

IT Audit Seminar

IS Audit Basics



IT Auditing



This slide deck expands our look at fundamental internal audit concepts

Agenda

- Types of IS Audits
- SEC, PCOAB, and the Rise of Internal Control Auditing
- Assertions, Attestation, and Auditing – e.g., IUC reviews
- IS Governance vs. Management
- Types of controls


Auditing is all about risk

This slide deck will build on previous materials with an emphasis on how an auditor assesses whether or not IS controls are effectively mitigating risk

College of Business

Types of IS Audits

- Generally done by public auditing firms:
 - Evaluate IS internal controls in support of a financial audit
 - Compliance audits (e.g., PCI audits)
 - Service organization audits
 - Agreed-upon procedures (e.g., due diligence assessments)
- Internal audits



3

Hint: there are some testable details here...

Information systems auditing is a constantly changing field with a wide variety of opportunities

Internal control effectiveness is evaluated in financial audits

- Required! Audits today are expected to be “integrated audits” where financial numbers, the internal control systems that ensure correct numbers, and the related information systems are “in scope”
- Public companies are required to make assertions about the effectiveness of their internal control systems and present audit findings that evaluate those assertions
- If the internal controls (mostly information system-related) fail, auditing the financial statements becomes more expensive

Compliance audits verify that an organization meets some designated standard; Examples:

- **PCI – Payment card industry** standards apply to organizations that accept credit cards; if you don’t meet them, you either pay more for each charge or you are not allowed to accept credit card payments; auditors verify compliance
- Organizations that accept money from grants may be subject to audit
- Healthcare providers have to comply with **HIPAA the Health Insurance Portability and Accountability Act of 1996** organizations often perform self-audits to ensure they are in compliance

SOC (System and Organization Controls) – formerly Service Organization Controls – audits are chartered by service organizations (e.g., payroll services, cloud vendors, email providers, etc...) to evaluate and report on the effectiveness of their internal control

- If your provider accidentally releases protected information, it is still your problem
- Imagine gmail allowing each customer’s auditors to come in and check their controls: impossible!

Agreed-upon procedures

- IS auditors sometimes perform engagements where, instead of attesting to management assertions or forming an opinion on a set of controls, they simply perform an agreed upon set of tests and report on the outcome
- Before a merger or acquisition, auditors often conduct due diligence assessments to see if a company’s information systems are properly controlled or risky

Internal auditors (auditors who work for the organization) perform many of the same kinds of audits as external auditors

Sometimes internal audits are for the board, sometimes they are done to prepare for external audits, sometimes they are intended to spur improvement, and sometimes results are used directly by external auditors

Audit Authority



- SEC (U.S. Securities and Exchange Commission) mission: protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation.
 - Oversee private regulatory organizations in the securities, accounting, and auditing fields
 - Establish accounting principles
 - Oversee the PCAOB
- They work with FASB, PCAOB, other groups to set standards

PCAOB
Public Company Accounting Oversight Board

<https://www.sec.gov/Article/whatwedo.html>

Oregon State
UNIVERSITY

4

The SEC provides Guidance on how auditing is to be done in the public arena

While many organizations including government agencies, privately-held businesses, and non-profits are NOT subject to SEC oversight, the SEC has a powerful role in determining what “good auditing” looks like – this understanding carries over to auditing in non-public companies as other regulators follow their lead

Of course, this is a U.S.-centric perspective, other countries have their own agencies, but they are often more or less in sync and follow each others’ pronouncements

Do you see how this works?

- To protect investors public companies need to report their finances in a consistent way – thus accounting standards
- Fair, orderly, and efficient markets require that organizations operate within reasonable risk boundaries, so the SEC mandates a variety of auditable controls: such as cybersecurity, for example

The SEC doesn’t just make up the rules, they work with other groups

- The **PCAOB (Public Company Accounting Oversight Board)** was created by **the Sarbanes-Oxley Act of 2002 (SOX)**
- PCAOB (sometimes called “Peekaboo”) registers and inspects the work of CPA firms that audit large public companies:
 - Every year if more than 100 SEC companies are audited
 - Generally, every three years if 100 or fewer SEC firms are audited
- Things the PCAOB emphasize become important for CPA firms – they don’t want to hear that their audits were sub-standard
- The **FASB (Financial Accounting Standards Board)** is a non-profit standards setting body recognized by the SEC as setting US GAAP (Generally Accepted Accounting Principles)
- **GAAS (Generally Accepted Auditing Standards)** are expressed in **SAS (Statements on Auditing Standards)** promulgated by the **AICPA (American Institute of Certified Public Accountants)**

