The Information Systems Audit

INFO 6008 Week 3

FANSHAWE

The Process of Auditing Information Systems

- **We are covering the following topics:**
- **Skills and Knowledge Required to Be an IS Auditor:** This is an overview of certifications and work-related skills needed in the field.
- **Knowledge of Ethical Standards:** is an overview of the ISACA Code of Professional Ethics.

The Process of Auditing Information Systems

- **ISACA Standards, Procedures, Guidelines, and Baselines:** provides a foundational understanding of standards, procedures, guidelines, and baselines. In addition, this section covers major laws, rules, regulations, and international standards.
- **Risk Assessment Concepts:** provides an overview of how to define, assess, manage, and mitigate various types of risks.

The Process of Auditing Information Systems

- **Auditing and the Use of Internal Controls:** defines and reviews common types of internal controls an auditor will encounter.
- **The Auditing Life Cycle:** examines the stages of the audit process, including planning, examination, reporting and following up.
- **The Control Self-Assessment Process:** defines the attributes of a self-assessment process and explains its importance in the audit process.

The Process of Auditing Information Systems

- **Continuous Monitoring:** the importance of continuous monitoring is described and its benefits.
- **Quality Assurance:** reviews QA attributes that help businesses prevent costly mistakes or defects and control risks.
- **The Challenges of Audits:** describes the types of audit opinions that are typically issued by an auditor and the challenges related to issuing an audit opinion.

The Process of Auditing Information Systems

- Most organizations regardless of size, have a heavy reliance on information technology to stay ahead of their competition.
- Information systems drive revenue and often reflect the organization's image on the Internet.
- Information systems (IS) auditing ensures that an organization's data is:

❖ confidentially stored,

❖that data integrity is maintained,

❖and that information systems are available when needed.

The Process of Auditing Information Systems

- Most organizations regardless of size, have a heavy reliance on information technology to stay ahead of their competition.
- Information systems drive revenue and often reflect the organization's image on the Internet.
- Information systems (IS) auditing ensures that an organization's data is (CIA):

❖ confidentially stored,

❖that data integrity is maintained,

❖and that information systems are available when needed.

The Process of Auditing Information Systems

We will be covering the ISACA objectives: understanding the role and importance of auditing standards, guidelines, and best practices all of which are important for the CISA exam.

- Understand the skills needed to be an IS auditor
- Explain what an IS audit is
- Explain how an IS audit is managed and performed
- Define risks and how to analyze them

The Process of Auditing Information Systems

- Describe internal controls
- Understand how control assessments are performed
- Understand how an audit report is written and issued
- Explain the end-to-end audit process and understand the challenges

SKILLS AND KNOWLEDGE REQUIRED TO BE AN IS AUDITOR

- The CISA exams test you on knowledge and hard skills such as how to plan an audit.
- The exam also tests you in combination with a situational context. This tests a candidate on the soft skills an auditor needs. For example how to communicate audit examination results.

SKILLS AND KNOWLEDGE REQUIRED TO BE AN IS AUDITOR

Work-Related Skills

- An auditor has a successful career when he or she has an ever-improving set of skills that are applied consistently, relentlessly, and professionally, along with excellent interpersonal soft skills.
- It is said that a good auditor needs to be knowledgeable about the business, efficient, capable of exposing risk, able to deliver a tough message, and still welcome to go out for a beer afterward.
- The following table lists some of the important work-related soft and hard skills an auditor needs.

SKILLS AND KNOWLEDGE REQUIRED TO BE AN IS AUDITOR

Skill Type	Skill
Soft	Honest and ethical
Soft	Ability to pay careful attention to detail when completing work tasks
Soft	Excellent interpersonal skills, displaying a good nature and the ability to stay focused and calm
Soft	Ability to create and maintain professional relationships and develop allies
Soft	Willingness to lead, take charge, and offer opinions
Soft	Strong active listening and ability to understand other points of view

SKILLS AND KNOWLEDGE REQUIRED TO BE AN IS AUDITOR

Skill Type	Skill
Hard	Technically competent, having the skills and knowledge necessary to perform the auditor's work
Hard	Excellent verbal and written communication skills
Hard	Analytical thinking skills and ability to analyze information through sound logical thinking
Hard	Good project management and organizational skills
Hard	Critical thinking and the ability to use logic and reasoning techniques to identify weaknesses and develop solutions to problems

SKILLS AND KNOWLEDGE REQUIRED TO BE AN IS AUDITOR

Work-Related Skills

- While not an exhaustive list, it illustrates the skills that typically separate good auditors from bad auditors.
- You can be a successful auditor when you are ever-improving yourself – this frankly applies to any and all careers and relationships.

KNOWLEDGE OF ETHICAL STANDARDS

- The ISACA Code of Professional Ethics involves more than conducting an audit and goes beyond legal requirements; it defines principles and values that govern acceptable behavior.
- As an auditor, you must be above question at all times. You must treat clients honestly and fairly, and your actions must reflect positively on yourself, your company, and your profession.
- Note - The word *client* in this context means the leadership of the area you are auditing. If you are auditing within a company, then you have internal clients for the audit services you are providing.

