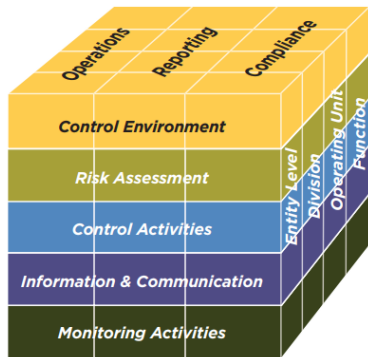


# IT Audit Seminar

Internal control,  
A few audit concepts



IT Auditing



This image shows the COSO Cube which depicts an integrated system of controls. IT controls are a central part of an organization's internal controls. You can't understand IT risks or IT audits without knowing how they fit into this larger risk management context.

This slide deck has a lot of information. You need to look at the comments as well as the slides to learn what you should.

# Agenda

- COSO and internal control definitions – Processes!
- ITAF and PCAOB Audit Standards
- A few additional fundamental concepts
  - Audit procedures collect evidence
  - Standards and Criteria
  - Testing phases

# The Rise of Regulation

- Banking Scandals in the 1980's resulted in COSO - It was voluntary
- More large failures of SEC companies lead to the 2002 Sarbanes-Oxley Act (SOX) which created rules that were NOT voluntary:
  - Management is responsible for internal control and financial reporting procedures
  - Annual reports must assess internal controls
  - Officers submitting inaccurate certifications are subject to a fine up to \$1m + 10 yrs, if purposeful, up to \$5m + 20 years
  - Significant deficiencies in controls (including IS controls) must be reported
  - SOX also created the PCAOB (Public Company Accounting Oversight Board)

For more see: [https://en.wikipedia.org/wiki/Committee\\_of\\_Sponsoring\\_Organizations\\_of\\_the\\_Treadway\\_Commission](https://en.wikipedia.org/wiki/Committee_of_Sponsoring_Organizations_of_the_Treadway_Commission) - Or ask ChatGPT!



3

IT audits came to be largely because of internal control failures.

COSO - **The Committee of Sponsoring Organizations of the Treadway Commission** - first came about when a series of Savings and Loans went bankrupt in the 1980's.

- The public and congress wondered how audited banks could actually be subject to risks related to assets that didn't exist or that weren't really properly represented in the financial statements; wouldn't the auditor notice such problems?
- The accounting industry collaborated in the creation of COSO – the idea was that they would evaluate the internal controls of an organization so as to be able to better understand audit risk.
- The chance that the numbers on the financial statement were incorrect or not in accordance with GAAP was smaller when a comprehensive internal control process was in place – the COSO framework specified the definition of a good internal control process.

It may be fair to say that auditors and public companies hoped to “self regulate” by assuring that audited organizations had robust systems of internal control that could fend off the kind of problems that arose from the bank failures in the early 1980s. You might even say the idea was to fend off the potential for government intervention.

The failure of WorldCom and Enron - multi billion dollar, audited, and SEC regulated companies – convinced the public that we needed laws (not just a self-policed framework) that require effective internal control.

The **Sarbanes-Oxley Act of 2002 (SOX)** codified internal control requirements and substantial penalties for inaccurate internal control assessment.

Its kind of a funny name, including the words committee and commission. But really it's a report and a framework.

*Hint: in this class, pay attention to the sponsoring commission and don't forget that that is part of what COSO means.*

You can see the penalties on the slide: Here is a little secret – CEO's don't like to go to jail, even if the jail is cushy!

Even now that SOX is in place, COSO remains as the foundation of most organization's internal control systems and is the source of criteria by which internal control systems are evaluated.

Evaluating internal controls is at the heart of IT audits and, really, of financial audits as well.

# COSO Defines Internal Control

Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations\*, reporting, and compliance.

Internal control is:

- Geared to the achievement of objectives in one or more categories—operations, reporting, and compliance
- A process consisting of ongoing tasks and activities—a means to an end, not an end in itself
- Effected by people—not merely about policy and procedure manuals, systems, and forms, but about people and the actions they take at every level of an organization to affect internal control
- Able to provide reasonable assurance—but not absolute assurance, to an entity's senior management and board of directors
- Adaptable to the entity structure—flexible in application for the entire entity or for a particular subsidiary, division, operating unit, or business process

COSO – Internal Control – Integrated Framework, Executive Summary

<https://www.coso.org/Shared%20Documents/Framework-Executive-Summary.pdf>

\* COSO documentation notes that operations includes safeguarding assets



4

Internal control is supposed to help organizations achieve the objectives for operations, reporting, and compliance.