SOX and IS Audit

- SOX requires that at least the financial reporting systems of SEC companies need:
 - An evaluation framework for IS operations
 - Useful IS metrics
 - A systematic way to apply the framework
- This perspective applies to non-SEC organizations as well:
 - Lenders may require IS audits
 - Financial services companies have their own somewhat similar regulations

Most internal control frameworks are quite similar to COSO

But it is not enough to say “We follow COSO”, organizations are expected to have metrics for IS. Examples might include:

- Percent of employees trained to appropriate levels of cybersecurity
- Frequency of review of relevant policies, procedures, and risks

And the details need to be somewhat specified

For example, for the risk assessment component of the framework, a risk management committee should meet regularly and report to the board no less than twice per year

The point is to show systematic implementation not just lip service

Management will need to assert that they have these things in place and report control weaknesses, or risk suffering penalties

Not Just SOX

- Gramm–Leach–Bliley Act (GLBA)
 - Financial institutions
- Health Insurance Portability and Accountability Act (HIPAA)
 - Healthcare (Supported in more depth by the HITECH act)
- Family Educational Rights and Privacy Act (FERPA)
 - Schools (including Universities)
- Europe’s General Data Protection Regulation (GDPR)
 - Personal data – anyone storing data on Europeans
- California Consumer Privacy and Privacy Rights Acts (CCPA/CPRA)
 - Privacy rights

While we say that SOX only applies to SEC-regulated companies, many other regulations and contractual relationships require internal control audits

- The **Gramm–Leach–Bliley Act (GLBA) of 1999**, for example imposes information security and other internal control requirements on financial institutions
- The **Health Insurance Portability and Accountability Act of 1996** (HIPAA) includes numerous information management requirements – these are specified in more detail in the HITECH act
- The **Family Educational Rights and Privacy Act (FERPA)** requires schools to protect their information
- **GDPR, the General Data Protection Regulation**, regulates how personal data is stored, shared, and managed
- Somewhat akin to GDPR, California created the **CCPA** in 2018 and the **CPRA** is coming online in 2023. Those are the **California Consumer Privacy and Privacy Rights Acts**

These requirements result in IS-focused, internal control audits, sometimes done by external auditors and sometimes by internal auditors

For example, Universities that handle various financial transactions are subject to provisions in the GLBA

And, any organization that processes data about European Union Residents (all major Universities, for example) are subject to GDPR regulations to some degree

While for many very small companies, internal control audits would not be productive, even medium sized organizations can save a lot on financial audits by demonstrating that their internal control systems mitigate reporting risks

And those audits can also help in the area of compliance – maybe its not a financial issue directly, but bad press or sanctions from mis-handling private data can be bad for an organization

Assertions, Attestation, and Auditing

- Management makes assertions, essentially:
 - “Financial statements are accurate and were prepared according to GAAP”
 - “We have proper internal controls in place”
- Auditor opinions attest to the truth of those assertions
- Auditing collects evidence that the assertions are true to form the basis for opinion

In attestation engagements, auditors evaluate written assertions by management to form an opinion

This formulation is important: auditors don't independently assess the finances of a company, they gather enough evidence to provide reasonable assurance that the written assertions of management are true

Internal control opinions also attest to written assertions

- Management asserts “We use the COSO framework” and provides details:
 - We do this and that to create a proper control environment
 - We assess risk appropriately (How? How often?)
 - We have needed controls in place
 - We properly manage the information needed to manage the control process
 - We systematically monitor our controls and control processes and make improvements as appropriate
 - Hint: that list explains each of the five COSO components...
- Auditors review management's statements and collect evidence to validate the veracity of the assertion
 - They assess implementation of the framework – Are all the parts there? Is the ongoing process functioning?
 - Are the controls designed in a way that should protect against the identified risks?
 - Are the control steps being carried out as designed?
 - Are they having the correct effect?

IUC – Information Used in Controls

- Control: managers review purchases on a monthly basis
 - ensure that expenditures are accurate and not fraudulent
 - relies on a computerized report
 - The report has to be right: Can we be reasonably assured that:
 - the data will be right,
 - the report program properly designed and tested so as to generate an accurate list, and
 - that the program or report were not altered without proper authorization?

