The Information Systems Audit

INFO 6008 Week 4

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.

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

- Business is all about risk and reward. Executives are required to weigh the benefits of investments with the risks associated with them.
- As a result, most have become quite adept at measuring risk through ROI analyses, key performance indicators, and a myriad of other financial and operational analysis tools.
- To be successful in managing organizational IT risk, you should understand that executives view risk in financial terms.
- As a result, some kind of financial analysis is normally required to make a business case for an investment in additional controls.

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

- Security teams are faced with too much to do and not enough time, money, or skilled resources to adequately address issues. Since you can only accomplish so much in a given period, how do you prioritize the many different tasks that could be done? The answer is to follow a methodical, risk-based approach with business-focused outcomes.
- This ensures that your decisions become more defensible in case something bad happens. By showing all the effort that went into your business-based decision-making process on where you decided to accept and mitigate risk, you will turn the attention from finger-pointing to restoring the business back to normal operations while improving the risk management process going forward.

Risk Management

- Risk management is a team effort. Executive oversight, sponsorship, and involvement are critical to getting the right business perspective and necessary support.
- Companies with mature risk management programs usually have a cross-functional risk governance board or steering committee composed of representatives from across the various business units and support groups.
- They provide input and guidance on risk evaluations and control priorities, since they are ultimately responsible for the data in their respective business units.

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

- Risk can be analyzed in two ways: quantitatively and qualitatively. Like anything else, each has advantages and disadvantages.
- The quantitative approach is more objective and expresses risk in financial terms that decision makers can justify. With the right data, it can provide more accurate cost and benefit information. The main challenge is that the right data is often unavailable.
- For example, many studies using scientifically controlled experiments have been conducted to quantitatively measure the safety impact of the use of seat belts in automobile accidents. The same cannot be said for antivirus software. If you use antivirus software on your company computers, how much do you reduce the risk of your company being a victim of a cyber attack?

Risk Management

- We inherently know it reduces the risk, but it is difficult to quantify. In addition to a lack of actuarial data, the quantitative approach is more complex and time consuming, requiring mathematical formulas. As a result, it is often reserved for conducting an analysis of a specific subset of the organization or performed at an individual project level.
- The qualitative approach is better suited for larger-scale risk analysis, and it provides a stratified view of risk. Since qualitative analysis uses common terminology and scales like high, medium, and low to express risk, it is a much easier and cheaper process to implement. The main drawback is that the results are mostly subjective and therefore difficult to substantiate.

Risk Management

- Users of qualitative risk analysis often spend a great deal of time defending their results.
- With so much room for interpretation, qualitative analysis may not provide the definitive answers needed to make appropriate decisions.
- The organizations with more successful risk management programs tend to blend the two approaches by relying more heavily on qualitative risk analysis to identify areas of focus and then using quantitative risk analysis techniques to justify specific risk mitigation expenditures.

Risk Management

- QUANTITATIVE RISK ANALYSIS
- With few exceptions, whether related to financial, physical, or technological resources, different types of risk can be calculated using the same universal formula. Risk can be defined by the following calculation:
- Risk = asset value × threat × vulnerability

Risk Management

- Elements of Risk

Risk comprises three elements:

- *asset value,*
- *threat,*
- *vulnerability*.

Estimating these elements correctly is critical to assessing risk accurately.

Risk Management

- Elements of Risk

Assets

- Normally represented as a monetary value, *assets* can be defined as anything of worth to an organization that can be damaged, compromised, or destroyed by an accidental or deliberate action.
- In reality, an asset's worth is rarely the simple cost of replacement; therefore, to get an accurate measure of risk, an asset should be valued taking into account the bottom-line cost of its compromise.

Risk Management

- For example, a breach of a customer's credit card information would initially result in a monetary loss necessary to cover all the costs associated with replacing the compromised credit card with a new one.
- If a large volume of credit card records were compromised, the incident would likely result in a lengthy incident response and investigative effort, legal action, damage to the company's reputation, and regulatory penalties.
- The cumulative effect of these consequences would cause a significant financial loss. In this case, the asset-value portion of the equation would represent the credit card information. The calculated value of the personal information would include an estimate of the cumulative dollar cost of the incident response and investigative activities, legal action, reputation damage, and regulatory penalties.