KNOWLEDGE OF ETHICAL STANDARDS

- Let’s revisit one major historical event that illustrates the importance of ethical standards.
- Enron was founded in 1985. At its peak in 2000, it was one of America’s largest energy companies.
- By 2001 Enron was taking on massive liabilities and incurring massive losses. To keep its stock price up and hide the losses form the public, it used highly questionable offshore transactions and creative bookkeeping methods.

KNOWLEDGE OF ETHICAL STANDARDS

- Arthur Andersen was one of the five largest accounting firms in the United States at the time. It had a reputation for high standards and quality. Arthur Andersen oversaw, audited, and signed off on Enron’s financials and accounts.
- By December 2001, Enron declared bankruptcy.
- By August 2002, Arthur Andersen had closed its doors.

KNOWLEDGE OF ETHICAL STANDARDS

- Let's look at the events involving the Arthur Andersen auditors at Enron from the point of view of the ISACA Code of Professional Ethics.
- Knowing that the accounting practices were at the time questionable and not consistent with industry norms, what was the auditors' obligation?

KNOWLEDGE OF ETHICAL STANDARDS

- They could have refused to sign off on the company's books. But that might have caused the accounting firm to be fired and lose millions of dollars in accounting fees.
- What they chose to do was to sign off, put their firm's reputation behind Enron, and, worse yet, when the regulators began investigating, they destroyed some of their Enron audit documents.
- Like Enron, they faced criminal charges and ended up having to close their doors.

KNOWLEDGE OF ETHICAL STANDARDS

What was Arthur Andersen auditors' obligation?

First let's look at the ISACA Code of Professional Ethics and then break down the third point in the statement:

KNOWLEDGE OF ETHICAL STANDARDS

- ISACA sets forth this Code of Professional Ethics to guide the professional and personal conduct of members of the association and/or its certification holders. http://www.isaca.org/Certification/Code-of-Professional-Ethics/Pages/default.aspx
- Members and ISACA certification holders shall:

KNOWLEDGE OF ETHICAL STANDARDS

- Support the implementation of, and encourage compliance with, appropriate standards and procedures for the effective governance and management of enterprise information systems and technology, including: audit, control, security and risk management.
- Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards.

KNOWLEDGE OF ETHICAL STANDARDS

- Serve in the interest of stakeholders in a lawful manner, while maintaining high standards of conduct and character, and not discrediting their profession or the Association.
- Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.

KNOWLEDGE OF ETHICAL STANDARDS

- Maintain competency in their respective fields and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge and competence.
- Inform appropriate parties of the results of work performed including the disclosure of all significant facts known to them that, if not disclosed, may distort the reporting of the results.

KNOWLEDGE OF ETHICAL STANDARDS

- Support the professional education of stakeholders in enhancing their understanding of the governance and management of enterprise information systems and technology, including: audit, control, security and risk management.
- Failure to comply with this Code of Professional Ethics can result in an investigation into a member's or certification holder's conduct and, ultimately, in disciplinary measures.

KNOWLEDGE OF ETHICAL STANDARDS

So what was Arthur Andersen auditors' obligation?

- **Serve in the interest of stakeholders…:**

Stakeholders include the Enron shareholders, the pensions dependent on the Enron stock, and the Enron employees, to name a few.

None were well served by the auditors' decision.

KNOWLEDGE OF ETHICAL STANDARDS

So what was Arthur Andersen auditors' obligation?

- **Serve in the interest of stakeholders in a lawful manner…:**
- We can assume that even if the auditors thought the accounting practices were questionable rather than illegal, it was clear that their intent was not to be honest.

KNOWLEDGE OF ETHICAL STANDARDS

- **…while maintaining high standards of conduct and character, and not discrediting their profession or the Association:** At the time, Arthur Andersen auditors not only hurt their firm but called into question the professionalism of the industry.
- Fortunately, Arthur Andersen closing its doors helps demonstrate that such conduct is unacceptable to the industry and not the norm.

KNOWLEDGE OF ETHICAL STANDARDS

- CISA exam questions will raise a number of situational questions related to the Code of Professional Ethics.
- A CISA candidate is not expected to recite each word in the code of ethics.
- However, a candidate needs to understand the importance of conduct during an audit and of conveying the results honestly and transparently.

ISACA STANDARDS, PROCEDURES, GUIDELINES, AND BASELINES

- The CISA exam candidate is expected to understand the difference between a standard, a procedure, a guideline, and a baseline as well as in what situations they should be applied.
- There are a number of definitions in the industry for these four terms. We will be using the COBIT 5 use of the terms as defined in the following table:

ISACA STANDARDS, PROCEDURES, GUIDELINES, AND BASELINES

Title	Description
Standards	Mandatory actions, explicit rules, or controls that are designed to support and conform to a policy. A standard should make a policy more meaningful and effective by including accepted specifications for hardware, software, or behavior. Standards should always point to the policy to which they relate.
Procedures	Written steps to execute policies through specific, prescribed actions; this is the how in relation to a policy. Procedures tend to be more detailed than policies. They identify the method and state, in a series of steps, exactly how to accomplish an intended task, achieve a desired business or functional outcome, and execute a policy.