PCAOB audit inspections in recent years have considered IUC – Information Used in Controls

Let's put some of the concepts we have discussed together by talking about a control and its IUC

- SOX requires that internal controls are in place to ensure accurate financial reporting
- Let's say that management asserts that they review expenditures on a monthly basis – this control is in addition to other controls such as segregation of duties and vendor management
- The auditor sets an audit objective: Determine whether a competent person regularly reviews expenditures
- The auditor decides on a set of procedures: Verify that reports were reviewed and acted upon
 - Perhaps the report is delivered by email or the report creation is logged
 - If the reports are saved, they could be spot checked to see if good judgement was applied
 - There could be evidence (email trails, memos, meeting notes) that demonstrate that meaningful review took place

But! If the lists the manager looked at were incorrect, the control might not be effective in detecting inappropriate spending even if the person does what they should:

- Maybe certain expenditures don't show up because of a system or programming error
- Maybe the data is inaccurate because what is really paid out is not properly adjusted when changes are made
- Maybe the report program was not properly tested before it was put into use and it has a logic error for some transactions
- Maybe the program was changed along the way intentionally or unintentionally introducing error

Do you see how things come together?

- There should be IS processes to design and create new software and reports – controls over those processes should ensure tests are conducted and approvals are documented
- There should be controls in place to protect against unauthorized changes to the financial software and data
 - Are the access rights to programming limited to authorized people?
 - Are credentials (user names, passwords, authorizations, etc..) managed to ensure that the access rights go to the right people?
 - Are people with access removed from the system when they leave the company?
 - Are the underlying databases protected from tampering or corruption?
- If the controls over these processes fail, the financial internal control (monthly expenditure review) might not be reliable. This could mean that the financial auditor should look more closely at the expenses reported in the financial statements
- In short, the information used in the control (IUC) was not reliable, so the control would be judged to be ineffective


College of Business

Governance AND Management

Ensure that we are doing
the right things

- Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives.
- Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

Organize and execute to
do things the right way



COBIT 5 © 2012 ISACA.
9

Governance and management are not the same thing, but managers (management) makes auditable assertions about both

As discussed before, the components of COSO reflect that internal control is an integrated process

In addition to performing control activities and managing related information, properly controlled organizations establish the control environment, assess risk, and monitor

Managers **Plan, Build, Run, and Monitor (PBRM)** operations

This generally means figuring out how to deploy existing resources effectively and acquiring new resources to address new risks and opportunities

But managers are not ultimately responsible for the success of the organization in the same way that the board of directors is. Governance bodies are charged with looking over management's plans and activities to ensure that the right things get done. In healthy organizations this is a partnership where the board provides feedback and additional insight to help managers successfully run the organization.

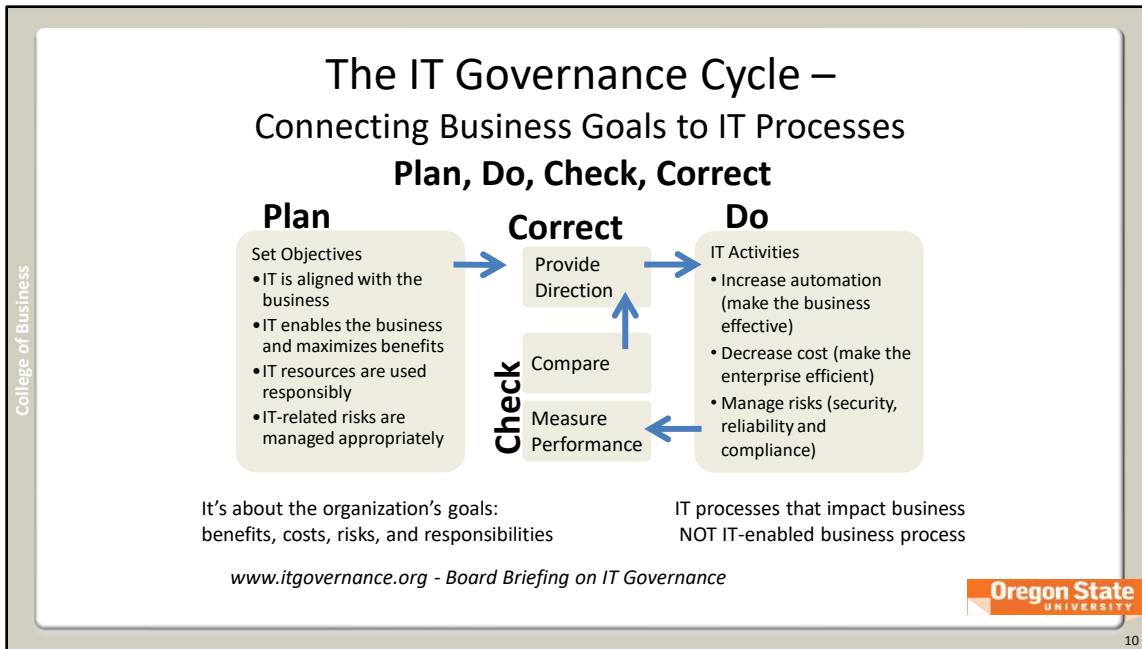
Just as auditors need to be independent from the organization to make sure that they present unbiased assessments, oversight bodies such as boards of directors or governance or advisory committees need to take a broad view that is not overly influenced by the people who do day-to-day work.