Risk Management

- Threats
- A *threat* can be defined as a potential event that, if realized, would cause an undesirable impact. The undesirable impact can come in many forms, but it often results in a financial loss. Threats are generalized as a percentage, but two factors play into the severity of a threat: degree of loss and likelihood of occurrence. The *exposure factor (EF)* is used to represent the degree of loss.
- It is simply an estimate of the percentage of asset loss if a threat is realized. For example, if we estimate that a fire will cause a 70 percent loss of asset value if it occurs, the exposure factor is 70 percent, or 0.7.

Risk Management

- The *annual rate of occurrence (ARO)*, on the other hand, represents the likelihood that a given threat would be realized in a single year in the event of a complete absence of controls.
- For example, if we estimate that a fire will occur every 3 years, the annual rate of occurrence would be 33 percent, or 0.33. A threat, therefore, can be calculated as a percentage by multiplying the exposure factor by the annual rate of occurrence. Given the preceding example, the threat of fire would result in a value of 23.1 percent, or 0.231.

Risk Management

- Vulnerabilities
- *Vulnerabilities* can be defined as the absence or weakness of cumulative controls protecting a particular asset. Vulnerabilities are estimated as percentages based on the level of control weakness.
- We can calculate *control deficiency (CD)* by subtracting the effectiveness of the control by 1 or 100 percent.
- For example, we may determine that our industrial espionage controls are 70 percent effective, so 100 percent – 70 percent = 30 percent (CD). This vulnerability would be represented as 30 percent, or 0.3.

Risk Management

- IT Risk Scenario
- The IT audit director at a national retailer has determined that the legal climate is changing in relation to the credit card information with which the company is entrusted. Until now, the company had not considered the risk of a disclosure of its customers' personal or credit card–specific information.
- After interviewing public relations, legal, and finance stakeholders, the IT audit director estimates the cost of a single breach to be approximately $30 million in lost revenues, legal costs, and regulatory consequences. So we now know that the asset is personal credit card and associated financial information.

Risk Management

- Furthermore, its value to the company is $30 million. Since several breaches that involved hacking have recently been reported in the news, the audit director decides to explore this threat. In a conversation with the information security director, the audit director learns that the company is under constant attack, although most of the attacks are nothing more than probes for vulnerabilities.
- He estimates that about one actual attack per week occurs and that a compromise of the credit card–processing system would result in a complete asset loss.

Risk Management

- The information security director estimates that current controls are 99.99 percent effective, but if the company does not invest in additional controls, a successful breach is imminent.
- Given this information, we can calculate the risk of an external security breach to be $30 million [asset value] × 100 percent loss (EF) × 52 hacking attempts per year (ARO) [threat] × 0.01 percent or 0.0001 control deficiency (CD) [vulnerability] = $156,000 [risk].

Risk Management

- Common Causes for Inaccuracies
- Most risk analyses attempted today result in bottom-line estimates that are way off the mark. Unfortunately, when organizational management loses faith in the risk information that is presented to it, it tends to dismiss a disproportionate number of requests for risk mitigation investments.
- Management is interested in investing limited resources in areas that either will make the organization money or will save the organization money. This is why it is so important that you present a solid analysis of risk whenever approaching management for additional resources.

Risk Management

- Following are the most common causes of risk analysis inaccuracies.
- **Failure to Identify Assets, Threats, or Vulnerabilities**
- The most common cause of inaccuracies in the risk analysis process is the failure to properly identify assets, threats, and vulnerabilities. This is mostly due to the fact that most organizations do not use a formal risk management process and practitioners have not been trained to analyze risk. You would be surprised at how poorly organizations track and manage assets from computer hardware to software applications.

Risk Management

- Virtual machines are software programs that emulate entire computer systems, meaning a company could have hundreds of virtual computer systems running on just a handful of actual physical machines.
- The problem is exacerbated by cloud providers, since any employee with a credit card can purchase hardware (Infrastructure as a Service, “IAAS”), software (Software as a Service, “SAAS”), and even entire business platforms (Platforms as a Service, “PAAS”) from service providers like Microsoft or Amazon and leverage them with the use of a web browser.

Risk Management

- It is even more difficult to identify threats and vulnerabilities because they are dynamic in nature and growing exponentially. We know that new variants of malware are introduced daily. Hacking software has grown more sophisticated to bypass traditional countermeasures.
- Exploit kits are specially designed applications that automate the process of attacking computer systems, alleviating the need to have deep technical knowledge of computer systems and programming techniques, allowing even novice hackers to wreak havoc on organizations. Additionally, new computer-related vulnerabilities are discovered almost daily.