ISACA STANDARDS, PROCEDURES, GUIDELINES, AND BASELINES

Title	Description
Guidelines	An outline for a statement of conduct. This is an additional (optional) document in support of policies, standards, and procedures and provides general guidance on what to do in particular circumstances. Guidelines are not requirements to be met but are strongly recommended.
Baselines	Platform-specific rules that are accepted across the industry as providing the most effective approach to a specific implementation.

ISACA STANDARDS, PROCEDURES, GUIDELINES, AND BASELINES

Let's look at an example to gain a deeper understanding:

- "If you bought a car, which term would best describe the fact that, on average, you should change the oil every 5,000 miles?"
- Your answer choices are standard, procedure, guideline, and baseline.
- Here's how you could logically break down the question to pick the best choice:

ISACA STANDARDS, PROCEDURES, GUIDELINES, AND BASELINES

- **Baseline:** A baseline could be the right answer if there were more details about the car, such as the type of car, age of the car, driving habits, and so on.
- A salesperson driving a car 120,000 miles per year will change the oil far more often than a telecommuter driving 5,000 miles per year.
- A generic statement about cars would not be considered platform specific.

ISACA STANDARDS, PROCEDURES, GUIDELINES, AND BASELINES

- **Procedure:** A procedure is a set of steps to follow. This definition is not a fit, given the question.
- **Standard:** A standard could be the right answer if the question said the car is under a lease, and the lease agreement requires changing the oil every 5,000 miles.
- In the lease situation, the changing of the oil is mandatory, which would make standard a good answer. A giveaway that a standard does not apply, is the use of the hint word *should*, which conveys that there are options. It's generally accepted that standards that use the word *should* are poorly written because standards are mandatory.

ISACA STANDARDS, PROCEDURES, GUIDELINES, AND BASELINES

- **Guideline:** The term *guideline* **is the correct answer** because a guideline provides a general rule.
- If you didn't have any other specific information, then changing your car's oil every 5,000 miles would make sense.
- If you were to gain more information, you could adjust the frequency of oil change. For example, some of the newer (and more expensive) synthetic oils last longer, and thus you can drive 10,000 miles between oil changes.

ISACA STANDARDS, PROCEDURES, GUIDELINES, AND BASELINES

- Standards and guidelines are the cornerstone of the audit profession.
- Standards articulate what must be followed, and they are typically technology platform agnostic.
- In comparison, a guideline is more of a *use case* for a standard. A guideline explains how to comply with a standard.

ISACA STANDARDS, PROCEDURES, GUIDELINES, AND BASELINES

- It is important to understand that the ISACA standards and guidelines are issued across multiple industries and across multiple countries.
- One size does not fit all!
- Guidelines are optional, intended to give organizations examples of successful implementation of ISACA standards.

ISACA STANDARDS, PROCEDURES, GUIDELINES, AND BASELINES

- While an organization may use the ISACA standards, an organization will have their own standards, procedures, guidelines, and baselines.
- Therefore an organization's standards will not be the same as the ISACA audit and assurance standards.
- An organization typically selects the standards that best meet its needs.
- ISACA's audit and assurance standards are one source.

ISACA STANDARDS, PROCEDURES, GUIDELINES, AND BASELINES

- A manufacturing company may place heavy reliance on International Organization for Standardization (ISO) standards.
- A credit card merchant will place heavy reliance on Payment Card Industry Data Security Standards (PCI DSS), and so forth.

ISACA STANDARDS, PROCEDURES, GUIDELINES, AND BASELINES

- The terms *procedure* and *baseline* can be confusing. A *procedure* usually is a series of steps to achieve a specific outcome—for example, the particular steps in a company that you have to take to obtain a logon account for a new employee.
- A *baseline* is platform specific on a set of accepted rules—for example, setting a workstation's Windows 10 platform to time out after 15 minutes. The line between a baseline and a procedure can be blurry.

ISACA STANDARDS, PROCEDURES, GUIDELINES, AND BASELINES

- The workstation Windows 10 platform baseline may not only state that a 15-minute timeout is required but may also show the steps and a screenshot for how to make the setting.
- In that case, it is still a baseline, not a procedure.
- For the ISACA exam, remember that if a document is platform specific to implement a specific rule, you can treat it as a baseline.
- If the document is purely procedural steps with a focus on a specific outcome (such as a deliverable), you can treat it as a procedure.