It's not that those people are not trustworthy or incompetent, it's just that they are likely to pay attention to the current over the long term, to see their own area as very important, and to miss risks that are outside their field of operation.

IS auditors need to verify that someone is looking at the big picture and looking out for various stakeholders.

Thus, it is not enough to observe that operational control procedures are being carried out, they need to look at controls over the governance processes that are supposed to result in good operations over time.

Are risks assessed regularly? Do governing bodies receive appropriate information to make decisions? Do governing bodies monitor the effectiveness of operations including the control systems that protect those operations?



By now you have heard a lot about processes versus activities

The IT Governance Institute (part of ISACA) highlighted the “Virtuous Cycle” created by effective governance processes

The Enterprise IT function in an organization should

First **Plan** – setting objectives while considering benefits, resource usage, and risk

Then **Do** – often involving automation, cost reduction, and again, risk management

Then **Check** by systematically measuring the impact of operations – we will talk more about metrics in later weeks

Then **Correct** by adjusting plans, operations, and monitoring processes

As emphasized by the animations on this slide, this is an ongoing process which is repeated over and over to drive continuous improvement


While this kind of cycle may be useful to lots of governance processes, remember that here we are talking about governing the IT function and that the IT function primarily operates a series of IT processes that are designed to deliver IT services effectively over time

College of Business

Types of controls

- From COSO: “Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls”
 - Preventive**, control - An activity that is designed to prevent an entity from failing to achieve an objective or addressing a risk *
 - Detective** control - An activity that is designed to discover when an entity is not achieving an objective or addressing a risk before the entity’s operation has concluded *
 - Corrective**: Neither COSO nor the green book does mention this type of control but many other sources do. “Procedures a company uses to solve or correct a problem” (Accounting Information Systems 13th edition, Wiley)
- Application Controls vs. ITGC: Are multiple “systems” protected?

* From the Federal “Green Book” which adapts COSO for federal agencies



11

COSO’s Principle 10 from the Control Activities component includes this point of focus: *Evaluates a Mix of Control Activity Types—Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls.*

In evaluating the design and operation of controls, it is important to understand how controls work
While each control works differently, here are some general ways to think about them:

A control can be **preventive** – preventive controls prevent negative events from happening
For example, a system can prevent creation of a short password like 123 – the user can try, but it just won’t work

A control can be **detective** – like a review of log entries generated whenever an approved transaction is altered – presumably by someone with override privileges; this control would not prevent bad things from happening, but it could help the organization realize that a bad thing had happened

Contrast the two controls designed to protect the numbers in approved checks

- A system-enforced preventive control ensures that only authorized users changed certain records
- But the log entry and review was detective, the error had already occurred and was only identified later

A control can also be **corrective**, for example:

- There can be documented rerun procedures in case the system crashes after a batch of checks has been sent to the printer; the bad event (crash) happens, but the control helps the system get back to the proper state
 - System backups are always corrective: their only purpose is to allow administrators to put data back when it is lost or corrupted
- Understanding if a control is preventive, detective, or corrective is important in understanding the level of risk

Another important control distinction considers whether the controls protect a certain “application” or generally address IT risks related to multiple applications. The word application here is sort of like “app” on a phone: a program. But it allows for more. A set of programs that work together can be an application. The related activities of people performing a certain set of activities might be considered part of that application. Some applications might be called “systems”. But be careful. If we are talking about controls for a platform (system) that supports multiple applications, we are not talking about application controls. ITGC – IT General Controls are controls that protect multiple applications or systems.

These characteristics impact what is needed for the control to be effective and influence how they can be tested or assessed.