Risk Management

- Although identifying and tracking threats and vulnerabilities is difficult, there are many resources where you can get help, such as information security alerts from CERT, Bugtraq, and other free and subscription-based security vulnerability notification services.
- Hardware and software vendors usually offer notification services of new releases designed to fix vulnerabilities in their products. A new cybersecurity offering called “threat intelligence services” has become almost a necessity for organizations.
- These services provide timely information on specific threats targeting a given industry or specific company.

Risk Management

- Even the U.S. government is partnering with industries to address the growing cybersecurity threats. Special industry consortiums have been created called Information Sharing and Analysis Centers (ISAC) where information on threats and attacks is freely shared among competitors in a given critical infrastructure industry, like the financial sector and with the U.S. government.
- IT auditors also can examine security incidents when they are publicized to learn how such violations occur. One Internet resource that consolidates and chronicles information about security incidents is www.privacyrights.org/ar/ChronDataBreaches.htm.

Risk Management

- Inaccurate Estimations
- Unfortunately, a fair amount of estimation is involved in analyzing risk, which makes it an inexact science. Many errors can be attributed to this fact.

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.

AUDITING AND THE USE OF INTERNAL CONTROLS

- An enterprise uses controls to comply with internal policies, meet regulatory expectation, and reduce the level of risk to a tolerable threshold.
- All business involves risk. Anyone who gets in a car in the morning to go to work takes a risk of a traffic accident. The question is one of risk and reward.
- So long as the reward outweighs the risk, a business can generally be successful. The key is to deploy the right type of controls to reduce risk to an acceptable level, which is sometimes referred to as a *risk tolerance*.

AUDITING AND THE USE OF INTERNAL CONTROLS

- Management might give an auditor a general control objective to review during the audit, but the primary goal is to verify the confidentiality, integrity, and availability (CIA) of information resources.
- Assuring compliance is also important.
- Compliance reviews are an integral part of any IT auditor job.
- Audited systems must meet regulatory and legal requirements while assuring compliance.

AUDITING AND THE USE OF INTERNAL CONTROLS

- Recall Substantive Testing ensures that controls are working.
- As such how much substantive testing is required depends on the level of internal controls and the amount of confidence the auditor has in the operation of the internal control structure.
- IS audits that examine systems with a large number of internal controls that have high confidence lower the number of required substantive tests.

AUDITING AND THE USE OF INTERNAL CONTROLS

- Management uses internal controls to exercise authority and effectively manage the organization.
- Controls typically start with high-level policy and apply to all areas of the company.
- IS auditors are interested in IS controls because they are used to verify that systems are maintained in a controlled state.
- IS controls should protect the integrity, reliability, and accuracy of information and data.

AUDITING AND THE USE OF INTERNAL CONTROLS

- Management uses internal controls to exercise authority and effectively manage the organization.
- Controls typically start with high-level policy and apply to all areas of the company.
- IS auditors are interested in IS controls because they are used to verify that systems are maintained in a controlled state.
- IS controls should protect the integrity, reliability, and accuracy of information and data.

AUDITING AND THE USE OF INTERNAL CONTROLS

Properly implemented IS control objectives should:

- guarantee efficiency and effectiveness
- protect the organization against outages
- provide for an effective incident response.

As mentioned before, these controls filter down the organizational structure by means of policy and procedure. These procedures can be divided into two categories:

1. general control procedures
2. IS control procedures.

AUDITING AND THE USE OF INTERNAL CONTROLS

- General control procedures are established by management to provide a reasonable amount of assurance that specific objectives will be achieved.
- The following table describes a sampling of general control procedures and IS control procedures.

AUDITING AND THE USE OF INTERNAL CONTROLS

General Control Procedures	Examples of Information System Control Procedures
Internal accounting controls used to safeguard financial records	Procedures that provide reasonable assurance for the control of database administration cannot impact financial statements.
Operational controls that are focused on recovery of day-to-day activities	Business continuity planning (BCP) and disaster-recovery procedures that provide reasonable assurance that the organization is secure against disasters. (BCP covers all critical areas of the organization and is not exclusively an IS control.)
Administrative controls designed for corporate compliance	System-development methodologies and change-control procedures implemented to protect the organization and maintain compliance.

AUDITING AND THE USE OF INTERNAL CONTROLS

General Control Procedures	Examples of Information System Control Procedures
Procedures that safeguard access and use of organizational resources	Procedures that provide reasonable assurance for the control of access to data and programs.
Logical security policies designed to support proper transactions	Procedures that provide reasonable assurance for the control and management of data-processing operations.
Logical security policies designed to support transactional audit trails	Procedures that provide reasonable assurance for the control of networks and communications.
Security policies that address the physical control of data centers	Physical access control procedures that provide assurance for the organization's safety.

