The Information Systems Audit

INFO 6008 Week 7

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.

POLICY DEVELOPMENT

- Policies are more than words on paper or data stored electronically. Policies reflect how management views risk.
- Policies reflect how much risk the business is willing to tolerate and reflect how leadership wants the business to run.
- For example, for a pizza shop that sells 12-inch hand-tossed pizzas, if the pizzas turn out to be between 11.5 inches and 12.5 inches, that may be well within the tolerance set by policy.
- However, for an airplane engine manufacturer, the parts design tolerance must be within 1 to 5 microns. These examples show the need to establish tolerance and the amount of risk that management is willing to accept.

POLICY DEVELOPMENT

- Policies reflect leadership perception of priorities. An auditor has two main roles related to policies:

1. ensure that a policy is complete and reasonable, given industry norms
2. identify any misalignment between stated policies and actual practice.

An auditor can learn a great deal about an organization by simply reviewing the strategic plan and examining the company's policies.

These documents reflect management's view of the company.

Policies should exist to cover almost every aspect of organizational control because companies have legal and business requirements to achieve organizational goals.

POLICY DEVELOPMENT

- Management is responsible for dividing the company into smaller subgroups so that control can be managed effectively.
- Policies will dictate how activities occur in each of the functional areas.
- One of the first steps in an audit is for the auditor to examine these critical documents.
- Any finding an auditor makes should be referenced back to the policy. This allows the auditor to specify how to rectify identified problems according to management views on risk.

POLICY DEVELOPMENT

- Management is responsible for dividing the company into smaller subgroups so that control can be managed effectively.
- Policies will dictate how activities occur in each of the functional areas.
- One of the first steps in an audit is for the auditor to examine these critical documents.
- Any finding an auditor makes should be referenced back to the policy. This allows the auditor to specify how to rectify identified problems according to management views on risk.

POLICY DEVELOPMENT

- Policies don’t last forever. Like most other things in life, they need to be reviewed periodically to make sure they stay current. Technology becomes obsolete, new technology becomes affordable, and business processes change. Although it’s sometimes easy to see that low-level procedures need to be updated, this also applies to high-level policies.
- **Policy**
- The term policy can be misleading; it can mean the policy environment, which includes standards, procedures, guidelines, and baselines.
- Or the term can refer to a specific document, which typically reflects a broad strategic view of risk taken by the highest levels of the organization.

POLICY DEVELOPMENT

- For the purpose of this discussion, we use the term *policy* to reflect the policy environment.
- Not all policies are created in the same way. The policy process can be driven from the top or from the bottom of the organization.
- *Top-down policy development* : policies are pushed down from the top of the company.
- The advantage of a top-down policy development approach is that it ensures that policy is aligned with the strategy of the company.
- The disadvantage is that it lacks speed and may not reflect a complete understanding of how detailed processes actually work.

POLICY DEVELOPMENT

- This lack of understanding of detail could lead to confusion and unrealistic expectations.
- It's a time-consuming process that requires a substantial amount of time to implement.
- A second approach is bottom-up policy development.
- *Bottom-up policy development* addresses the concerns of operational employees because it starts with their input and concerns and builds on known risk.
- This is faster than a top-down approach but has a huge disadvantage in that it risks lack of senior management support.

POLICY DEVELOPMENT

- Regardless of the development type, policies are designed to address specific concerns, including the following:
- **Regulatory:** Regulatory policies ensure that the organization's standards are in accordance with local, state, and federal laws. Industries that frequently use these documents include health care, public utilities, refining, and the federal government.
- **Advisory:** Advisory policies ensure that all employees know the consequences of certain behaviors and actions. An example of an advisory policy is one covering acceptable use of the Internet. This policy, called an acceptable use policy (AUP), might state how employees can use the Internet during the course of business; violating the policy could lead to disciplinary action or dismissal.

POLICY DEVELOPMENT

- **Informative:** Informative policies are designed not for strict enforcement but for teaching. Their goal is to inform employees and/or customers. An example of an informative policy is a return policy on goods purchased on the business's website.

Policy, Standards, Procedures, and Baselines

- *Policy* as a strategic document is one that outlines broad and strategic goals. It is typically approved by a board of directors–level committee.
- The policy document outlines accountabilities and broad risk tolerance statements in the form of a business document.
- For example, a policy document may authorize CISO to be accountable for setting and enforcing information and cybersecurity standards and procedures across the enterprise. The intent can ensure that the CISO has the authority to stop a cybersecurity attack, which may include taking some business systems offline.
- The policy may also outline the business's priority for IT, such as stating opening up of operations in Europe is a strategic goal and holding the CIO accountable to ensure that appropriate technology is in place to control the cross-border movement of data.

Policy, Standards, Procedures, and Baselines

- ***Standards*****,** in contrast to policy, describe how control should be deployed to achieve the policy and IT steering committee goals.
- Standards are much more specific than policies. A standard reflects industry-accepted norms and specifications for hardware, software, or human behavior.
- Standards should always point to the policies to which they relate.
- **Standards are often technology agnostic**.
- For example, a standard may say that “database administrators must use dual-factor authentication.” In this case, the standard does not specify which technology would be used to satisfy this requirement.

Policy, Standards, Procedures, and Baselines

- ***Procedure*** is an operational document that **lays out specific steps or processes** required to meet the requirements within the standards.
- **Procedures also identify roles and accountabilities**. To extend our dual-factor authentication example, procedures might say that to obtain a hardware token, an individual must request the device from a specific internal website and then get the device activated by the individual's manager.
- During an audit, an auditor must review all relevant procedures and map them to employee behavior through direct observation or interview.
- Misalignment can mean that there are no existing procedures, or that procedures don't map well to existing practices, or employees have not had the proper or adequate training on the procedures they are tasked with following.

Policy, Standards, Procedures, and Baselines

- ***Baselines*** *procedures* are operational documents that define the minimum configuration settings to achieve the standards requirements and support the procedure steps.
- This is the absolute minimum level that a system, network, or device must adhere to.
- To extend our dual-factor authentication example, a baseline may describe how to configure a Windows OS and Oracle database to accept only the approved hardware tokens for authentication.
- The Windows OS and Oracle database configuration setting for dual-factor authentication would be quite different, and thus two separate baselines would be created.

Policy, Standards, Procedures, and Baselines

Level/Intent	Policy	Standard	Procedure	Baselines
Strategic	✓			
Tactical		✓		
Operational			✓	✓

Auditing Policies, Standards, Procedures, and Baselines

- An audit of policies documentation can improve the quality of the control environment.
- Audits can verify that documents are being used in the way that management has authorized and intended them to be used.
- An audit can also help verify that policies are up-to-date and are adhered to.
- Per ISACA, the following items should be examined:

Auditing Policies, Standards, Procedures, and Baselines

- Human resources documents
- Quality assurance procedures
- Process and operation manuals
- Change management documentation
- IT forecasts and budgets
- Security policies and procedures
- Organizational charts and functional diagrams
- Job details and descriptions
- Steering committee reports
- Documents that deal with external entities (sometimes referred to as *third parties*) should also be reviewed.

Auditing Third Party Documentation

- A company might have contracts with vendors or suppliers for an array of products and services. How vendors are chosen, how the bidding process functions, what factors are used to determine the best bid, and what process is used to verify contract completion should all be reviewed.
- During the review process with policies, procedures, and documentation, any of the following might indicate potential problems:
- Lack of guidance on what policies are to be followed
- Excessive costs
- Budget overruns
- Late projects
- A large number of aborted projects
- Unsupported hardware changes or unauthorized purchases

Auditing Third Party Documentation

- Lack of documentation
- Out-of-date documentation
- Employees unaware of or not knowledgeable about documentation
- Policies related to external entities (that is, third parties) is a complicated topic and often a point of interest for regulators.
- Why? Because an organization is ultimately accountable for how an external entity conducts business on its behalf.
- Yet often the organization has no direct control over how the external entity operates—no direct control but ultimately accountable for someone else's actions.
- For example, assume that a company makes loans and, in the process, collects all kinds of personal and private information. The organization then hires an external entity (typically referred to as a *vendor*) to obtain a credit report on each applicant and sort the results by credit scores and demographics by region.