ISACA STANDARDS, PROCEDURES, GUIDELINES, AND BASELINES

- According to ISACA: http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Pages/ObjectivesScopeandAuthorityofITAudit.aspx
- Standards contain statements of mandatory requirements for IS audit and assurance. They inform:

ISACA STANDARDS, PROCEDURES, GUIDELINES, AND BASELINES

- IS audit and assurance professionals of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics.
- Management and other interested parties of the profession's expectations concerning the work of practitioners
- Holders of the Certified Information Systems Auditor (CISA) designation of their requirements.

ISACA STANDARDS, PROCEDURES, GUIDELINES, AND BASELINES

Standards for IS Audit and Assurance - 17
1001 Audit Charter
1002 Organisational Independence
1003 Professional Independence
1004 Reasonable Expectation
1005 Due Professional Care
1006 Proficiency
1007 Assertions
1008 Criteria
1201 Engagement Planning
1202 Risk Assessment in Planning
1203 Performance and Supervision
1204 Materiality
1205 Evidence
1206 Using the Work of Other Experts
1207 Irregularity and Illegal Acts
1401 Reporting
1402 Follow-up Activities

ISACA STANDARDS, PROCEDURES, GUIDELINES, AND BASELINES

- Guidelines
- The objective of the IS Audit and Assurance Guidelines is to provide guidance and additional information on how to comply with the IS Audit and Assurance Standards.
- The IS audit and assurance professional should consider these guidelines when implementing, applying and justifying any departure from the standards.
- http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Pages/ObjectivesScopeandAuthorityofITAudit.aspx

ISACA STANDARDS, PROCEDURES, GUIDELINES, AND BASELINES

IS Audit and Assurance Guidelines
Audit Charter
Organizational Independence
Professional Independence
Reasonable Expectation
Due Professional Care
Proficiency
Assertions
Criteria
Engagement Planning
Risk Assessment in Planning

ISACA STANDARDS, PROCEDURES, GUIDELINES, AND BASELINES

IS Audit and Assurance Guidelines
Performance and Supervision
Materiality
Evidence
Using the Work of Other Experts
Irregularity and Illegal Acts
Audit Sampling
Reporting
Follow-up Activities

KNOWLEDGE OF REGULATORY STANDARDS

- An organization must work within a framework of laws and regulations, which may dictate how data is processed, handled, stored, and destroyed.
- Businesses are increasingly being tasked with processing a growing amount of electronic information.

KNOWLEDGE OF REGULATORY STANDARDS

- If they fail to handle this information properly and with due care, they could be subject to legal fines or loss of public confidence, and the top executive may even run the risk of jail time.
- Companies can be held liable if personal data is disclosed to an unauthorized person.

KNOWLEDGE OF REGULATORY STANDARDS

- The **General Data Protection Regulation (GDPR)**, agreed upon by the European Parliament and Council in April 2016, replaced the **Data Protection Directive 95/46/ec** on May 25, 2018 as the primary law regulating how companies protect EU citizens' personal data.
- Companies that fail to achieve GDPR compliance before the deadline will be subject to stiff penalties and fines.

KNOWLEDGE OF REGULATORY STANDARDS

- GDPR requirements apply to each member state of the European Union, aiming to create more consistent protection of consumer and personal data across EU nations. Some of the key privacy and data protection requirements of the GDPR include:

KNOWLEDGE OF REGULATORY STANDARDS

- Requiring the consent of subjects for data processing
- Anonymizing collected data to protect privacy
- Providing data breach notifications
- Safely handling the transfer of data across borders
- Requiring certain companies to appoint a data protection officer to oversee GDPR compliance
- Simply put, the GDPR mandates **a baseline set of standards** for companies that handle EU citizens' data to better safeguard the processing and movement of citizens' personal data.

KNOWLEDGE OF REGULATORY STANDARDS

- The following list of regulatory standards and links to websites, while not exhaustive, is a good representation of important U.S. regulatory expectations:
- **U.S. Health Insurance Portability and Accountability Act (HIPAA):** U.S. standards on management of health care data (www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html)
- **Sarbanes-Oxley Act (SOX):** U.S. financial and accounting disclosure and accountability for public companies (www.soxlaw.com)

KNOWLEDGE OF REGULATORY STANDARDS

- **Basel III:** Risk management in banking (www.bis.org/bcbs/basel3.htm)
- **Payment Card Industry (PCI) standards:** Handling and processing of credit cards (www.pcisecuritystandards.org/pdfs/pcissc_overview.pdf)
- **U.S. Federal Information Security Management Act (FISMA):** Security standards for U.S. government systems (www.gsa.gov/portal/content/150159)

KNOWLEDGE OF REGULATORY STANDARDS

- **Committee of Sponsoring Organizations of the Treadway Commission (COSO):** A series of frameworks to help identify factors that lead to fraudulent financial reporting (www.coso.org/Pages/default.aspx)
- **U.S. Supervisory Controls and Data Acquisition (SCADA):** Enhanced security for automated control systems such as those found in the power plants or oil and gas industry (www.dhs.gov/sites/default/files/publications/csd-nist-guidetosupervisoryanddataccquisition-scadaandindustrialcontrolsystemssecurity-2007.pdf)

KNOWLEDGE OF REGULATORY STANDARDS

- **U.S. Fair and Accurate Credit Transaction ACT of 2003 (FACTA):** Legislation to reduce fraud and identity theft (www.ftc.gov/enforcement/statutes/fair-accurate-credit-transactions-act-2003)
- Some regulatory guidelines are not truly laws. For example, PCI is not a law but was developed by the major credit card companies (Visa, MasterCard, American Express, Discover, and JCB) and is referenced in regulatory guidelines such as the *FFIEC Handbook* for best practices for banks.