We all immediately understand how regulators have a role in ensuring reliable reporting (no lying to investors) and compliance (we have laws – follow them!)

But an internal control framework goes beyond those minimums to address operational risks.

The explanation shown on the slide emphasizes some key ideas about internal control:

- It is focused on the objectives of the particular organization. Different organizations have different objectives. COSO doesn't determine them. It talks about how to assure that they are achieved.
- It is an integrated process – or a set of interrelated processes.
- People are involved – it is explicitly not enough to have documentation and paperwork. People control operations. Note the definition also specifically calls out the board and management as being responsible. But it also indicates “other personnel”. If internal control is working right, everyone has to be involved to some degree.
- Complete assurance is essentially impossible. Internal control does not ask for the impossible, just the reasonable.
- COSO does not specify a one-size-fits-all set of operations or even define a set of control activities. COSO is a framework that describes the key elements of an ongoing process for internal control.

COSO specifies control processes, not controls. That is, it talks about how an organization is to GO ABOUT protecting itself without listing controls that provide protection. At a high level: set up structure, culture, and processes so that the many things you do to reasonably assure success will workout well.

It specifies components – which are like foundations on which an effective process of internal control has to include.

It specifies principles which guide how those components are to be shaped and what they are to accomplish in a general way.

And it specifies points of focus which very generally identify some actions an organization is expected to take to accomplish the identified priorities.

College of Business

## Internal Control Key Elements

- 1 - process,
- effected by an entity's
  - 2a - board of directors,
  - 2b - management,
  - 2c - and other personnel,
- designed to provide 3 - reasonable assurance
- regarding the 4 - achievement of objectives relating to
  - 4a - operations,
  - 4b - reporting, and
  - 4c - compliance


Process

All Hands On Deck

Reasonable Assurance

Achieve Objectives

Don't forget to  
protect assets!



"You may want to remember" these 9 key, underlined points in the internal control definition. They are all really important if you are to understand how internal controls are audited.

Think about internal control as important for operations, reporting, compliance.  
The board, management, and others are involved.

Financial reporting is very closely monitored. Other kinds of reports such as environmental and safety reporting also matter, but financial reporting is what we think of most often. The Securities Exchange Commission (SEC), Banks, and Governments all expect that an organization will produce accurate, complete, and informative financial reports so that investors are protected, and taxes are properly collected.

Numerous compliance concerns arise. Is personally identifiable information (PII) protected as it should be? Are labor laws followed? Are workers protected from unwarranted risks? Are trade restrictions followed? And more....

Some definitions of internal control have suggested that internal controls safeguard assets. COSO includes that important class of control objectives in operations.

While assets are only part of the picture, they are very important. Using accumulated assets appropriately is, debatably, the most important thing an organization must do. You can think of that either as wisely stewarding society's resources and/or as allocating resources so that wealth and well-being are maximized. But either way, resources should not be used outside of the organization's mission (unauthorized use), lost or given away (unauthorized disposition), or acquired in a way that is wasteful or risky (unauthorized acquisition).

Internal control processes are supposed to provide reasonable assurance the organization will accomplish these objectives.

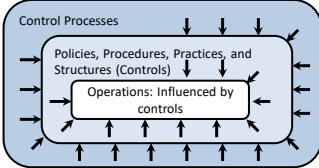
**Financial auditors are trying to gain assurance that a set of financial statements properly describes a firm. But often, instead of checking to see if every number in the statement is based on verifiable facts, auditors focus on the process by which those facts are recorded and summarized.** If they believe that a system is very likely to produce accurate statements, they worry less that the actual statements are incorrect.

So, internal control auditors are usually not all that interested in any single event. Everyone makes mistakes. Instead, they think of operations, reporting, compliance, asset management, and internal control as ongoing processes.


College of Business

## Internal Control → Internal Controls → Operations

- Internal control is a process
- Solid internal control processes result in the design and deployment of internal controls, which are:
  - “The policies, procedures, practices, and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected.”\*
- Controls address:\*
  - What should be achieved
  - What should be avoided



\* ISACA IT Audit Fundamentals Study Guide, pp. 215



If internal control is a process, what are internal controls? Policies, procedures, practices, and organizational structures.

These are the building blocks organizations use to create ongoing, integrated, and effective control processes.

If you look up these terms, you will find that they overlap. Sometimes they are treated as synonyms or they are used in each others' definition. But those four terms indicate a wide range of actions and artifacts. Policies are guidance for action, procedures specify actions, practices are general ways of acting, and organizational structures can tend to facilitate (or hinder) various actions.

Inherent in the idea of a set of internal control processes is the notion that it is not enough to just go through the motions and check all the right boxes. Internal control processes are supposed to result in effective internal controls.