Auditing Third Party Documentation

- Assume there is a data breach of the external entity's computer, and someone steals all your customers' personal information.
- Who may be legally accountable for a breach at the external entity or vendor site?
- As an auditor, you would be expected to sort through the complexities and determine internal accountabilities—that is, what went wrong and why.
- **An auditor does not determine legal accountability** but can determine whether the actions taken by the organization meet the requirements and rules set by the regulators.
- Only the courts and a judge can determine legal accountability. In this example, here are a few assessment areas that may be of interest to an auditor:

Auditing Third Party Documentation

- In this example, here are a few assessment areas that may be of interest to an auditor:
- **The quality of the vendor:** How were the vendor selection and the vendor's capability assessed by the organization? Did the vendor have the resources to properly protect the organization's data? An organization should never select a vendor exclusively based on cost.
- **Expectations on the vendor:** Were expectations clearly conveyed to the vendor through contract, policies, standards, and so on? How were those expectations monitored by the organization? An organization has an obligation to monitor whether vendors are living up to their expectations. This may include onsite inspections of the vendor's facilities.

Auditing Third Party Documentation

- **Expectations on the organization:** Did the organizational policies and controls contribute to the vendor's breach?
- Let's assume that to obtain credit scores and determine demographics, the vendor needed a tax ID, name, and ZIP Code.
- Assume that the organization passes all the personal information obtained during the loan application process, such as address, salary information, mother's maiden name, and so on.
- While the organization did not contribute to the failure to protect the customer's information effectively, the organization did contribute to the impact of the breach by sending too much personal information to the vendor.

Data Classification

- Every piece of data has its own value to an organization and unique legal handling requirements.
- Most organizations have huge data stores. It’s not practical or cost-effective to examine how to handle every individual piece of data.
- Data classification is used to simplify the data handling rules by categorizing data into distinct classes.
- Then each data class (or data classification) can be subject to common rules for how the data should be treated.

Data Classification

- Most organizations prefer to use three to five data classifications.
- This way, handling rules and controls can be simplified and standardized.
- In addition, the smaller the number of data classifications, the easier it is to train personnel.
- Data and information assets are classified with respect to the risk of unauthorized disclosure, such as lost, stolen, and inadvertently disclosed.
- A simple data classification scheme is illustrated in the following table:

Data Classification

Class	Description
Public	Information released to the public Examples: press release, Dow Jones stock price
Proprietary	Information related to processes and methods that are necessary for staff to perform their work and day-today communication within the business Examples: emails, meeting minutes
Business confidential	Information critical to the business that provides a significant competitive advantage, such as trade secrets Example: secret recipe for Coca-Cola
Customer confidential	Information related to the customers of the business Examples: tax ID information, health records

Data Classification

- A data classification process typically separates information into distinct classes, which are then aligned to various standards, procedures, and baselines.
- It is also important to align these policies with regulatory requirements. For example, the Health Insurance Portability and Accountability Act (HIPAA), a U.S. law designed to provide privacy standards to protect patients' medical records, requires that patient information be stored securely.
- Electronic health records could be classified as customer confidential, and the hospital standards could require such data to be stored in encrypted form.

Data Classification

- Given the explosion of data collected, data classification has become increasingly important to managing the volume of information.
- Keep in mind the cost of classifying data. Data that is more valuable requires more controls. The more controls applied to data, the higher the cost to securely collect, store, and manage the data.
- The first step to take before classifying any information is to define the levels of classification and what controls should be applied to each classification. Consider the overall costs of the controls, based on the volume and value of data.
- Once classifications are defined, an organization faces the costs of inventorying existing data against the classification types and of implementing the supporting controls.

Data Classification

- Automation can help. Data loss prevention (DLP) technology can help automate the protection of data such as blocking any attempt to email documents labeled “business confidential.”
- Automation can be used to manage data leakage and generate reports that support these policies.
- In addition, automation can support records retention schedules by identifying the types of data specified and their location, allowing for proper archiving or destruction to occur.
- DLP systems can also be incorporated in baseline and configuration settings that block the transfer of data onto a USB drive.
- Another action could result in the system encrypting the sensitive data in such a way that only authorized users can decrypt it. The key point is that data classification is a powerful tool that can support the policies of an organization.

Data Classification

- An audit of data classification processes is important to gain an accurate view of the nature of the data, including how data is valued and types of risks perceived by leadership if that data was compromised.
- An audit can start with the existing metadata information, as well as the details of where and how the information has been stored, to give the richest possible view of the content.
- It’s important for an audit to sample data based on the metadata definitions and standards. For example, a payroll clerk might, out of convenience, create a spreadsheet to balance a department budget. If that spreadsheet is stored on the clerk’s laptop, it may be more susceptible to a data breach, which may violate the organization’s security standards.

Security Policy

- One specific type of policy is the organization's s*ecurity policy.* It dictates management's commitment to the use, operation, and security of information systems and assets.
- It specifies the role security plays in the organization. **The security policy should be driven by business objectives and should meet all applicable laws and regulations.**
- The security policy should also act as a basis to integrate security into all business functions. It serves as a high-level guide to developing lower-level documentation, such as procedures.
- The security policy must be balanced in the sense that all organizations are looking for ways to implement adequate security without hindering productivity. The issue also arises that the cost of security cannot be greater than the value of the asset.

Security Policy

- An auditor must look closely at security policies during the audit process and should review them to get a better idea of how specific access controls should function.
- Often security requirements are added to many different types of policies.
- For example, an auditor should examine policies that have been developed for disaster recovery and business continuity.
- Some questions to consider are what kind of hardware and software backup are used; whether the software backup media is stored offsite; and, if so, what kind of security the offsite location has and what type of access is available.
- These are just a few security-related items an auditor needs to review - what else?

Security Policy

- It is common to see the *principle of least privilege* in security policies.
- The idea is that you can improve security by limiting access to just the functions that are consistent with the individual's job function.
- This way, if an account is compromised, the amount of harm that can be performed is contained or limited to that job's role.
- The concept is simple, but the implementation is challenging as the size of an organization grows.
- When an organization has thousands or hundreds of thousands of accounts. The idea of going through each account one at a time and customizing security may not be practical.

Security Policy

- Grouping the accounts into roles and assigning access permissions by roles is much simpler.
- The challenge is that two users may be almost identical except in terms of a few functions that are different.
- What do you do? Create two roles with lots of duplication? Put both users in the same role, knowing they may have slightly more access than they need?
- Many organizations adopt the principle of least privilege but make compromises to balance the need to reduce access to the least amount practically possible.
- In other words, least privilege is a concept, not a hard rule.

Security Policy

- Most security policies make a distinction between privileged and non-privileged accounts.
- ***Privileged accounts*** - are administrative accounts and accounts with higher risk privileges, such as the ability to transfer money. The privileged accounts are sometimes referred to as *superusers* - if these accounts are compromised, the risk of significant impact to the organization rises.
- *Non-privileged accounts* are standard users whose access is limited under least privilege to a single job function and typically a specific set of transactions. If these accounts are compromised, the risk of significant impact to the organization is reduced compared with a privileged account.

MANAGEMENT PRACTICES OF EMPLOYEES

- Employee management practices deal with the policies and procedures that detail how people are hired, promoted, retained, and terminated.
- Employees can have a huge impact on the security of a company.
- Insiders have greater access and opportunity for misuse than outsiders typically do.
- Insiders can pose a malicious, accidental, or intentional threat to security.
- Although there is no way to predict future events, employee risks can be reduced by implementing and following good basic human resources (HR) practices.