KNOWLEDGE OF REGULATORY STANDARDS

- Whether a regulation calls out a framework as best practices or is written into the law makes little practical difference.
- The regulator knocking on your door has an expectation of compliance or a very clearly articulated and well-managed reason compliance was not possible.
- Consideration for regulatory requirements is a high priority when planning and scoping an audit.

KNOWLEDGE OF REGULATORY STANDARDS

Guidance Documents

- While regulatory guidance is important, it's typically not comprehensive.
- A challenge with regulatory guidance is that it's often too late!
- Many laws are written in response to an event such as, in the case of information systems - a major breach.
- Enacting laws takes a long time because of public debate, hearings, pressure from special interests, and so on.

KNOWLEDGE OF REGULATORY STANDARDS

Guidance Documents

- Industry norms emerge from the combination of industry guidance documents and regulation guidance.
- These industry guidance documents align to major regulatory requirements and often are more detailed and published more often.
- This is particularly important when a new threat in cybersecurity is identified.

KNOWLEDGE OF REGULATORY STANDARDS

Guidance Documents

- You are not required to know detailed knowledge of each industry guidance but you need to understand what industry guidance is and most importantly the benefits of effectively adopting industry guidance, which include the following:
- Demonstrating to customers compliance with industry best practices
- Demonstrating the ability to adopt lessons learned across the globe

KNOWLEDGE OF REGULATORY STANDARDS

Guidance Documents

- Ensuring that organizations' products and services meet quality and environmental stewardship
- Proving through audits that an organization's systems operate according to accepted norms, as defined by industry standards
- Ensuring that products and services are produced with acceptable consistency
- Reacting quickly to emerging events related to technology defects and breaches

KNOWLEDGE OF REGULATORY STANDARDS

Guidance Documents

- Benefits depend on effectively adopting the industry guidance.
- An important role of an auditor is verifying compliance.
- Some industry standards have certification programs in which an external examiner audits the organization and certifies the organization's compliance with specific industry guidance.

KNOWLEDGE OF REGULATORY STANDARDS

Guidance Documents

- These external examiners are similar to a health inspectors, who ensure that a restaurant meets health codes.
- If an organization passes, it obtains a certification of compliance, which may give it a business advantage or provide evidence to a regulator that it is operating within industry norms.
- The following list of industry guidance, while not exhaustive, is a good sampling of important U.S. industry expectations:

KNOWLEDGE OF REGULATORY STANDARDS

Guidance Documents

Control Objectives for Information and Related Technologies (COBIT):

- COBIT was first published in 1996 as one of the first definitive guides for IS auditors. COBIT has evolved into a globally accepted framework, providing an end-to-end business view of the governance of enterprise IT.
- COBIT 5 is the latest version and is considered a framework that embodies global thought guidance for information systems audit, assurance, and control functions.

KNOWLEDGE OF REGULATORY STANDARDS

Guidance Documents

- **International Organization for Standardization (ISO):** Since 1987 the ISO has created a series of international standards that define and structure a company's management systems.
- These standards are rigorous, and obtaining certification is not easy. While they cover multiple industries, they often are referred to in manufacturing.
- The standards cover design, manufacturing, production, purchasing, quality control, packaging, handling, storage, shipping, and customer service.

KNOWLEDGE OF REGULATORY STANDARDS

Guidance Documents

- **National Institute of Standards and Technology (NIST) standards:** NIST, a unit of the U.S. Commerce Department, issues a number of technology-related standards.
- Most notably, in 2014 the U.S. government issued a NIST Cybersecurity Framework.
- Initially this framework only applied to U.S. government systems, but today the NIST Cybersecurity Framework has been widely adopted by banking and other industries.

KNOWLEDGE OF REGULATORY STANDARDS

Guidance Documents

- **Federal Information Processing Standards (FIPS):**
- FIPS is a set of U.S. government standards that describe document processing, encryption algorithms, and related information technology standards for use in non-military U.S. government agencies.
- Government vendors and contractors who work for government agencies must comply with FIPS.

Auditing Compliance with Regulatory Standards

- The growing dependence on automated IT systems to store and transmit data has driven the creation of many compliance rules and regulations. An auditor's role is to evaluate the design and operation of internal controls.
- Most organizations want to do the right thing and are interested in proper controls. They might be overwhelmed by the day-to-day demands of business. However, it is very important for auditors to verify their compliance.