Admittedly, that does not always work out. Sometimes organizations (people) do the minimum. Some see internal control as merely a compliance cost. There is some truth in that notion. Also, an organization can do the right thing without documenting and monitoring whether or not it is doing the right thing. But in practice, unmonitored good intentions eventually come up short.

The basic structure of COSO, which defines internal control as a process, is designed to reasonably assure that an organization will do what it means to do (operational), honestly communicate about its operations and finances (reporting), and meets it legal, contractual, and promised obligations (compliance). That's a good start towards avoiding and minimizing the impact of catastrophes even if it does not absolutely prevent them.

Internal control processes design, deploy, maintain, and support a large number of internal controls.

The processes are not the controls, but the controls are ineffective without supporting processes.

Internal controls seek to assure that operations meet objectives.

The controls are not the operations, but operations may go off track without controls.

Often, a specific internal control can be performed half-heartedly in the absence of solid control processes, leaving the organization exposed to risk. Here is an example:

**Operations:** Payments are approved and databases are managed for purchases. Certain individuals have privileged access. They can approve an expense or change a database.

**Control:** Because allowing an unauthorized person to make changes can result in problems, someone is charged to regularly check the system to see if the right people are authorized: no old or incorrect accounts are configured in a way that allows them to approve payments or make changes.

**Control processes at work:** Someone designed the review procedure. Someone makes sure the list of who should be authorized is correct. Someone verifies that the review is done on a regular basis. This can go wrong if the people don't take appropriate care.

# What Do We Mean By “Process”?

- Something we do over and over again
- Be systematic, don't just do it right this time
  - Sell Products Business Process
  - Install a new ERP system (once or rarely) Not a process
  - Acquire new systems (repeated) IS Process
- Processes
  - Account for known risks
  - Aim for consistent results
  - Systematic
  - Business vs IS Processes



Let's think about processes; When we talk about processes, we mean something ongoing – not something we did once. In common conversation we don't make this distinction, but we have to here if we are to understand internal control.

- Selling products on the internet is a business process.
- Acquiring new information systems is an IS process.
- Installing a new ERP system is not a process – it is a one-time project.

Why is “Installing a new ERP system” NOT a process?

- Processes are done over and over: we repeatedly sell products on the internet, we install lots of information systems, but we only rarely install a new ERP.
- We may have a plan for a particular installation, but that plan will only be used once.
- Installing this particular ERP system presents specific risks even though many risks are common to other system implementations.

Why is “Acquiring new systems” a process?

- We acquire multiple systems over time.
- We do some of the same things over and over.
- Each new acquisition shares familiar risks.
- Standards, policies, guidelines, and procedures can help us do them better, these would apply to any new system we acquire:
  - Make sure the right people approve.
  - Assess cost and benefit.
  - Monitor progress.

“Sell Products” is an organizational or business process.

- It is “doing our business”; we are in the business of selling stuff, that's how we accomplish our mission.
- Like acquiring new systems, it is done over and over again, is subject to risk, and can have related policies and procedures.
- Do you see how business and IS processes are different?
  - IS processes are processes we need to have but we are not in business to do them.
  - IS processes affect multiple business processes.

Two key ideas:

1. We want a consistent controls over processes so that we are confident those organizational processes will achieve goals. That applies to both business and IS processes.
2. Internal control is itself a process; it is ongoing, involving multiple steps that work together to accomplish objectives

## “Manage Security Services” - an IS Process defined in COBIT – an authoritative standard

- Our business sells things on the internet
  - Business sub-processes include: Order taking, Shipping, Collecting payments, Marketing
  - These share common security risks - systematic cybersecurity is better than ad-hoc protections
- A good security process employs good practices:
  - Scan for malware
  - Limit how computers can connect to the network
  - Safeguard user lists
- IS processes, like this one, support multiple business processes

Controlled IS processes that support organizational processes.

COBIT – a well recognized source of authoritative IS control standards defines *Manage Security Services* as an IS process that should be managed and controlled.

This is in contrast with an Organizational or “Business” Process – *Sell products on the internet*.

Securing systems is a necessary requirement to do business but it does not directly conduct our business. IT processes generally support multiple business processes, applications, and systems. The way we go about securing systems impacts lots of systems.

Do you see how this works? We need an IS process for managing security services. For example:

- We want to ensure we maintain an acceptable level of security risk to minimize the negative business impact of adverse security events.
- There are some key practices that should be part of the process of managing security services, here are a few:
  - We need to protect against malware (nefarious programs that might get loaded onto our systems.)
  - We need to manage how computers connect to and within our network.
  - We need to have a way to manage our list of users.