MANAGEMENT PRACTICES OF EMPLOYEES

- Everyone wants to get the right person for the job, but good HR practices require more than just matching a resume to an open position.
- Depending on the position to be filled, company officials need to perform due diligence in verifying that they have matched the right person to the right job.
- For example, Kevin might be the best security expert around, but if it is discovered that he served a 10-year sentence for extortion and racketeering, his chances of being hired by an interested company will be slim. Some basic common controls should be used during the hiring practice:
-

MANAGEMENT PRACTICES OF EMPLOYEES

- Background checks
- Educational checks
- Reference checks
- Confidentiality agreements
- Non-compete agreements
- Conflict-of-interest agreements

MANAGEMENT PRACTICES OF EMPLOYEES

- Hiring practices should be performed with due diligence. References can be checked, education verified, military records reviewed, and even drug tests performed, if necessary. When an employee is hired, he/she brings not only his/her skills but also his/her background, history, attitude, and behavior.
- Once hired, employees should be provided with an employee handbook detailing the employee code of conduct, acceptable use of company assets, and employee responsibilities to the company. Per ISACA, the handbook should address the following issues:

MANAGEMENT PRACTICES OF EMPLOYEES

- Use of social media while at work
- Use of company-owned devices (assets and technology)
- Employee package of benefits
- Paid holiday and vacation policy
- Work schedule and overtime policy
- Moonlighting and outside employment
- Employee evaluations
- Disaster response and emergency procedures
- Disciplinary action process for noncompliance

MANAGEMENT PRACTICES OF EMPLOYEES

- Hiring is just the first step in good employee management. Employees can follow policies only if they understand them.
- Auditors should verify that HR has a written, well-defined performance evaluation process. Performance assessments should occur on a predetermined schedule and should be based on known goals and results. A fair and objective process should be used. Pay raises and bonuses should be based strictly on performance.
- Training is another area that falls under the responsibility of HR and the business unit.

MANAGEMENT PRACTICES OF EMPLOYEES

- Training can range from lunchtime programs to learning programs, multiday events, or degree programs. Common training methods include the following:
- In-house training
- Classroom training
- Vendor training
- On-the-job training
- Apprenticeship programs
- Degree programs
- Continuing education programs

Forced Vacations, Rotation of Assignments, and Dual Control

- Forcing employees to take vacations is an important control. A *forced vacation* is not something that is done strictly for the health or benefit of the employee.
- Required vacations also enable the company to ensure that someone else does the regular employee's job tasks for at least a week. This control helps verify that improper or illegal acts have not been occurring. It also makes it harder for an employee to hide any misuse.
- Another control is *rotation of assignment*, which allows more than one person to perform a specific task. This not only helps ensure a backup if an employee is unavailable but also can reduce fraud or misuse by preventing an individual from having too much control over an area.

Forced Vacations, Rotation of Assignments, and Dual Control

- *Dual control* requires two individuals to provide input or approval before a transaction or an activity can take place.
- In banking, moving large sums of money is often under dual control. For example, sending a large wire transfer from one account to another typically requires the manager and supervisor to sign off on the transaction.
- This prevents a manager from wiring herself a large sum of money and vanishing.

Separation Events

- An employee termination is often referred to as a *separation event*.
- The term *termination* has a bit of rough tone and does not fully describe why the employee is leaving; therefore, separation event has become a common term.
- A separation event could be for any reason, such as the employee finding a better job or being dismissed.
- HR typically manages the separation procedures, which should include a checklist to verify that the employee has returned all equipment that has been in his possession, including remote access tokens, keys, ID cards, cell phones, pagers, credit cards, laptops, and software.

Separation Events

- A separation event may not be voluntary, and there needs to be a process to handle the situation properly.
- The applicable policy must cover issues such as escorting the employee out of the facility, exit interviews, review of non-disclosure agreements (NDAs), and suspension of network access.

Roles and Responsibilities

- Individuals can hold any number of roles or responsibilities within an organization.
- The responsibilities each employee has and to whom he or she reports should be noted.
- An auditor’s first option for determining this information should be an organizational chart.
- After obtaining and reviewing the organizational chart, the auditor should spend some time reviewing each employee’s area to see how the job description matches actual activities. The areas to focus attention on include these:

Roles and Responsibilities

- Help desk
- End-user support manager
- Quality assurance manager
- Data manager
- Rank-and-file employees
- Systems development manager
- Software development manager

Roles and Responsibilities

- Most organizations have clearly defined controls that specify what each job role is responsible for.
- An auditor should be concerned with these common roles in the IS structure:
- **Data-entry employees:** Although most data-entry activities are now outsourced, in the not-too-distant past, these activities were performed in-house at an information processing facility (IPF). A full-time data-entry person was assigned the task of entering all data. Barcodes, scanning, and web entry forms have also reduced the demand for these services. If this role is still used, key verification is one of the primary means of control.

Roles and Responsibilities

- **Systems administrators:** This employee is responsible for the operation and maintenance of the LAN and associated components, such as midrange or mainframe systems.
- **Quality assurance employees:** Employees in a quality assurance role can fill one of two roles: quality assurance or quality control. Quality assurance employees make sure programs and documentation adhere to standards; quality control employees perform tests at various stages of product development to make sure products are free of defects.
- **Database administrators:** This employee is responsible for the organization's data and maintains the data structure. The database administrator has control over all the data; therefore, detective controls and supervision of duties must be observed closely. This role is filled by a senior information systems employee because these employees have control over the physical data definition, implementing data definition controls, and defining and initiating backup and recovery.

Roles and Responsibilities

- **Systems analysts:** These employees are involved in the system development life cycle (SDLC) process. They are responsible for determining the needs of users and developing requirements and specifications for the design of needed software programs.
- **Network administrators:** These employees are responsible for the maintenance and configuration of network equipment, such as routers, switches, firewalls, wireless access points, and so on.
- **Security architects:** These employees examine the security infrastructure of the organization’s network.

Segregation of Duties (SoD)

- Job titles can be confusing, and different organizations sometimes use different titles for various positions. It helps when the title matches the actual job duties the employee performs. Some roles and functions are just not compatible. For an auditor, concern over such incompatibility focuses on the risks these roles represent when combined. Segregation of duties, or separation of duties, usually falls into four areas of control:
- **Authorization:** Verifying cash, approving purchases, and approving changes
- **Custody:** Accessing cash, merchandise, or inventories
- **Record keeping:** Preparing receipts, maintaining records, and posting payments
- **Reconciliation:** Comparing monetary amounts, counts, reports, and payroll summaries

Segregation of Duties (SoD)

- An individual having excessive access privileges beyond those needed for his or her role may lead to malicious, negligent, or accidental misuse of access.
- The more dangerous combinations of access that could cause the greatest harm are sometimes referred to as *toxic combinations*.
- The table on the following slide lists some of the duties (that is, toxic combinations) that should not be combined because they can result in control weaknesses.

Segregation of Duties (SoD)

First Job Role	Combined (Yes/No)	Second Job Role
Systems analyst	No	Security administrator
Application programmer	Yes	Systems analyst
Help desk	No	Network administrator
Data entry	Yes	Quality assurance
Computer operator	No	Systems programmer
Database administrator	Yes	Systems analyst
Systems administrator	No	Database administrator
Security administrator	No	Application programmer
Systems programmer	No	Security administrator

Compensating Controls

- Because of the problems that can occur when certain tasks are combined, separation of duties is required to provide accountability and control. When it cannot be used, compensating controls should be considered. In small organizations, it may be very difficult to adequately separate job tasks. In these instances, one or more of the following compensating controls should be considered:
- **Job rotation:** The concept is to not have one person in one position for too long a period of time. This prevents a single employee from having too much control.
- **Audit trail:** Although audit trails are popular after security breaches, they should be examined more frequently. Audit trails enable an auditor to determine what actions specific individuals performed; they provide accountability.

Compensating Controls

- **Reconciliation:** This is a specific type of audit in which records are compared to make sure they balance. Although it is primarily used in financial audits, reconciliation can also be used for computer batch processing and other areas in which totals should be compared.
- **Exception report:** This type of report notes errors or exceptions. Exception reports should be made available to managers and supervisors so that they can track errors and other problems.
- **Transaction log:** This type of report tracks transactions and the time of occurrence. Managers should use transaction reports to track specific activities.
- **Supervisor review:** Supervisor reviews can be performed through observation or inquiry, or they can be done remotely, using software tools and applications.