AUDITING AND THE USE OF INTERNAL CONTROLS

- Controls can be preventive, detective, or corrective.
- Regardless of how well controls are designed, they can provide only reasonable assurance.
- Using the three types of controls in conjunction with each other creates a system of checks and balances.
- Keep in mind that no system is perfect, and controls will always be subject to error due to breakdowns or system overrides or even employees or outsiders.

AUDITING AND THE USE OF INTERNAL CONTROLS

Class	Function	Example
Preventive	Prevents problems before they occur	Access control software that uses passwords, tokens, and/or biometrics
Detective	Senses and detects problems as they occur	Security logs
Corrective	Reduces the impact of threats and minimizes the impact of problems	Backup power supplies

AUDITING AND THE USE OF INTERNAL CONTROLS

- The key difference between preventive, detective, and corrective controls is in how a threat is handled.
- A preventive control stops a threat immediately.
- A detective control identifies a threat after the fact.
- A corrective control tries to remediate risk of a threat after the fact.

THE AUDITING LIFE CYCLE

- An audit can be defined as a planned, independent, and a documented assessment to determine whether agreed-upon requirements and standards of operations are being met.
- An audit it is a review of an operation and its activities.
- An IS audit deals specifically with the technology used for information processing.

THE AUDITING LIFE CYCLE

- An auditor is responsible for reporting the facts and providing an independent review of the technology and manual systems.
- As an auditor, you are in a position of *fiduciary* responsibility, which means you hold a position of special trust and confidence.

Audit Methodology

- The purpose of an IS audit is to evaluate controls against predetermined control objectives.
- For example, an operational control objective might be used to ensure that funds accepted on the company's e-commerce website are properly posted in the company's bank account.
- However, in an IS audit, the objective might be expanded to make sure that dollar amounts are entered correctly into the e-commerce website and that they match the posted prices of the items being sold.

Audit Methodology

An *audit methodology* is a documented approach for performing an audit in a consistent and repeatable manner. The audit methodology is designed to meet audit objectives by defining the following:

- A statement of work
- A statement of scope
- A statement of audit objectives

Audit Methodology

- The methodology should be approved by management and thoroughly documented so that it provides a highly repeatable process.
- The audit methodology is an important educational tool for avoiding surprises during an audit.
- All audit employees must be trained and must have knowledge of the methodology.

The Auditing Life Cycle Steps

- Using a structured and repeatable methodology allow the establishment of boundaries and builds confidence in the audit process.
- The steps of the audit process are described in greater detail here:

1. Audit subject: Identify which areas are to be audited, based on risk.

2. Audit objective: Define why the audit is occurring. For example, the objective of an audit might be to ensure that access to private information, such as Social Security numbers, is controlled.

The Auditing Life Cycle Steps

3. Audit scope: Identify which specific functions or systems are to be examined.

4. Pre-audit planning: Identify what skills are needed for the audit, how many auditors are required, and what other resources are needed. Necessary policies or procedures should be identified, as should the plans of the audit. The plans should identify what controls will be verified and tested.

5. Data gathering: Identify interviewees, identify processes to be tested and verified, and obtain documents such as policies, procedures, and standards. Develop procedures to test controls.

The Auditing Life Cycle Steps

6. Evaluation of test results: Results will be organization specific. The objective is to review the results.

7. Communication with management: Document preliminary results and communicate them to management.

8. Preparation of audit report: Ensure that the audit report is the culmination of the audit process and might include the identification of follow-up items.

Chain of Custody and Evidence Handling

Chain of custody is an important issue that cannot be overlooked during an audit—especially one that may be litigated.

To show chain of custody, an auditor must be able to:

- account for who had access to the collected data
- ensure that the access to the information was controlled
- show that it has been protected from tampering

Chain of Custody and Evidence Handling

For example maintaining the chain of custody when say a server was breached; and there is a log file of the user accounts that were logged into a server at the time of the breach.

That log file could be captured and preserved by being written to write-once media.

The write-once media could indicate when the log file was captured and ensure that evidence cannot be altered.

In addition, the evidence would need to be locked up so that from the point when the evidence was captured to the point it is used in court, there is proof that the evidence could not have be altered.