These practices are specified in COBIT as important and expected parts of this process.

These practices involve controls for risks

- Scanning protects our system from malware that might cause downtime that would reduce our sales or keep us from sending out packages out on time.
- Limiting access to our network might keep a hacker from rerouting (stealing) shipments or altering purchase records.
- Protecting our user list reduces the chance a customer’s credit card information or our intellectual property is stolen from our systems.

Note that this general process (Manage Security Services) protects multiple business processes and that many of the activities in this process control for multiple risks.

- Malware scanning protects servers and desktops.
- Malware scanning protects against disruption of service and loss of data.
- These benefits apply to payroll, sales, accounts payable, and many other business processes.

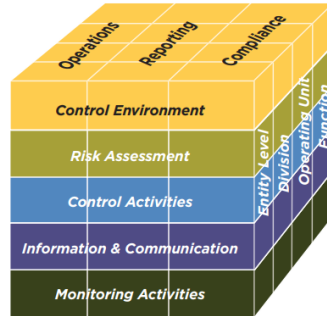
The process is not “We don’t have malware” it is “We protect against malware.”

One important theme of IS auditing focuses on providing assurance that controls embedded in IS processes are effective.



# COSO Components

- Integrated COSO Cube:
  - Five components (Top to bottom)
  - Impacting operations, reporting and compliance (left to right)
  - Across the organization (front to back)
- Implications
  - Individual controls become and remain effective only when all the components are functioning well
  - Control processes embody the components



The five COSO components highlight different facets of an effective and integrated system of internal control. Failing to implement any of the five components would result deficient controls. Organizations need to cover all five reasonably well if they are to meet expected standards for internal control.

So, both auditors and managers can benefit from understanding what the components mean.

Culture and organization – **Control Environment** supports control. Leaders commit to integrity and the board is independent. Structure supports achievement of objectives. Competent people are in place and are held accountable for internal control.

Effective **Risk Assessment** is essential if risks are to be controlled. Clearly defining success facilitates identification of risks and strategies to manage them. Organizations pay attention to the potential for fraud and watch for changes that can lead to risk.

Control processes guide effective **Control Activities**. Protective actions are selected, developed, and supported by policy and procedures. Information technology, in particular, is generally protected so it can help the organization achieve its objectives.

**Information and Communication** efforts support controls and control processes. Control-related information is gathered, generated, and shared. People know what to do and have the information they need to act.

Systematic **Monitoring** keeps control efforts on track. Control systems are continuously improved. Control weaknesses are surfaced and shared. Controls and control processes are repeatedly reevaluated so that effective changes can be made.

To help organizations implement effective and integrated control systems, these components are further described in COSO. **Principles** are identified for each component and provided **points of focus** promote a shared understanding of what it means to implement those principles. These authoritative resources help practitioners build effective systems. And, from an assurance perspective, they provide guidance and criteria. Auditors use them to help design, execute, and interpret the results of audit procedures. The contents of COSO lets auditors and auditees work from a shared understanding.