Key Employee Controls

Terms	Control Usage	Attributes
Background checks	Hiring practice	Helps match the right person to the right job
Required vacations	Uncovers misuse	Serves as a detective control to uncover employee malfeasance
Rotation of assignment	Prevents excessive control	Rotates employees to new areas
Dual control	Limits control	Aids in separation of duties
Non-disclosure agreement (NDA)	Aids in confidentiality	Helps prevent disclosure of sensitive information
Security training	Improves performance	Improves performance and gives employees information on how to handle certain situations
Segregation of duties (SoD)	Reduces the risk of error and fraud	Reduces the risk of human error or fraud by requiring that higher-risk transactions be performed by two or more people

PERFORMANCE MANAGEMENT

- Measuring performance is important to ensure that the organization's goals are consistently being met in an effective and efficient manner.
- You take measurements to see if you're headed in the right direction through quantitative analysis.
- This may seem obvious, but organizations have for years had difficulty selecting and understanding what to measure and how to measure an organization's performance.
-

PERFORMANCE MANAGEMENT

- How should IT performance management be measured.
- Does measuring the number of technology changes implemented over the past month seem important?
- Or does measuring the number of business service requests seem more appropriate?
- These measurements certainly have value, but they do not tell leadership whether the services are effective, cost-efficient, or aligned to strategic goals.
- When we think about performance management, we need to think broader than the processes we run.
- Consider the following perspectives:

PERFORMANCE MANAGEMENT

- **The customer perspective:** Includes the importance the company places on meeting customer needs. Even if financial indicators are good, poor customer ratings will eventually lead to financial decline.
- **Internal operations:** Includes the metrics managers use to measure how well the organization is performing and how closely its products meet customer needs.
- **Innovation and learning:** Includes corporate culture and its attitudes toward learning, growth, and training.
- **Financial evaluation:** Includes timely and accurate financial data. Typically focuses on profit and market share.

PERFORMANCE MANAGEMENT

- We put these broader perspectives into performance management, which helps us understand not only *what we produce* but also *what we consume* to produce our products and services.
- The pitfall of performance management measurements is taking the easy way out and only measuring quantitative waypoints that are readily available, such as the number of widgets produced, cost, speed, and quality.
- These readily available metrics have operational value but by themselves do not tell management if they are headed in the right direction.

PERFORMANCE MANAGEMENT

- These broader perspectives help understand not only *what we produce* but also *what we consume* to produce our products and services.
- The pitfall of performance management measurements is taking the easy way out and only measuring quantitative waypoints that are readily available, such as the number of widgets produced, cost, speed, and quality.
- These readily available metrics have operational value but by themselves do not tell management if they are headed in the right direction.
- Addong the broader perspective just discussed, we force performance management to align measurements to business objectives. For example, rather than just measuring speed to delivery in the abstract, you might measure customer satisfaction. Measuring customers who are highly satisfied with the product or service will tell you if the speed and quality are meeting their expectation. Conversely, customers who are less satisfied will have an issue with quality, the speed of delivery, and/or cost.

Key Performance Measurement Terms and Examples

Term	Definition
Metric	A unit of measurement
Unit	Scale against which a unit is measured
Target value	Business goal
Threshold	A minimum or maximum limit that indicates an unacceptable defect
Key performance indicator (KPI)	Defines how well a process is performing
Key goal indicator (KGI)	Defines how well a process is performing against a stated goal
Balanced scorecard (BSC)	A scorecard that brings together in one view key measurements such as metrics, target values, and key indicators

PERFORMANCE MANAGEMENT

- Say that management is trying to understand the effectiveness of the malware controls.
- The key to preventing operational disruptions is the capability to detect and cleanse malware.
- Knowing that cleansing is automated based on detection, management chooses the rate at which it can detect malware as its KPI.
- A high detection rate means less malware can cause disruptions. Knowing the level of redundancy in the processes, assume that management is comfortable that they can successfully manage one malware event per quarter.
- This threshold (typically referred to as a *risk threshold*) may indicate for the business the level at which unacceptable disruptions occur for products or services.

PERFORMANCE MANAGEMENT

- Complicated? Performance management is all about what needs to be accomplished, the business goals, and key measurements.
- Once a goal is set, it's a matter of comparing actual measurements against targets. In our example, the risk threshold is to have no more than one malware event per quarter, and given that the total number of malware events was four for the year, that threshold was achieved.
- Then why is the KGI a –400 percent? While the risk threshold was achieved, the business target value goal was to have only one malware event per year. The KGI is a broader indication of the business goal to be achieved.
- There is a close relationship between KPI and KGI: as the KPI changes, so does the KGI. In our example, if the malware detection rate is raised (as represented by the KPI), then we would expect to see a business goal being achieved, as represented by the KGI.

PERFORMANCE MANAGEMENT

- A steering committee needs to measure performance and align business strategy with IT objectives.
- A steering committee can be flooded with metrics.
- Selecting the metrics that are most insightful and can foster consensus among different organizational departments and groups to take action is essential in promoting healthy change.
- This is where a balanced scorecard (BSC) comes in.
- The information gathered using the balanced scorecard should be passed down the organizational structure to supervisors, teams, and employees.
- Managers can use the information to align employees' performance plans with organizational goals.

PERFORMANCE MANAGEMENT

- There is no set format for a balanced scorecard.
- The measurements should reflect business goals and targets compared to actual performance.
- There should be a direct or implied relationship between the measurements.
- That is, as one performance measure changes, related indicators should also change, as in the example that increased malware detection capability will have a positive effect on achieving a business goal.

MANAGEMENT AND CONTROL FRAMEWORKS

- A control framework categorizes and aligns an organization’s internal controls to identify and manage risk in the most optimal manner.
- A control framework is based on industry best practices to provide management with an effective tool to establish processes that create business value and minimize risk.
- An organization will adopt multiple management and control frameworks, based on the risk being controlled. For example:
- An enterprise architecture framework is adopted to control the risks related to software and system deployments.
- A security framework is adopted to control risks related to information and cybersecurity,
- A quality management framework is adopted to ensure that products and services are maintained within acceptable risk thresholds.

MANAGEMENT AND CONTROL FRAMEWORKS

- Think of management and control frameworks as *best practices rules* for unique disciplines in an organization.
- A larger organization with more diverse disciplines will have a greater number of frameworks adopted.
- This concept of organizational disciplines is important and explains many of the origins of the frameworks.
- This is especially true for the information systems disciplines. A finance department will have very different risks and challenges than an information security department.
- Both are important disciplines, and both have industry groups and associations promoting industry best practices. These industry groups and associations eventually create what we know as management and control frameworks.

MANAGEMENT AND CONTROL FRAMEWORKS

Framework	Definition
COSO	COSO is a commonly used framework for running an efficient and well-controlled financial environment.
Control Objectives for Information and Related Technologies (COBIT)	The Information Systems Audit and Control Association (ISACA), an international industry association, has published COBIT, which 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.
ISO	International Organization for Standardization (ISO), an international industry group, creates requirements, specifications, and guidelines across many information system disciplines. The following example illustrates several key ISO publications: ISO 9001 series focuses on quality management ISO 14001 series focuses on environmental systems ISO 27000 series focuses on information security
NIST Cybersecurity Framework (CSF)	The National Institute of Standards and Technology (NIST), a unit of the U.S. Commerce Department, published the CSF, which provides guidance on how to assess and improve the ability to prevent, detect, and respond to cyberattacks. The framework is mandatory for many non-defense U.S. government agencies and has been adopted by the private sector.

Enterprise Architecture

- Enterprise architecture is a good example of multiple frameworks coming together to define a discipline within an organization.
- We know that information security governance focuses on the availability of services, integrity of information, and protection of data confidentiality. Information security governance has become a much more important activity in the past decade.
- The growing number of Internet businesses and services has accelerated this trend. The Internet and global connectivity extend a company's network far beyond its traditional border. This places new demands on information security and its governance. Attacks can originate from not just inside the organization but from anywhere in the world.
- Failure to adequately address this important concern can have serious consequences.