Auditing Compliance with Regulatory Standards

- The process of verifying regulatory compliance is highly structured and detailed.
- The results may have to be presented to a regulator to demonstrate due care. Most organizations must comply with many different laws and legal requirements, and this has an impact on an audit.
- An organization must be aware of these laws and regulations and must have evidence that the organization's controls demonstrate compliance.

Auditing Compliance with Regulatory Standards

1.The following is a step-by-step high-level procedure for verifying regulatory compliance:

Based on the industry and jurisdiction locale in which the organization operates, keep an inventory of laws, rules, and regulations that the organization must adhere to.

2. Review the specific laws and regulations with which the organization must be compliant.

Auditing Compliance with Regulatory Standards

3. Determine whether the organization's policies and procedures and controls reflect these laws and regulations.

4. Determine whether identified standards and procedures adhere to regulatory requirements.

5. Determine whether the employees are adhering to specified standards and procedures or whether discrepancies exist.

Knowledge of Business Processes

- Knowledge of the business and related processes is needed throughout an audit, from planning, examination, and reporting through follow-up.
- This business knowledge provides the filter and context by which an audit assesses and identifies issues.

Knowledge of Business Processes

- Although you might not think of scuba diving when discussing auditing, the two are actually similar.
- They both follow standards and guidelines.
- No one who has ever gone diving would consider jumping into the ocean without checking the oxygen tank or performing other basic safety checks.

Knowledge of Business Processes

- Auditing is similar, in that you cannot just show up at a site and announce that you are there to perform an audit.
- Auditing requires a specific set of skills and knowledge.
- For example, an auditor must know when to perform a compliance test or a substantive test and must understand the differences between them.

Knowledge of Business Processes

Compliance tests are used to verify conformity

Substantive tests verify the integrity of claims.

What does it mean to *verify conformity*?

- It means that an audit verifies that the proper controls are in place to ensure compliance to a specific standard.
- The compliance test, in essence, makes sure the control is in place.

Knowledge of Business Processes

What does the *integrity of claims* mean?

• It means the controls are actually working.

So in short:

• compliance tests ensure that controls are in place,

and

• substantive tests ensure that controls are working.

Knowledge of Business Processes

- Let’s consider a home inspection company example.
- Say a government program provides first-time home buyers a deeply discounted mortgage rate but requires a home inspection. Consider the following questions and answers:

1. What type of audit is it if the auditor assesses that the closing process control of the mortgage includes a home inspection?

2. What type of audit is it if the auditor assesses that the home inspectors are qualified and their inspections are highly accurate?

Knowledge of Business Processes

- *Answer Q1:* Compliance test. The test tells us whether the closing process control is compliant with the intent of the government program.

- *Answer Q2:* Substantive test. The test tells us whether the closing process control is working effectively.

Types of Audits

- A key step in audit planning is to select the type of audit to perform.
- This decision will help drive the scope and determine which audit area will take the lead.
- There are three basic types of audits:

Types of Audits

- **Financial:** A *financial audit* is an audit of financial statements and processes. An IS auditor is typically not involved in a purely financial audit.
- **Integrated:** When a financial audit's scope includes the underlying technology, such as application and network infrastructure, the IS auditor joins the assessment. This type of audit, which covers non-technology (such as financial) controls and technology controls is referred to as an *integrated audit*.

Types of Audits

- One of the major advantages of an integrated audit is that the business is only audited once rather than twice (for example, for financials and for technology).
- **Operational:** An *operational audit* assesses how well the business operations are managed. This includes reviewing the organization's policies, key processes, controls, and operating environment. An example of an operations IS audit is an assessment of data center operations.

Types of Audits

- The various audits together are typically referred to as an *audit program*.
- Each audit program has a specific objective, scope, and predetermined methodology.
- An enterprise's information systems can be audited in many different ways, and each audit program can be customized—for example, a cybersecurity audit versus a data center operations audit versus a compliance audit for a specific regulation. Collectively, the audit programs represent the scope of risk covered by the auditors.

Types of Audits

- A *compliance audit* is a comprehensive review of an organization's adherence to regulatory guidelines.
- IS auditors are playing an increased role in compliance audits today. One reason is that handling, notification, storage, and processing information has emerged as a central theme in many regulations.
- For instance, the Sarbanes-Oxley Act requirements designate that an entity must utilize an IT control framework (such as COBIT) as a foundation for IT systems and processes.
- Health care providers that store or transmit electronic health (e-health) records, such as personal health information (PHI), are subject to HIPAA requirements.

Types of Audits

- A *compliance audit* is a comprehensive review of an organization's adherence to regulatory guidelines.
- IS auditors are playing an increased role in compliance audits today. One reason is that handling, notification, storage, and processing information has emerged as a central theme in many regulations.
- For instance, the Sarbanes-Oxley Act requirements designate that an entity must utilize an IT control framework (such as COBIT) as a foundation for IT systems and processes.
- Health care providers that store or transmit electronic health (e-health) records, such as personal health information (PHI), are subject to HIPAA requirements.