Chain of Custody and Evidence Handling

- *Evidence handling* refers to the auditor handling any information obtained during the audit.
- Evidence can be obtained from interviews, work papers, direct observation, internal documentation, compliance testing, and/or substantive testing.
- All evidence is not created equal; some evidence has more value and provides a higher level of confidence than other forms.
- Evidence the auditor obtains should be sufficient, usable, reliable, and relevant, and it should achieve audit objectives effectively.

Chain of Custody and Evidence Handling

- This is sometimes referred to as the SURRE rule:
- **S**ufficient
- **U**sable
- **R**eliable
- **R**elevant
- **E**ffective

Chain of Custody and Evidence Handling

- You should be aware of ISACA standards for auditing and understand how evidence can be used to support any findings.
- The ISACA website(www.isaca.org) provides both standards and guidelines related to evidence handling:
- IS Audit and Assurance Standard 1205 on Evidence
- IS Audit and Assurance Guideline 2205 on Evidence
- The following table lists some basic questions to answer in determining the reliability of evidence:

Chain of Custody and Evidence Handling

Question	Description
Is the provider of the evidence independent?	Evidence from inside sources is not considered as reliable as evidence obtained from outside sources.
Is the evidence provider qualified?	The person providing the evidence has to have his or her qualifications reviewed to validate his or her credibility.
How objective is the evidence?	Some evidence requires considerable judgment; other evidence (such as dollar amounts) is easy to evaluate.
When is the evidence available?	Backups, the write process, and updates can affect when and how long evidence is available.

Evidence Handling

Auditors should observe auditees in the performance of their duties to assist in gathering evidence and understanding how procedures, job roles, and documentation match actual duties. Auditors should perform the following:

- Observe employee activity
- Examine and review procedures and processes
- Verify employee security awareness training and knowledge
- Examine reporting relationships to verify segregation of duties

Automated Work Papers

- An important part of auditing methodology is documentation.
- Findings, activities, and tests should be documented in work papers (WPs), which can be either hard copy or electronic documents.
- Since WPs are created and stored, they must be properly dated, labeled, and detailed; clear; and self-contained.
- ISACA IS auditing standards and guidelines detail specifications that pertain to WPs.
- WPs are subject to review by regulators.

Automated Work Papers

- Auditors are aware of the importance of the control of WPs; these same controls must be provided for automated WPs.
- Controls that protect the confidentiality, integrity, and availability of electronic WPs should be applied at the same level as their paper-based counterparts.
- Some items to consider:
- Encryption to provide confidentiality
- Backups to provide availability
- Audit trails and controls
- Access controls to maintain authorized access

Automated Work Papers

- Remember that accountability for maintaining confidentiality of paper, electronic, and sensitive client information **rests with an auditor**.
- **Sensitive information should always be protected**.

Computer-assisted audit techniques (CAATs)

- In recent years audit teams have moved to simplifying and automating the audit process.
- Although auditors word processors and spreadsheet programs have been in use for quite some time, audit teams are moving to more advanced methods for automating WPs.
- Computer-assisted audit techniques (CAATs) are one example of this. CAATs are software audit tools used for statistical sampling and data analysis.

Computer-assisted audit techniques (CAATs)

- An area of particular interest to auditors is sampling using software.
- What do you do when you cannot test an entire population or a complete batch?
- You use sampling—a process of selecting items from a population of interest.
- The practice of sampling can give the auditor generalized results for the population as a whole. There are two basic types of audit sampling:

Computer-assisted audit techniques (CAATs)

1. **Statistical sampling:** This type of sampling is based on probability. Every item in the population has a known chance of selection. The prominent feature of statistical sampling is its capability to measure risk and the use of quantitative assessment. An auditor quantitatively determines the sample size and confidence level.
2. **Nonstatistical sampling:** This type of sampling involves using auditor judgment to select the sample size and determine which items to select. Nonstatistical sampling is also known as *judgmental sampling*.

Computer-assisted audit techniques (CAATs)

Each sampling type, statistical and nonstatistical, has two subgroups of sampling techniques:

- **Variable sampling:** Variable sampling is used primarily for substantive testing. It measures characteristics of the sample population, such as dollar amounts or other units of measurement.
- **Attribute sampling:** Attribute sampling is used primarily for compliance testing. It records deviations by measuring the rate of occurrence that a sample has a certain attribute. Attribute sampling can be further divided into three subcategories:

Computer-assisted audit techniques (CAATs)

- Attribute sampling can be further divided into three subcategories:

1. **Frequency estimating sampling:** Answers the question “How many?”
2. **Stop-and-go sampling:** Used when it is believed that few errors exist
3. **Discovery sampling:** Used to discover fraud or irregularities

Sampling and ongoing monitoring

Sampling is not the only way to ensure compliance.