Enterprise Architecture

- One way to enhance security and governance is to implement components of the NIST framework as requirements in an *enterprise architecture* (*EA*) plan. Such a plan organizes and documents a company's IT assets to enhance planning, management, and expansion.
- The primary purpose of using EA is to ensure that business strategy and IT investments are aligned. The benefit of EA is that it provides traceability that extends from the highest level of business strategy down to the fundamental technology.
- EA has grown since John Zachman, the originator of the Framework for Enterprise Architecture, first developed it in the 1980s; companies such as Intel, BP, and the U.S. government now use this methodology.
- Federal law requires government agencies to set up EA and a structure for its governance. This process is guided by the Federal Enterprise Architecture Framework (FEAF) reference model, which is designed to use six models:

Enterprise Architecture

1. **Performance reference model (PRM):** A framework used to measure performance of major IT investments
2. **Business reference model (BRM):** A framework used to provide an organized, hierarchical model for day-to-day business operations
3. **Infrastructure reference model (IRM):** A framework used to classify service components with respect to how technology supports the business through hardware, hosting, data centers, cloud, and virtualization
4. **Application reference model (ARM):** A framework used to categorize the standards, specifications, and applications that support and enable the delivery of service components and capabilities
5. **Data reference model (DRM):** A framework used to provide a standard means by which data may be described, categorized, and shared
6. **Security reference model (SRM):** A framework used to provide a standard means to describe information security and cybersecurity controls and how to adjust the risk and protect individuals' privacy

Enterprise Architecture

- Management is tasked with the guidance and control of the organization; managers are the individuals who are responsible for the organization.
- Although companies are heavily dependent on technology, a large part of management's duties still involves people, processes, and related technology.
- People are key to making a company successful. Therefore, a large portion of management's duties depends on people skills, including interaction with staff and with those outside the traditional organizational boundaries.
- *Outsourcing* might not be a term that some people like, but it's a fact of life that companies depend on an array of components and services from around the world. For example, consider Dell Computer. Dell might be based in Round Rock, Texas, but its distribution hub is in Memphis, Tennessee; Dell assembles PCs in Malaysia and has customer support in India. Many other parts come from the far corners of the globe. The controls that a company places on its employees and contracts, as well as its agreements with business partners and suppliers, must be examined and reviewed.

Change Management

- Change is inevitable, especially when dealing with technology, whose evolution is relentlessly fast paced. When it comes to meeting management and customer expectations, the stakes are high. Get it right, and you are a hero! Have enough failed deployments or system outages, and you may be looking for a new job.
- Technologists and IS auditors are tasked with ensuring that all changes are documented, accounted for, and controlled. Companies should have a well-structured process for change requests (CRs). The following steps provide a generic overview of the change management process:

    1. Request a change.

    2. Approve the request.

    3. Document the proposed change.

    4. Test the proposed change.

    5. Implement the change.

Change Management

- Change is inevitable, especially when dealing with technology, whose evolution is relentlessly fast paced. When it comes to meeting management and customer expectations, the stakes are high. Get it right, and you are a hero! Have enough failed deployments or system outages, and you may be looking for a new job.
- Technologists and IS auditors are tasked with ensuring that all changes are documented, accounted for, and controlled. Companies should have a well-structured process for change requests (CRs). The following steps provide a generic overview of the change management process:

    1. Request a change.

    2. Approve the request.

    3. Document the proposed change.

    4. Test the proposed change.

    5. Implement the change.

Change Management

- CRs are typically examined by a subject matter expert (SME) before being implemented.
- CRs must also be assessed to ensure that no change poses a risk for the organization.
- If an application or code is being examined for a potential change, other issues must be addressed, including how the new code will move from the coding to a production environment and how the code will be tested, as well as an examination of user training.
- Change management ensures that proper governance and control are maintained.

Quality Management

Quality management is an ongoing effort to provide information systems–related services that meet or exceed customer expectations.

It is a philosophy to improve quality and strive for continuous improvement. An auditor should be knowledgeable in these areas:

- Hardware and software requisitioning
- Software development
- Information systems operations
- Human resources management
- Security

Quality Management

- Why are so many quality management controls and change management methods needed?
- Most companies move data among multiple business groups, divisions, and IT systems. Auditors must verify the controls and attest to their accuracy. ISO 9001 is one quality management standard that is receiving widespread support and attention.
- ISO 9001 describes how production processes are to be managed and reviewed. It is not a standard of quality but covers how well a system or process is documented.

Quality Management

- Companies that want to obtain an ISO 9001 certification must perform a gap analysis to determine what areas need improvement. The ISO 9001 consists of six procedure documents that specify the following:
- Control of documents
- Control of records
- Control of nonconforming product
- Corrective action
- Preventive action
- Internal audits

Quality Management

- Being ISO certified means that the organization has the capability to provide products that meet specific requirements; this includes the process of continual improvement.
- Being ISO certified can also have a direct bearing on an IS audit because it places strong controls on documented procedures.
- Another ISO document that an auditor should be aware of is ISO 27000 series, which is considered a code of practice for information security. These documents are written for individuals who are responsible for initiating, implementing, or maintaining information security management systems. Its goal is to help protect confidentiality, integrity, and availability, and it includes the following:

Quality Management

- Risk assessment and treatment
- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management
- Compliance

Quality Management

- Risk assessment and treatment
- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management
- Compliance

Quality Management

A final control framework worth mentioning and that we know is the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which was designed to improve the quality of financial reporting.

- The framework considers changes in business and operating environments and demonstrates how a variety of entities should operate, including public, private, not-for-profit, and government organizations. COSO framework definitions and principles include the following core areas:
- Control Environment
- Risk Assessment
- Control Activities
- Information & Communications
- Monitoring Activities

Quality Management

- The underlying premise of all these management and control frameworks is that an organization exists to provide value for its stakeholders.
- All organizations face uncertainty, and the challenge for management is to determine how much uncertainty to accept as it strives to grow its services to its customers and drive stakeholder value. Uncertainty presents both risk and opportunity.
- Effective management of risk can bolster confidence or enhance value. Management and control frameworks can maximize value when management sets strategy and objectives to strike an optimal balance between delivery, growth, and risks. Effective management and control frameworks will achieve the following:
- Align strategy and risk appetite
- Implement effective processes to enable risk response decisions
- Reduce operational surprises and losses

MATURITY MODELS

- Another means of quality management is the ***capability maturity model*** (*CMM*), designed to improve any process.
- As processes mature, the quality of their products and services become more consistent and reliable.
- There are many CMMs on the market, focused on different industries and addressing different risks. Most CMMs align to five maturity levels:

