types of qualitative assessment techniques include these:

- **The Delphi technique**: This group assessment process allows individuals to contribute anonymous opinions.
- **Facilitated Risk Assessment Process (FRAP)**: This subjective process obtains results by asking a series of questions. It places each risk into one of 26 categories. FRAP is designed to be completed in a matter of hours, making it a quick process to perform.

Qualitative Risk Assessment

- The disadvantage of performing a qualitative assessment is that you are not working with monetary values. This type of assessment lacks the rigor that accounting teams and management typically prefer.

Other types of qualitative assessment techniques include these:

- **The Delphi technique**: This group assessment process allows individuals to contribute anonymous opinions.
- **Facilitated Risk Assessment Process (FRAP)**: This subjective process obtains results by asking a series of questions. It places each risk into one of 26 categories. FRAP is designed to be completed in a matter of hours, making it a quick process to perform.

The Three Lines of Defense Model

Internal control functions are an essential part of the ERM model. It works with the idea that no process is expected to be perfect. Over time:

- technology wears out,
- processes become prone to errors,
- the rotation of personnel introduces unskilled workers.

Whatever the cause, over time, process defects begin to be introduced into products or services.

Without a cohesive and coordinated approach to managing risk, the number of defects and problems can increase.

The Three Lines of Defense Model

- The Three Lines of Defense model is one method to continually assess the environment to ensure that people, process, and technology are meeting the organization’s goals.
- The Three Lines of Defense model provides a simple and effective way to ensure that risk is identified and reported to leadership.
- This model works for all industries and organizations of all sizes.

The Three Lines of Defense Model

- The Three Lines of Defense model identifies the key roles and responsibilities for managing risk in layers.
- The idea is that while one or two layers may miss a material risk, it is highly unlikely that all three layers would miss identifying a major risk. The roles and responsibilities in this model are as follows:
- **Business unit leadership:** These business leaders have primary and ultimate accountability to ensure that appropriate management and internal controls are in place to manage risk. Key responsibilities include the following:
- Day-to-day risk management of defects and process problems
- Following policies and risk management process
- Promptly remediating and reporting risk

The Three Lines of Defense Model

- **Risk and compliance teams:** These teams vary from one organization to another and generally advise and verify that management and internal controls are working as designed.
- Compliance and operational risk teams are typical examples of this internal control function. Key responsibilities include the following:
- Advising and educating management on required controls and emerging risks
- Managing key ERM processes
- Testing to ensure that management and internal controls are working
- Reporting to senior leadership on enterprise aggregated risk

The Three Lines of Defense Model

- **Auditor:** An auditor provides the risk governance committees and senior management with comprehensive assurance that risk is being appropriately managed across the enterprise.

Key responsibilities include the following:

- Reviewing the first and second lines of defense
- Providing **an independent opinion** to senior leadership and the board of directors on the state of risk in the enterprise
- Promptly remediating and reporting risk

The Three Lines of Defense Model

- A key fact is understanding the auditor's independence in the reporting structure.
- Audit teams generally report directly to a board of directors audit committee.
- For publicly traded companies, the head of the internal audit department (sometimes referred to as the *General Auditor*) is required to meet with the full board of directors several times each year.

The Three Lines of Defense Model

- Because the audit department reports directly to the board of directors, auditors' opinions are considered **the highest level of independence and objectivity in the organization**.
- This high level of independence is not available in the second line of defense. Because the first and second lines of defense are subject to management oversight (including annual performance reviews), they cannot be considered completely independent.

The Three Lines of Defense Model

- Because the audit department reports directly to the board of directors, auditors' opinions are considered **the highest level of independence and objectivity in the organization**.
- This high level of independence is not available in the second line of defense. Because the first and second lines of defense are subject to management oversight (including annual performance reviews), they cannot be considered completely independent.

The Three Lines of Defense Model

- Auditors play a big role in the success of an organization.
- Auditors must be independent of management and have the authority to cross departmental boundaries.
- Auditors must also have the proper skills.
- If in-house individuals do not have the skills required to lead an audit, an external independent third-party auditor should be hired.

The Three Lines of Defense Model

- This situation requires careful attention. It’s natural to develop relationships with those we work with.
- Internal auditors interact extensively with their clients.
- This can lead to problems because the level of closeness between management and internal auditors might affect the results of an audit.

The Three Lines of Defense Model

- Finally, both external and internal auditors can burn out as a result of staleness and repetition, and they may thus start to lose attention to detail, which is very important.
- An auditor is expected to be free to provide guidance and recommendations to senior management.
- The objective of providing recommendations is to improve quality and effectiveness.
- The first step of this process is to review the following:

The Three Lines of Defense Model

- Finally, both external and internal auditors can burn out as a result of staleness and repetition, and they may thus start to lose attention to detail, which is very important.
- An auditor is expected to be free to provide guidance and recommendations to senior management.
- The objective of providing recommendations is to improve quality and effectiveness.
- The first step of this process is to review the following:

The Three Lines of Defense Model

- **Learn the organization:** Know the company's goals and objectives. Start by reviewing the mission statement.
- **Review the IT strategic plan:** Strategic plans provide details for the next three to five years.
- **Analyze organizational charts:** Become familiar with the roles and responsibilities of individuals in the company.
- **Study job descriptions:** Job descriptions detail the level of responsibility and accountability for employees' actions.
- **Evaluate existing policies and procedures:** These documents detail the approved activities of employees.