Ongoing monitoring might be required.

One ongoing monitoring method is to use *embedded audit modules*.

Embedded modules are designed to be an integral part of an application and are designed to identify and report specific transactions or other information, based on predetermined criteria.

Sampling and ongoing monitoring

- Identification of reportable items occurs as part of real-time processing.
- Reporting can be performed by means of real-time processing or online processing, or it can use store-and-forward methods.
- *Parallel simulation* is another test technique that examines real results that are compared to those generated by the auditor.
- *Integrated test facilities* (*ITFs*) use data that represents fake entities, such as products, items, or departments. ITF is processed on actual production systems.

Audit Closing

- After interviewing employees, reviewing documentation, performing testing, and making personal observations, an auditor is ready to compile the information and provide findings. These findings should be recorded in the audit opinion. The audit opinion is part of the auditor’s report and should include the following components:

Audit Closing

- Name of the organization being audited
- Auditor’s Name, date, and signature
- Statement of audit objectives
- Audit scope
- Any limitations of scope
- Audience
- Standards used in the audit
- Details of the findings
- Conclusions, reservations, and qualifications
- Suggestions for corrective actions
- Other significant events

Audit Closing

- Auditors should always attempt to follow written procedures.
- If procedures are not followed, the auditor must keep documentation on why procedures were not followed and what the findings were.

Report Writing

- After the closing session, typically an auditor has all the information needed to write the audit report.
- The auditor should be clear and unambiguous about which issues should be in the report and the reasoning.
- The audit report language should be equally clear and supported by the evidence obtained.

Report Writing

- An audit report is designed to provide information needed persuade to the audience where corrective action is needed and why.
- An audit report with no major issues is valuable! Such an audit report confirms that the controls in place are working effectively, which means management can spend limited resources elsewhere.
- When issues are raised, a well-written audit report is a call to action for leadership to not only improve control defects but potentially address why it took an auditor to find the control defect.

Report Writing

- When writing an audit report, consider this sampling of best practices:
- **Timely manner:** An audit report issued months after an audit is completed may no longer represent the current state of controls.
- **Report classification:** Be clear on the intended recipients and any restrictions on handling.
- **Key message:** Keep the report centered on the final opinion and key supporting evidence; keep the focus on the results and not on how those results were obtained.

Report Writing

- **Scope clarity:** Be sure the reader knows immediately the scope of the audit and any qualifications, such as the results being limited to compliance tests versus substantive tests.
- **Severity of issues:** A good audit report tells the reader the severity of the issues and opinion in the context of the risk; the audit report tells a risk story and should be compelling.
- **Tech jargon:** Avoid unnecessary technical language. Effective audit reports use simple language to convey powerful ideas.
- **Leverage WPs:** Keep details in the work papers.

THE CONTROL SELF-ASSESSMENT PROCESS

- In an ideal world, any control defect should be identified and remediated through the risk management program.
- One step closer to an ideal state is to identify and remediate control defects through the control self-assessment process, which is when the business participates in a formal self-assessment.

THE CONTROL SELF-ASSESSMENT PROCESS

- Although the traditional approach to auditing has proven itself over the years, it does have some problems, primarily because responsibility for the audit is placed on the auditors.
- Managers and employees might feel that it is an auditor's job to find and report problems.
- Using a *control self-assessment* (*CSA*) is an attempt to overcome the shortcomings of the traditional approach.

THE CONTROL SELF-ASSESSMENT PROCESS

- According to ISACA, the CSA methodology is designed to provide assurance to stakeholders, customers, and employees that internal controls have been designed to minimize risks.
- CSAs are used to verify the reliability of internal controls. Unlike in traditional auditing, some of the control monitoring responsibilities are shifted to functional areas of the business.