College of Business

Don't Forget the ITGC

Access Controls Including controls over

- Identity management
- Assignment of privileges
- Protection of physical security

Security Management processes and safeguards that ensure:

- Integrity
- Confidentiality
- Availability

Configuration Management controls addressing processes for:


- Managing changes to information systems
- Ensuring that systems are configured and operated securely and as intended

Segregation of Duties of IS personnel:

- Separating Development and Operations
- Ensuring Personnel Supervision and Review

Contingency Planning controls to:

- Protect against unplanned outages
- Provide for recovery



12

When students think about controls, they often think of things they directly connect with financial transactions rather than risks related to the systems that manage those transactions

Do you remember what ITGC stands for? IT General Controls or General IT Controls

This is a good moment to increase your familiarity with categories of ITGC including:

Access Controls Including controls over

- Identity management
- Assignment of privileges
- Protection of physical security

Segregation of Duties of IS personnel:

- Separating development and operations
- Ensuring personnel supervision and review

Contingency Planning controls to:

- Protect against unplanned outages
- Provide for recovery after a disaster, failure, or interruption

Security Management processes and safeguards that ensure:

- Integrity
- Confidentiality (Including, but not limited to, protecting **PII Personally Identifiable Information**)
- Availability

Configuration Management controls addressing processes for:

- Managing changes to information systems
- Ensuring that systems are configured and operated securely and as intended

If you think about it, you will realize that if these controls are not in place, financial systems have no hope of being reliable. And reports generated by a financial system cannot reasonably be deemed accurate or reliable:

- If access is not properly controlled through protected logins, physical security over the data center, and robust procedures for assigning privileges
- If financial software has not been properly tested or if unauthorized changes could be made to it
- If the same person who configures access rights in the system can alter records of who has been granted access

Much of IT auditing focuses on seeing whether ITGC are well designed and in operation

While the ITAF and PCOAB audit standards relate to the discipline of auditing, many elements of FISCAM and other useful audit resources focus on ITGC

Other Ways to Differentiate Controls

- Compensating: Always part of a narrative
- Does someone have to choose to perform the control activity?
 - Automatic vs. Manual

Automated control activities are either wholly or partially automated through the entity's information technology. Manual control activities are performed by individuals with minor use of the entity's information technology. Automated control activities tend to be more reliable because they are less susceptible to human error and are typically more efficient. *

* Federal Green Book 10.06



13

Sometimes one control fails and another control catches the mistake

We categorize a control as compensating as part of a narrative about another failed or missing control – either an expected control is not in place (increasing risk), or a control has been tested and found to be improperly designed or operated (revealing risk) Oops! That's a compliance problem because policy or standards have not been met, but maybe another control also helps It's not just that the controls overlap, it's that the risk associated with a missing/failed control is otherwise addressed

Overlapping controls can include a mix of Preventive, Detective, and Corrective controls

Consider for example, controls over the vendor list in an AP system, many frauds have been committed by adding fake vendors A company may have a policy and an implemented program requiring two employee approvals before a new vendor can be added to a system or a mailing address can be changed

What if it turns out that those control procedures are ineffective because of a misconfiguration of the program or because someone shares their password with a co-worker? But also, what if, when changes are made, a log entries are generated and the log is reviewed monthly by the AP manager

This log review can be a **compensating** control: even if the policy and segregation of duties controls fail, the log review has a good chance of catching errors that can lead to losses or misstatements

You should be provide, recognize, and explain examples of preventive, detective, and corrective controls and you should recognize and explain compensating controls and ITGC which can also be preventive, detective, and/or corrective

Automatic control activities happen without anyone choosing to do them; e.g., vendor approval controls can be enforced by the computer system leaving the user no choice – the system won't print a check or record a payment to an unapproved vendor

Manual control activities require that a person choose to act, even if that action is "required" by policy and monitored Auditors generally assign lower levels of control risk to **automatic** controls;

Consider, for example, that the person charged with reviewing the log might get busy and not pay due attention when looking at the list of vendor changes; manual controls are often ineffective if the person does not do the right thing the right way Automatic controls, on the other hand, are usually very narrow, and can be both expensive and intrusive or disruptive

Let's compare: A manager who manually reviews a budget to actual report can use judgment whereas an automatic control that prevents over-budget checks might result in operational delays or might block needed payments But an automatic control might allow an under-budget but inappropriate expenditure that a manager would manually disallow