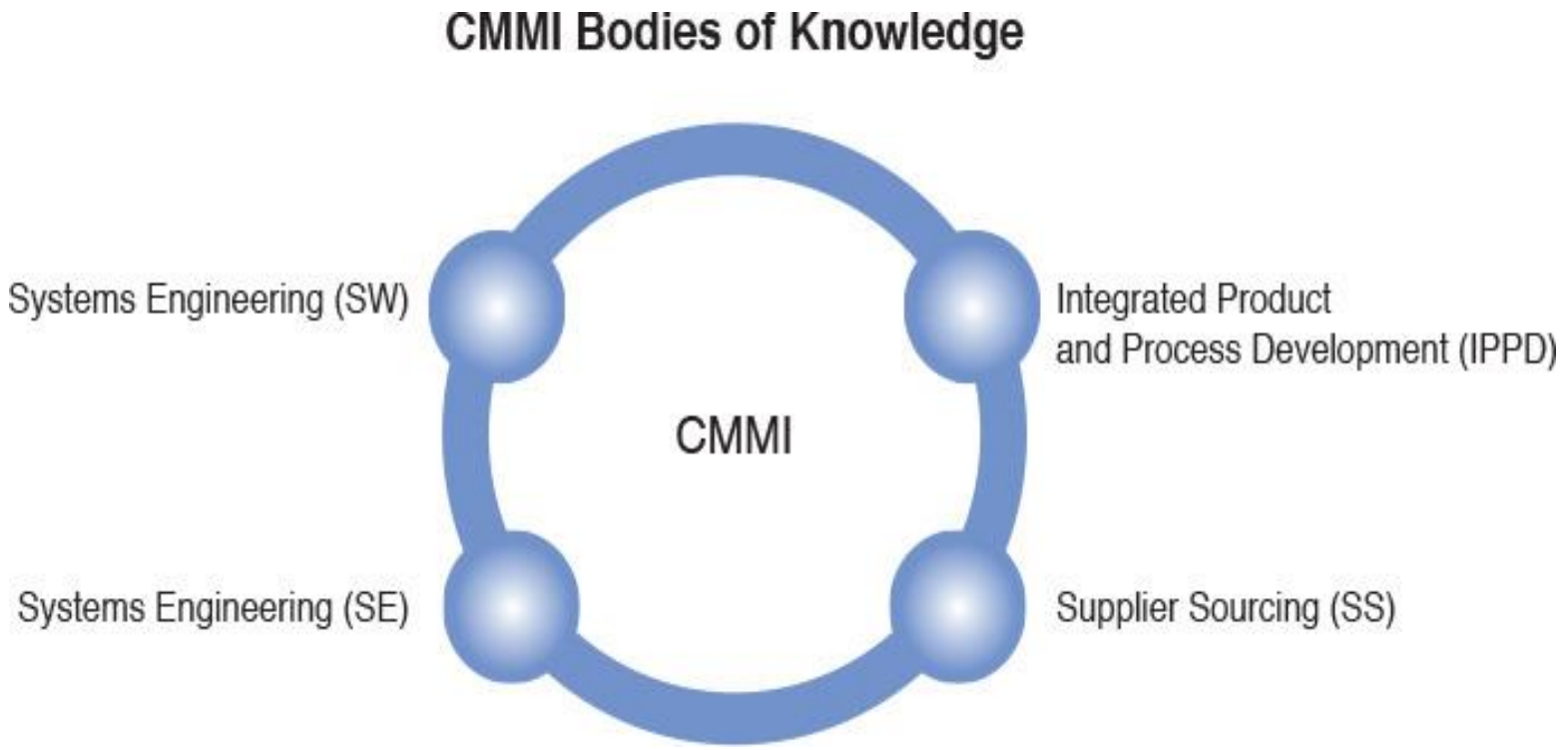
MATURITY MODELS

Maturity Level	Name	Description
1	Initial	This is an ad hoc process with no assurance of repeatability.
2	Repeatable	Change control and quality assurance are in place and controlled by management, although a formal process is not defined.
3	Defined	Defined processes and procedures are in place and used. Qualitative process improvement is in place.
4	Managed	Quantitative data is collected and analyzed. A process improvement program is used.
5	Optimized	Continuous process improvement is in place and has been budgeted for.

MATURITY MODELS

- Carnegie Mellon University provided one of the first major CMM models adopted by the industry in 1990. In 2006 Carnegie Mellon University released a major upgrade, referred to as the *capability maturity model integration* (*CMMI*) model. The COBIT 5 Capability Maturity Model references the same five maturity levels and is based on the ISO/IEC 15504 Capability Determination Model.
- A CMM is an activity-based model. It focuses on the completion of a process and does not care about the desired result and, hence, does not motivate the organization to make the necessary changes.
- In contrast, CMMI is a result-oriented model based on key performance areas and, therefore, represents best practice for a given knowledge area.
- The idea is that establishing and continually improving knowledge areas will help organizations decrease costs and improve quality and speed of delivery.

CMMI Bodies of Knowledge



MATURITY MODELS

- The COBIT 5 CMM is outcome based. The difference between COBIT 5 CMM and CMMI is that COBIT 5 is applied against five domains that include 37 processes, covering all aspects of managing and delivering technology solutions, from the board level to the developer. These are the five COBIT 5 domains:
- Evaluate, Direct and Monitor (EDM)
- Align, Plan and Organize (APO)
- Build, Acquire and Implement (BAI)
- Deliver, Service and Support (DSS)
- Monitor, Evaluate and Assess (MEA)
- While both CMMI and COBIT 5 CMM are outcomes based, CMMI can be viewed as more industry and specific process focused. The CMMI knowledge areas tend to be more prescriptive and detailed. In contrast, COBIT 5 CMM has broader application across multiple industries and aligns to specific control objectives across 37 well-defined processes.

Implementing a Maturity Model

- Implementation of a maturity model is fairly straightforward. Depending on the maturity model framework selected (such as CMMI or COBIT 5 CMM), the fram
- Think about maturity levels the same way you think about school. Assume that your local school requires Algebra I for eighth grade and Algebra II for ninth grade. An individual will be eligible to graduate from eighth grade to ninth grade only when she demonstrates that she has achieved proficiency in Algebra I. In addition, the proficiency in Algebra I is foundational for meeting the next requirements for Algebra II.
- Maturity models work much like the algebra graduation analogy. To graduate between maturity levels, an individual must demonstrate having met all the prescriptive requirements, as defined by whichever framework has been chosen. In addition, each subsequent layer will build on the previous layer as the maturity level increases.

Implementing a Maturity Model

- We can illustrate this point with a simplified example related to project management process maturity requirements:
- Level 2 requires the following:
- Establish cost estimates.
- Establish a plan.
- Obtain approval.
- Level 3 requires the following:
- Coordinate and collaborate with stakeholders.
- Establish a back out plan.

Implementing a Maturity Model

- The project management process maturity requirements shown here illustrate the set of simplified requirements needed to graduate from Level 2 to Level 3 maturity. This is not to suggest that the project would not be successful at maturity Level 2.
- As maturity level rises, risk is taken out of the process. In this case, two risks would be eliminated in moving from maturity Level 2 to Level 3.
- The first risk is reduced by formally engaging the stakeholders in the development and deployment of the project.
- The second risk is reduced by ensuring that a formal backout plan is established in the event that the project does not function as expected. Neither of these risks may occur at Level 2.
- Nonetheless, having a formal plan to deal with both instances will increase the projected likelihood of success.

Implementing a Maturity Model

- Achieving maturity Level 5 is generally accepted as applying a higher level of automation to reducing defects and driving consistency.
- Should all organizations strive for maturity Level 5? No.
- Each progressive maturity level comes at a cost. Applying maturity Level 5 to every process would be cost-prohibitive, and the introduction of automation can make simple tasks more complex. For example, updating a monthly price table may be ideal for humans, while scanning for malware requires a high degree of automation.
- The determination of what maturity level is required is driven by balancing risk, cost, industry best practices, and what's needed to achieve regulatory compliance.
- An IS auditor needs to ensure that an appropriate set of tools and criteria have been used within management's risk decision process.

MANAGEMENT'S ROLE IN COMPLIANCE

- We previously looked at and know of Regulatory Standards – these are key laws, rules, and regulations.
- Let's now consider management's role in compliance with these regulations, which were also introduced earlier:
- **U.S. Health Insurance Portability and Accountability Act (HIPAA):** U.S. standards on management of health care data
- **Sarbanes-Oxley Act (SOX):** U.S. financial and accounting disclosure and accountability for public companies
- **Payment Card Industry (PCI) standards:** Handling and processing of credit cards
- **U.S. Federal Information Security Management Act (FISMA):** Security standards for U.S. government systems
- **U.S. Fair and Accurate Credit Transaction Act of 2003 (FACTA):** Legislation to reduce fraud and identity theft

MANAGEMENT'S ROLE IN COMPLIANCE

- You should see two themes emerging from these regulations related to the importance of protecting privacy and maintaining effective information security controls.
- Laws are often enacted after a major event or data breach. After such an event that broadly impacts markets or millions of customers, lawmakers often feel pressure to do something to ensure that such events do not reoccur. That something often takes the form of passing new laws or regulations.
- Laws and regulations have the benefit of being mandatory, which is a strong motivator for the market to move in a certain direction. The inherent weakness of laws and regulations is that they take a long time to enact and often are not put into place until well after the initial event occurred.
- Consequently, laws and regulations are typically considered *lagging indicators* of risk.

MANAGEMENT'S ROLE IN COMPLIANCE

- Management and control frameworks created by industry groups and associations are much better *leading indicators* of risk.
- These frameworks have the benefit of direct support and updates from industry leaders. In addition, industry framework updates are released on a much shorter timeline than laws and regulations.
- The **inherent weakness** of these frameworks is that they are optional and not enforceable in the same way as laws and regulations.
- The scope and level of adoption of industry frameworks are dependent on leadership's commitment, regulatory inquiries, and peer pressure.
- Consequently, organizations will comply with both regulations and industry frameworks to control technology risks.
- Industries that are highly regulated generally tend to have more formal adoption programs related to industry frameworks and regulatory mandates.