THE CONTROL SELF-ASSESSMENT PROCESS

- Because the functional areas are directly involved and play an important role in the design of the controls that protect critical assets, employees tend to be motivated.
- CSAs also tend to raise the level of control, which allows risk to be detected sooner and, consequently, reduces cost.
- The following table outlines the differences between traditional auditing and the CSA approach

THE CONTROL SELF-ASSESSMENT PROCESS

Control Self Assessment	Traditional Auditing
Empowers employees and gives them responsibility	Places responsibility on the auditing staff and management
Offers a method for continuous improvement	Limited by policies and rules and does not involve functional area management or give them as much control
Involves employees and raises their level of awareness	Offers little employee participation
Involves staff and employees and makes them the first line of control	Decreased awareness of staff and employees of internal controls and their objectives

THE CONTROL SELF-ASSESSMENT PROCESS

- The CSA does have drawbacks.
- Some individuals have a misconception that CSAs can replace audits. This is not correct.
- The CSA was not designed to replace the audit function; it was designed to enhance the audit function.
- Some employees might also offer objections because a CSA program places an additional workload on employees.

THE CONTROL SELF-ASSESSMENT PROCESS

- The key to making a CSA program work is to identify what processes are the most important to the department under examination.
- Interviews, meetings with appropriate business unit employees, and questionnaires are some of the methods used to identify key processes.
- COBIT 5 under the Monitor and Evaluation Section documents the CSA control objectives (referred to as COBIT 5 ME2.4) and provides related material for CSA.

CONTINUOUS MONITORING

- Both the speed of transactions and the volume of accompanying data have exploded in recent years.
- Changes in technology result in quicker transactions, and the need for instant information has grown.
- *Continuous monitoring* can help meet the demand. Continuous monitoring allows an auditor to program certain control tests.
- It can alert an auditor to a potential threat or control breakdown.

CONTINUOUS MONITORING

- Continuous monitoring is not itself an audit. When a potential threat or control breakdown is detected through continuous monitoring, further examination through an audit is typically required.
- This is the same as a doctor finding an abnormality in an X-ray and wanting to run further tests to understand more.
- Continuous monitoring works well for automated processes that capture, manipulate, store, and disseminate data.

CONTINUOUS MONITORING

- Research produced by the American Institute of Certified Public Accountants and the Chartered Professional Accountants of Canada found that six preconditions should be present before an organization can adopt continuous auditing:

1. The system must have acceptable characteristics. Cost and factors such as technical skill must be considered.

2. The information system must be reliable, have existing primary controls, and collect data on the system.

CONTINUOUS MONITORING

3. The information system must have a highly automated secondary control system.

4. The auditor must be proficient in the system and information technology.

5. The audit process must offer a reliable method for obtaining the audit procedure results.

6. Verifiable controls of the audit reporting process must exist.

CONTINUOUS MONITORING

There are challenges in implementing a continuous monitoring program.

It is important to allocate the appropriate amount of time and effort for the development of a continuous auditing environment.

Auditors need to acquire the skills for this program to meet the demands of the changing audit environment.

.

QUALITY ASSURANCE

The core concept of quality assurance (QA) is to improve two key attributes:

- quality
- adherence.

In both cases, you need to measure the QA results with a yardstick.

In other words, QA needs a definition of quality and adherence.

QUALITY ASSURANCE

- The QA process tests transactions against the quality and adherence yardsticks. Deviations are typically reported to the business for remediation.
- At a minimum, adherence should mean adherence to the organization’s standards. Consequently, adherence expectations should be well defined and easier than quality to measure.
- When regulatory obligations are added into an organization’s standards, adherence to the standards results in adherence to regulatory obligations.

QUALITY ASSURANCE

- If quality expectations are baked into standards, adherence to those standards can drive improvement in quality.
- If they are not defined in standards, then separate testing is needed through the QA program.
- Defects identified and corrected through a QA program are generally not considered an audit issue.
- This is because the QA process is a control specifically designed to catch and remediate defects.

QUALITY ASSURANCE

- As long as the defect rate stays at acceptable levels, the QA process is working as it is designed to work.
- An auditor's interest in the QA process should be to perform testing of the controls to ensure that the program is well designed and effective.
- The QA process is audited as any other process, starting with understanding the intent and overall design.
- The QA process would most likely result in an operational audit that includes both compliance and substantive testing.

THE CHALLENGES OF AUDITS

- It is important to keep in mind that an auditor's presence disrupts the normal operations of the business and can make staff feel uncomfortable.
- Individuals may take an audit personally and consider it a grading of their work.
- Some individuals may perceive a negative outcome of an audit to reflect their competency and to have a negative impact on their career.

THE CHALLENGES OF AUDITS

- Many of these fears are unwarranted.
- An auditor must overcome any unwarranted perceptions and demonstrate confidence.
- A smart, experienced auditor does not waste people's time and makes a point to ask relevant questions.
- The better the auditor knows the business and can ask insightful and deep questions, the more likely it is that the business will have confidence in the audit.