Types of Audits

- An audit program should be defined so that the scope of audit objectives and the scope of procedures are clear.
- The scope and type of testing that occurs may vary depending on how the understanding of risk has changed since the last audit.
- Testing and evaluation of system controls require an auditor to fully understand proper test procedures, which can include the following:

Types of Audits

- Sampling of a population
- Auditing through observation
- Reviewing documentation
- Documenting systems and processes by means of flowcharting
- Examining log files and data record
- Using specialized software packages to examine system parameter files

RISK ASSESSMENT CONCEPTS

- You may think defining risk is fairly straightforward, but virtually every framework changes the definition just enough to introduce more questions and confusion.
- COBIT 5, for example, defines *risk* as “the combination of the probability of an event and its consequence.” This means if you know how likely it is that an event will occur and you know what the impact is if it occurs, then you can understand the risk.

RISK ASSESSMENT CONCEPTS

- Understanding risk is one of the most important steps in audit planning.
- The goal should be to plan an audit that assesses the greatest amount of the risk controllable by the organization.

RISK ASSESSMENT CONCEPTS

- Understanding risk is one of the most important steps in audit planning.
- The goal should be to plan an audit that assesses the greatest amount of the risk controllable by the organization.
- Auditors typically focus on the risks that have the highest impact on an organization. The following table describes the three main risks that are called out by COBIT 5:

RISK ASSESSMENT CONCEPTS

Item	Attributes
Inherent risk	The risk that naturally occurs because of the nature of the business before controls are applied
Control risk	The risk that internal controls will not prevent a material error
Detection risk	The risk that misstatements or possibly material errors have occurred and were not detected

RISK ASSESSMENT CONCEPTS

- The word material appears in control and detection risk. Material is generally defined as an item of significance that has a real impact on the organization.
- For example, a traffic accident that delays your arrival at work may or may not be material. If your late arrival causes you to lose a million-dollar contract because the client gets tired of waiting, then it most likely is material.
- Arriving at the office late and finding that the offer is gone is not material. Understanding of these risks helps you judge whether something is material or not.

RISK ASSESSMENT CONCEPTS

- **Inherent risk:** *Inherent risk* is often described as the risk that exists if no controls have been deployed. Given the nature of a business, what is its susceptibility to making a material error if there are no internal controls? For example, given the nature of driving, would having no speed limits be an inherent risk? Yes!

RISK ASSESSMENT CONCEPTS

- **Control risk:** *Control risk* is often described as a control that is deployed but not working as expected. For example, assume that your car has an airbag only in the steering column. A driver-side collision occurs, and the airbag fails to deploy. There is a risk that the airbag has a defect and also a risk that the design of the airbag is flawed.

RISK ASSESSMENT CONCEPTS

- **Detection and audit risk:** *Detection risk* is often described as a defect in a control going undetected. An *audit risk* is a type of detection risk in which an auditor fails to find a material error or defect in a control.
- Detection risks can also result from an internal failure of a business, such as an inadequate quality assurance program. Detection control risk is often realized when volumes are high. For example, reviewing security logs is an important control. The volume of logs could increase the likelihood that an event is missed and increase the detection risk.

RISK ASSESSMENT CONCEPTS

- **Residual risk:** The *residual risk* is the risk that remains after controls are applied to the inherent risk. This risk is not included in the prior table because it's not directly referenced in COBIT.
- It is however a common term in the industry and an important concept.
- Residual risk in essence is inherent risk minus controls. For example, the inherent risk may be high for driving with no speed limit signs, but that risk becomes greatly reduced when speed limit signs are posted. The risk is further reduced when police presence is visible. It's an important concept that residual risk is reduced by layering controls against the inherent risk.

RISK ASSESSMENT CONCEPTS

- The assessment of what is material is left to the professional judgment of the auditor.
- This includes both *quantitative* analysis and *qualitative* judgment, based on the understanding of the business and the potential for errors and omissions.

RISK ASSESSMENT CONCEPTS

- The concept of *quantitative* analysis involves coming to an objective conclusion based on a series of measurements. The following are some measurements that may be taken related to risk:
- Identifying populations (for example, information assets)
- Valuing the assets (for example, cost to recover)
- Identifying the risks to the assets
- Identifying the likelihood of the risk being realized
- Identifying the cost to the organization of the risk being realized
- Identifying the cost to mitigate the risk

RISK ASSESSMENT CONCEPTS

- A quantitative analysis based on these measurements may conclude that the cost to mitigate such a risk is too high.
- For example, say that the measurements captured indicate that a particular risk is predicted to occur is every three years, the cost to remediate is $100,000 per year, and the recovery cost is $50,000 per event.
- The quantitative analysis may show that it’s not worth the cost to mitigate.