MANAGEMENT'S ROLE IN COMPLIANCE

- Management must demonstrate and evidence compliance. It's not enough to have trained teams of employees and published standards.
- An IS auditor looks for evidence that an organization complies with key requirements and controls risk consistently.
- Regulators want to see a culture of managing risk effectively through regulatory compliance. Organizations that tend to do well during an audit or a regulatory exam have the following in place to support evidence of compliance:
- **Organizational functions dedicated to compliance:** Management must demonstrate that teams understand regulatory expectations and continually review internal controls for compliance
- Examples: Compliance, operational risk, and audit functions

MANAGEMENT'S ROLE IN COMPLIANCE

- **Risk culture:** Management must promote a risk culture. More than publishing standards, management must establish a *tone at the top*—a term that refers to actions taken by leadership to visibility demonstrate active support for the compliance program.
- Examples: Leadership placing risk discussion as a priority on agendas and management reaction to noncompliance events
- **Risk strategy:** An organization needs to have a well-articulated risk strategy.
- Examples: Policies, standards, and processes to control risk and ensure compliance
- **Risk registry and risk assessments:** An organization needs to have continuous risk assessments and a repository that tracks risks from identification, to remediation, to acceptance. This includes the organization's ability to evaluate and communicate internal control deficiencies in a timely manner to the parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.
- Examples: Audits, risk examination, remediation tracking

PROCESS OPTIMIZATION TECHNIQUES

- Regardless of your role as an information systems audit, assurance, and control professional, you are expected to understand basic process optimization techniques. The concept behind process optimization is the ability to apply a systematic technique that reduces the following:
- Variances and inconsistencies
- Risks to the process operations
- Complexity
- Costs

Taguchi

- The Taguchi method was developed by Genichi Taguchi to improve the quality of manufacturing in Japan after World War II. The Japanese manufacturers were struggling with very limited resources and poor equipment. Genichi Taguchi developed his technique to optimize manufacturing processes to reduce costs, eliminate waste, and utilize resources for their maximum value.
- The Taguchi method is a statistical approach to optimizing how a process is designed and improving the quality of each of its components.
- Since its introduction, the Taguchi method has been adopted and adjusted to work across industries beyond manufacturing. All processes are affected by outside influences, which Genichi Taguchi refers to as *noise*.
- The Taguchi method offers a systematic way of identifying the noise sources that have the greatest effects on product variability. The idea is that if you can reduce or eliminate this noise, you can produce products (and services) in an optimized and consistent manner.

Taguchi

- While the Taguchi method can be used to improve existing processes, most engineers believe that the greatest value lies in applying the method when creating new processes. They believe that the best way to improve process quality is to design it into the process.
- The key concept to the Taguchi method is what's termed an *experiment*. It's an iterative process in that the following stages can be repeated over time:
- Build → Test → Fix
- Basically, each iteration of the test after the build is an experiment to measure the level of noise. As you pass through iterations and use statistical methods to measure the noise and outcome, you can determine the level of optimization being achieved.
- The Taguchi principles and methods are a unique quality and process improvement technique. Optimized processes tend to produce consistent quality outcomes and be more insensitive to noise and variations in the environment. The Taguchi method to quality engineering places emphasis on minimizing variation as the main means of improving quality. The Taguchi approach is illustrated in the following iteration steps:

Taguchi

- Identify the main function and unintended outcomes.
- **2.** Identify the noise factors and testing condition.
- **3.** Identify key quality characteristics.
- **4.** Identify the objective method of measuring optimization.
- **5.** Conduct the experiment.
- **6.** Examine the data; predict optimum control levels and adjust.
- **7.** Conduct the verification experiment.
- This is a very useful method because it is statistically accurate. The outcome of the process becomes consistent and predictable, with low levels of variance. The Taguchi method gives you a quantitative way of measuring outcome quality. In addition, you can measure when optimization efforts result in no tangible effort or, worse, a negative effect. These experiments and measurements collectively improve management's understanding of the process and avoid wasted efforts that do not significantly improve quality.

PDCA

- Whereas the Taguchi method is a quantitative approach that can be time-consuming, is expensive to execute, and requires a team that is well trained and experienced, the Plan-Do-Check-Act (PDCA) approach is more qualitative and, though less rigorous than the Taguchi method, can also be of value.
- The PDCA cycle is an iterative four-step problem-solving model that promotes continuous improvement.
- The PDCA model dates back to 1939, when Walter A. Shewhart, an American physicist, engineer, and statistician, first published the concept that constant evaluation of management practices is key to the evolution of effective processes and a successful enterprise.
- Since its first introduction, the concept has been widely adopted across different industries as a means of achieving continuous process improvement.

PDCA

Step Number	Step Name	Description
1	Plan	Establish process objectives.
2	Do	Implement the process.
3	Check	Measure actual process outcomes against objectives.
4	Act/adjust	Adjust the process to close the gap between actual and planned objectives.

PDCA

Plan: The *plan* step establishes formal control objectives, projects outcomes, and defines the processes needed to achieve the objectives and outcomes. The output from the expectations created in the plan step will become part of the development cycle for the check step. Pilot and prototype testing are encouraged in the PDCA model.

- As an IS auditor or control partner assessing the process, you would either obtain these details from existing process documentation or reverse engineer to obtain them.

Do: The *do* step involves implementing the plan and executing the process. Data is then collected on the outcome, including data on the quality of the product and services produced. Data should be collected on each key requirement specified in the plan step.

PDCA

Check: During the *check* step, the outcome from the do step is assessed. This assessment is sometimes referred as the *PDCA study*. The assessment compares the actual results collected in the do step against the predicted results in the plan step. Variances can be positive or negative. Positive variance means more value is obtained. Negative variance means less value than expected is obtained. Negative variance typically requires some level of corrective action.

Act/adjust: The *act/adjust* step takes as input the results from the check step and applies corrective action. During the act/adjust step, root causes are determined. Over time, trends are tracked and feedback is considered in the plan step so future processes can benefit. This iterative process establishes continuous improvement. Each pass through a PDCA iteration incrementally improves the process. The goal is to ensure that quality is both initially and continuously achieved.

Taguchi Versus PDCA

- The Taguchi and PDCA methods share many common techniques. They are both iterative and incrementally improve quality over time. But quantitative and qualitative techniques are fundamentally as different as night and day. Both methods have utility and value when applied under the right circumstances.
- The Taguchi quantitative approach is far more precise in the identification and statistical certainty of its outcome. Its high cost and complexity make it better suited for expensive and more critical processes.
- PDCA places a high reliance on qualitative judgment, and it's far more reliant on the expertise of the assessor. Its comparable lower cost and agility makes it ideal for lower-cost, low-volume processes, such as back-office IT support processes.

.

MANAGEMENT OF IT SUPPLIERS

- When an organization uses an external service provided to deliver IT solutions on its behalf, the practice is called *IT outsourcing*. The external service provided is called an *IT supplier*, *IT vendor*, or *IT third-party provider*, though often *IT* is dropped, and terms are shortened to *supplier*, *vendor*, or *third party*.
- The services provided by an IT supplier can include any IT function, such as hosting applications in the cloud, providing external data storage, or processing transactions on behalf of the organization. Outsourced IT services can improve your organization's focus. It is neither practical nor possible to be a jack of all trades.
- Outsourcing lets management focus on core competencies and competitive advantage while suppliers focus on being the best at their business. Suppliers also have the advantage of scale when an organization outsources information technology to a supplier that specializes in a particular area and can spread costs across multiple customers.
- An organization must effectively manage the relationship and services it provides—whether on its own or through third parties—and balance the benefits and risk of handing control to an external supplier.

Third-Party Outsourcing

- Outsourced IT functions can occur at a wide range of locations, including the following:
- **Onsite:** Employees and contractors work at the company's facility.
- **Offsite:** Staff and contractors work at a remote location.
- **Offshore:** Staff and contractors work in a separate geographic region.
- Organizations should go through a sourcing strategy to determine what information systems tasks must be done by employees. Commodity services that do not offer a competitive advantage are often targeted for IT outsourcing. That has the benefit of allowing an organization to focus internal IT resources on the services that provide maximum value. Commodity services that are often outsourced include the following:

Third-Party Outsourcing

- Data entry
- Application/web hosting
- Help desk
- Payroll processing
- Check processing
- Credit card processing

Third-Party Outsourcing

- One key to the outsourcing decision is determining whether a task is part of the organization's *core competency* or *proficiency* that defines who the organization is. This is a fundamental set of skills or knowledge that gives the company a unique advantage. Outsourcing a core competency could put the company at risk because of the over reliance on the vendor.
- For example, if the core competencies were moved to a vendor who later went out of business then the company could lose that unique market advantage. Additionally, the company should analyze whether the tasks being considered for outsourcing can be duplicated at another location and whether they can be performed for the same or less cost.