THE CHALLENGES OF AUDITS

- An audit is successful when the business recognizes that the auditor has no agenda beyond finding risk exposures that could help avoid business disruptions or losses.
- This perception of value is not always shared by a control owner who has a defect identified through an audit.
- The reactions can range from reluctant admission to lukewarm denial to borderline threats of complaints about the auditor to management.
- Police officers are not often thanked for issuing speeding tickets, but those tickets inevitably save some lives!

Communicating Results

- The best way to avoid surprises is to *communicate frequently* to the stakeholders of an audit.
- A common pitfall is waiting until the end of an audit to communicate any major issue.
- It’s highly effective to communicate interim observations to the control owner, who can provide supplemental evidence if necessary.

Communicating Results

- When the examination concludes, an auditor needs to be clear and concise about the type of opinion that will be reported.
- An auditor looks at the controls, the findings, and the supporting evidence in the context of all the material respects of the design and operational control procedures tested.
- The auditor then forms an opinion, in one of four possible categories:

Communicating Results – Audit Opinion Categories

Opinion Category	Description
Unqualified opinion	Testing and obtained evidence are complete and persuasive.
Qualified opinion	Appropriate testing and obtained evidence exist that cite instances of control weaknesses but the opinion cannot conclude that the control weakness is pervasive.
Adverse opinion	Multiple significant deficiencies add up to a material and pervasive weakness.
Disclaimer	An auditor cannot obtain appropriate evidence on which to base an opinion.

Communicating Results

- These opinions can be applied to either an entire audit report or a specific finding.
- For example, say that you have 10 findings, of which 9 are unqualified in that the evidence and testing obtained are clear and persuasive.
- Now assume the tenth issue is qualified because the test results are just not clear in terms of the extent to which the control weakness exists.

Communicating Results

- At this point, an auditor has a few choices, depending on the nature of the issues found.
- The auditor could drop the tenth issue from the report and issue the entire report as an unqualified opinion.
- Alternatively, the auditor could issue the report as qualified and clearly state that the tenth issue indicates a concern that may not be fully understood.

Communicating Results

- Many organizations determine an audit report opinion based on the scope, number, and severity of risks found.
- These audit rating labels can vary greatly. For example, a simple rating scheme for audit reports could be *unrated*, *satisfactory*, and *unsatisfactory*, based on the following mapping to opinion categories:
- **Unrated report:** Some findings disclaimed
- **Satisfactory report:** A low volume of qualified or unqualified findings
- **Unsatisfactory:** Any adverse opinion

Negotiation and the Art of Handling Conflicts

- Negotiations start when an auditor starts communicating to stakeholders observations or findings.
- An auditor can expect disagreements. The key obligation of an auditor is to ensure that any observation or finding is fact based and fair and that the conclusion is reasonable, given the obtained evidence.
- Reaching consensus may not always be possible.

Negotiation and the Art of Handling Conflicts

- When stakeholders want to challenge and negotiate, their arguments typically fall within three possible areas of disagreement:

1. The finding itself: Are the facts accurate and complete?

2. The severity of the finding: Is the risk well calculated?

3. The process by which the finding was identified: Was the testing fair and unbiased?

Negotiation and the Art of Handling Conflicts

- It’s important for an auditor to review the facts and evidence from the client perspective for gaps or inconsistencies.
- An audit that is well prepared with facts and a well-documented audit program can be very persuasive.
- Conflict can be handled by staying calm and letting the audit process and results speak for themselves.
- When you have a sound audit process, your observations (that is, findings) will be strong.
- As a result, many conflicts and negotiations focus on the severity and the aggregated risk as the point of disagreement.

Negotiation and the Art of Handling Conflicts

- The best way to negotiate and cut down the disagreements is to make an audit report relevant to the business.
- Relevance is critical for stakeholder satisfaction.
- Focus the interim discussions on each individual finding to ensure that it is factual.
- As the audit begins to wind down, the negotiation focus will shift to the severity.
- The overall audit report rating is typically reserved for discussion with senior leaders..

Negotiation and the Art of Handling Conflicts

- Discussing the overall rating with key stakeholders (such as the control owner) will help drive awareness and provide an opportunity for senior leaders to negotiate any concerns with the report's wording.
- **Any audit report rating is typically not open to negotiation.**
- Once the facts have been verified, an auditor must issue an independent opinion.
- Independence is not only the concern of the auditor but also of senior management, who need an independent view of their control environment