RISK ASSESSMENT CONCEPTS

- A qualitative judgment looks at the broad understanding of the business and asks the question, what might go wrong?
- A qualitative judgment can override a quantitative analysis. In that case, be sure to clearly document the rationale.
- For example, you may be entering a new market and, given the uncertainty and concerns over how the regulators will react, you err on side of caution and remediate the potential risk.

RISK ASSESSMENT CONCEPTS

- When quantitative analysis is not available, then qualitative judgment is used.
- Be careful to avoid overreliance on judgment versus analysis.
- Often a hybrid approach is used, where both methods are applied.
- When both are applied, the quantitative analysis can be used to validate the qualitative judgment.

Risk Management

- Risk management is the practice of identifying risks, assessing them, making a judgment of disposition, and monitoring.
- Many organizations, especially those that operate in regulated industries, have formal risk management programs.

Risk Management

- Risk management follows a defined process that includes the following steps:

1. Implement a formal risk management program.
2. Identify assets.
3. Identify threats.
4. Perform risk analysis.
5. Disposition of risk.
6. Monitor.

Risk Management

- A risk management program often falls under the corporate governance function, such as the chief risk officer.
- It should be a formal program that is supported by senior leadership.
- The risk-management team needs support and funding from senior management and should be led by someone with strong project-management skills.

Risk Management

- Organizations must identify assets and understand their value to the business. For example, Coca-Cola places value on the original formula for Coke and must protect it.
- Assets include people, processes, and technology. It is important not to define assets too narrowly. Any asset that is bought or built has value.

Risk Management

- Depending on the size of the organization, a material threshold should be used.
- For example, a $5,000 copier/fax machine is not material to a billion-dollar corporation.
- But if that asset sits in the chairman’s office, the asset becomes much more valuable.
- Getting the balance right so an inventory can be quickly obtained is the purpose of setting a materiality threshold.

Risk Management

- The identification of threats should be part of both an ongoing refresh of the threat inventory and a threat assessment of each business area at least annually. It should include an exercise that includes senior management.
- Risk analysis is performed using both quantitative and qualitative methods. Regardless of the method used, the idea is to rank threats in some order to determine what requires immediate action.

Risk Management

- Some threats might have the potential for great impact but very little risk. Other threats might present a high level of risk but have very little impact.
- The idea is for the team to identify high-impact, high-risk concerns and focus on those items.
- For example, a company based in Galveston, Texas, would most likely consider a hurricane a high-risk, high-impact item.

Risk Management

- Galveston is no more than 14 feet above sea level, and the Gulf of Mexico is a prime area for strong storms.
- This same approach should be used during audits to ensure that audit time is spent on areas with the highest risks.
- The disposition of risk has changed over the years. For example, immediately following the financial meltdown in 2008, regulators were at times driving for high rates of risk remediation, regardless of cost.

Risk Management

- As risks across the financial industry were demonstrated to be more balanced with the threats, there was some easing on the push for massive remediation efforts.
- Remember that there is a difference between a threat and a risk. A *threat* is something that can happen to create a negative impact, such as a malware attack. A *risk* is the outcome of the threat, such as an online shopping website being shut down.

Risk Management

- After identifying high-risk, high-impact concerns, the risk-management team can move on to the risk mitigation or risk disposition phase. Risk can be disposed of in the following ways:

Risk Management

- **Avoiding risk (also referred to as *risk avoidance*):**
- Avoiding risk can seem like a simple alternative:
- You simply don’t perform the activity that allows the risk to be present.
- In reality, many activities cannot be avoided.
- Even when they can be, an opportunity cost might be involved so that avoiding the risk involves missing the opportunity for profit.

Risk Management

- **Reducing risk (also referred to as *risk reduction*):**
- Reducing risk is one of the most common methods of dealing with risk.
- Examples include installing a firewall and implementing a new internal accounting control.

Risk Management

- **Accepting risk (also referred to as *risk acceptance*):**
- Risk acceptance means that the organization knows about a risk and makes a conscious decision to accept it.
- Accepting risk means that the company is retaining the potential costs that are associated with the risk.
- For example, a business might be considering building an e-commerce website but has determined that it will face an added risk.
- However, along with the risk is the potential to increase revenue, so the company accepts the risk.

Risk Management

- **Transferring risk (also referred to as *risk transference*):** Transferring risk means placing the risk in someone else's hands.
- A good example of risk transference is insurance.
- Although there are benefits to risk transference, there are also some drawbacks. Chief among them is that insurance is an ongoing expense.
- In addition, it is time-consuming and costly to document and settle relatively small losses.
- Finally, even small payouts by the insurance company can have an adverse effect on future insurance costs.

Risk Management

- The monitoring of the portfolio of risks is important. You can think of monitoring as a type of change management.
- Any time a change is made to systems or the operating environment, a reassessment should be performed to see how the changes affect a potential risk.
- Risk analysis is a powerful tool in the hands of an auditor because it can help identify risks and threats. It also aids the auditor in examining existing controls to determine their effectiveness and helps the auditor focus his or her efforts on a high-risk, high-impact area.