Third-Party Outsourcing

- Information security should also play a role in the outsourcing decision because some tasks take on a much greater risk if performed by others outside the organization. Any decisions should pass a thorough business process review.
- For example, does data entry report a large number of errors, is the help desk backlogged, or is application development more than three months behind schedule? Some of the most common outsourced tasks are data entry and processing.
- When a task is outsourced, accuracy can be retained by implementing a ***key verification*** process to ensure that the process was done correctly.
- For example, the company's data entry department might key in information just as the outsourcing partner does in India. After both data sets are entered, they can be compared to verify that the information was entered correctly. Any keystroke that does not match flags an alert so that a data-entry supervisor can examine and verify it.

Third-Party Audits

- When the decision is made to outsource, management must be aware that it will lose some level of visibility when the process is no longer done in-house.
- Outsourcing partners face the same risks, threats, and vulnerabilities as the client, but they might not be as apparent to the client. Because of this loss of control, every outsourcing agreement should contain a ***right-to-audit*** clause.
- Without a right-to-audit statement, the client would be forced to negotiate every type of audit or review of the outsourcing partner's operation.
- These negotiations can be time-consuming and very costly. Therefore, a right-to-audit clause is one of the most powerful mechanisms a company can insist upon before an agreement is signed.

Third-Party Audits

- From a supplier's viewpoint, having large numbers of customers auditing processes and facilities can be disruptive and can impact costs.
- Many suppliers recognize the need to provide their customers' management with evidence that their processes are following industry best practices.
- Suppliers often hire external audit firms to perform what is called SSAE 16 assessments.
- The SSAE 16 is an industry-accepted assessment of a supplier's general control environment.
- It allows a supplier to be audited once, and the reports can be provided to multiple customers.
- Customers' management can accept an audit in its entirety or call on its right-to-audit statement to focus on specific areas not covered by the SSAE 16 assessment.

Third-Party Audits

- The Statement on Standards for Attestation Engagements (SSAE) No. 16, “Reporting on Controls at a Service Organization,” was issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) in April 2010. The SSAE 16 replaced SAS 70 as the standard for reporting on external IT service providers.
- While SSAE 16 was replaced by SSAE 18 effective May 2017.
- The SSAE 18 update brings in a couple significant differences than its predecessor, SSAE 16. Its main purpose is to clarify certain old standards and streamline and simplify the review process. The update to this standard will also demand companies take more control and responsibility of the people they work with, primarily third-party vendors.

Third-Party Audits

- The changes do not seem so arduous for organizations to deal with, but the changes seem to be for the better and could help bridge any spaces between these company relationships.
- Under the new SSAE 18 guidelines, service organizations will now need to have specific management programs for their third-party vendors. If an organization has third-party vendors, also known as Subversive Organizations, the company needs to have clearly described responsibilities for each of these vendors.
- In addition to this, they need to have recorded performance reviews that **contain routine audits** and reviews on what they learned from these findings.

.

Third-Party Audits

- Service Organizations also need to have a formal process to gauge annual risk assessment. This new statement of standards also addresses risks and mandates an assessment for them.
- As a part of each report for third-party vendors, each company needs to include specific plan details on how they deal with risk management. The report for this program also needs to explain and outline the efficiency of this plan.
- Another facet that this guideline states is that any third-party vendor working for a company should also uphold the same standards as the company they are working with.
- Also under the new statement of standards, the management team will also be required to provide a written statement for further assurance. This document should declare the entire capacity of whom they are working with.

Contract Management

- An important control within a supplier's contract is the service level agreement (SLA).
- The supplier's SLA outlines management's expectations of the supplier, such as the timeliness and quality expected in the supplier's services.
- With a time-sensitive process, implementing an SLA is one way to obtain a guarantee of the level of service from the supplier.
- The SLA should specify the uptime, response time, and maximum outage time to which the parties are agreeing.

Contract Management

- Think of contracts as the early stages of establishing a relationship with an IT supplier. Both parties in negotiation convey their expectations and commitments. There is a difference between having committed outcomes and trying your best to achieve an outcome.
- If an organization’s transaction must be completed within a specific time, the supplier should add that SLA to the contract. Once contract terms have been agreed upon, the parameters of the relationship have been set.
- An important benefit of effective contract management is clarity. The terms of a contract often become what is measured and managed. For example, an outsourced call center may require that 99 percent of calls be answered within so many rings of the phone.
- That term in the contract can be used as a measurement point to monitor the vendor’s performance.

Contract Management

- A good contract anticipates disputes between management and the supplier and negotiates terms of mutual benefit.
- This concept of mutual benefit is important. When contract terms for the supplier are not cost-effective, the supplier may cut corners and may fail to deliver the quality and speed needed.
- Having healthy suppliers benefits the organization and the industry.

Performance Monitoring

- Once the contract terms are in place, the supplier's performance must be monitored. Performance is typically monitored against specific terms set in the contract.
- The key in performance monitoring of suppliers is to identify the risks that management wants to control.
- Not every term of a contract will be monitored. Management needs to focus on key risks to the business.
- The organization is ultimately accountable for the performance of a supplier. It needs to view the supplier as an extension of the organization.
- **The supplier will have access to the organization's data and product.** As a result, the quality of the organization's products and services is often tied to a supplier's performance.

Performance Monitoring

- Think of it this way: if management chose not to outsource and produced an IT service internally, would they check on the quality?
- If the answer is yes, then most likely management needs to also check on the supplier’s quality.
- Most risks can be avoided altogether if management creates a team that is dedicated to monitoring supplier performance and performing effective relationship management.
- Such a specialized team can establish a performance monitoring program based on controlling risks related the following themes:

Performance Monitoring

- **Speed:** The SLA terms are typically used to monitor the speed of delivery by the supplier.
- **Quality:** Management should consider monitoring both the quality of the product or services being delivered by the supplier and the quality of the supplier's staff. The contract should include terms related to the qualifications of the supplier team working on the IT solutions (for example, background checks, technical expertise).
- **Cost:** Billing from the supplier should be monitored against contract terms. Outsourcing IT services often provides financial benefits that should be managed as well. A *change order* typically involves asking a supplier to vary the normal process. Costs associated with change orders need to be carefully monitored to ensure that a supplier does not overcharge and erode the cost benefits projected

Relationship Management

- Management can overcome many outsourcing difficulties simply through good communication with the supplier.
- This ongoing relationship builds trust and creates a partnership that helps manage risks consistently. Not every situation can be anticipated or codified in the contract.
- When unexpected situations arise, you need two reasonable entities to come together to solve the problem to the mutual satisfaction of both parties. At the core of this process should be a well-established relationship.
- Relationship management takes time and effort. The benefits are obvious when it’s done well. On the other hand, the outcome can be devastating when the supplier relationship is poor or when the supplier does the minimum to stay within prescriptive terms of the contract.

Relationship Management

- For example, say that you have a supplier providing partial hosting services. Let’s assume that your own data center has a significant power disruption that is estimated to last 24 hours.
- Management would ideally like to shift additional processing to the supplier hosting facility. However, the supplier is at nearly full capacity, and the additional hosting is beyond the terms of the agreement.
- Sounds like an unsolvable problem, and management simply needs to take the hit on being out of business for 24 hours. When a supplier perceives the relationship with the client as long-term and profitable, however, it will go to great lengths to preserve the relationship.

Relationship Management

- This may include contacting other customers and determining the feasibility of freeing capacity for the next 24 hours so the supplier can support additional hosting services.
- Now let’s reverse the example and assume that the supplier is moving between data center facilities, and the supplier will not be able to meet the contract’s SLA during that period of time. In this case, management can plan for the SLA disruption and reduce any associated risks.
- The point is that effective relationship management with suppliers can bridge the interests of both entities and balance rewards and risks. It can also protect both parties from unexpected situations and ensure that risks are effectively managed.

Relationship Management

- Here’s are some key takeaways:
- **Treat suppliers as an extension of your organization’s accountability:** Maintain a close relationship with each supplier.
- **Expect the unexpected:** Not all situations can be anticipated or covered in a contract.
- **Anticipate problems:** Manage the supplier relationship for the long term and to mutual benefit.
- **Review core services at least annually:** Even if a contract has not expired, the terms should be reviewed periodically.
- **Monitor performance:** Monitor performance against key terms in the contract.