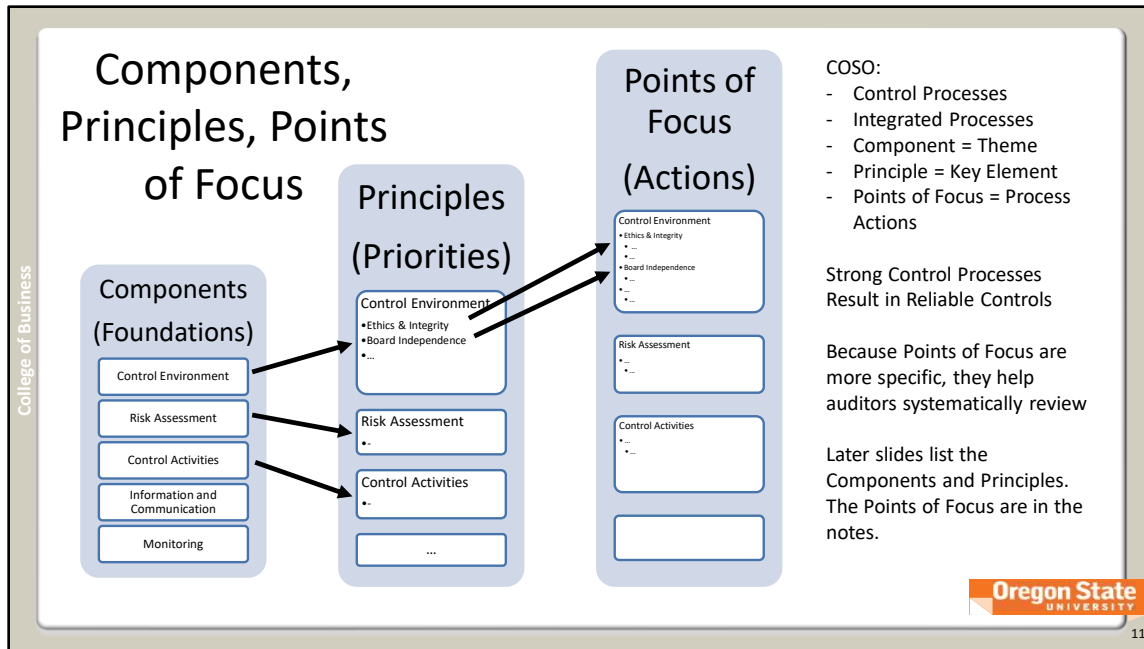
# COSO: Integrated Systems of Control

- COSO calls for integrated processes
- Think control processes, not just controls
- Think about how weakness in one component can nullify the effectiveness of efforts in other components

Control systems need to be integrated. These explanations demonstrate how weak integration can reduce control effectiveness.

They also illustrate each COSO component at work. Can you identify references to the components?

1. Controls activities interact. For example, a list of users might be stored in an encrypted form, but the encryption key might not be properly protected. The weak control (unprotected key file) would make the encryption essentially useless. Auditors need to understand how controls rely on one another for effectiveness.
2. Lack of commitment can nullify the effectiveness of controls. For example, access to certain functions may be segregated. One person is charged with making changes to an important financial system and those changes are supposed to be reviewed by a second person. But if the second person doesn't think the checking is very important and simply approves changes without paying much attention, the control is ineffective. Management needs to be sure that employees believe they are supposed to cooperate with control requirements not just go through the motions.
3. Controls often rely on provided information. For example, the IT manager may be expected to review the list of database administrators on a quarterly basis to see if the right people, and only authorized people, are on the list. But if the report that lists such users is flawed, it might not show everyone who is configured for high-level access. The weak information used in the control (IUC) renders the control (quarterly review) ineffective.
4. Controls can be a waste of time if they address insignificant risks while missing important ones. Employees may comply with the rules, but the people who developed the rules may not have considered important problems that could arise. For example, maybe the quarterly review looks at administrative access for systems directly controlled by the organization but does not include servers housed in the cloud. The organization's risk assessment was inadequate, so the control design is flawed.
5. Control systems need to be verified and need to change over time to adapt to reality. Quarterly reviews may stop or become ineffective over time. For example, a new manager may not realize they should look at the list or not know how to make sure the right people have the right access. Or, they may note problems that never get fixed. If the organization does not monitor the operation and effectiveness of controls, they likely have ineffective controls.



Do you remember how internal control became important? Large, regulated organizations failed spectacularly.

Investors, (and other stakeholders) want to avoid more big failures. But how?

The answer was to encourage organizations to implement a comprehensive internal control framework. A framework does not say how an organization should operate, but it does describe the shape of the processes by which an organization can reasonably assure that it will not fail.

The five components are the foundations or pillars of solid internal control.

The 17 COSO principles provide insight into the intent of the components.

The 77 points of focus identify specific things done or accomplished when an organization has solid system of internal control processes.



We want to bridge from generalities to specifics in ways that help organizations build solid internal control programs and also allow others to assess the quality of those programs.

From an internal control audit or IT audit perspective, the points of focus are really important because they include more tangible elements that can be more easily matched to specific actions and artifacts.


A more in depth look at the contents of COSO is central in understanding internal control and internal control auditing. But this is enough for us to go along with for now.

College of Business

## Two More Resources

- ITAF: A Professional Practices Framework for IS Audit  
<https://www.isaca.org/bookstore/audit-control-and-security-essentials/witaf4>  
*(Choose English/Digital and it is a free download; you just have to have an ISACA account)*
- PCAOB's audit standards  
<https://pcaobus.org/Standards/Auditing/pages/default.aspx>



12

COSO provides guidance on how internal control systems in an organization are supposed to work.

FISCAM provides guidance on how to audit governmental information systems including some instructions about how to audit as well as communicating some common expectations for organizational internal controls.

To get more deeply into IT auditing practices, you will need to learn about the contents of auditing standards.

COSO describes key elements of strong internal control systems. These resources provide authoritative guidance an auditor can use to support a choice to audit for certain controls that address certain risks.

FISCAM also has some control information. In many cases it provides control listings and corresponding audit procedures.

FISCAM also provides guidance on the practice of IT auditing as opposed to the substance of audited control systems.

As we focus more on auditing, the ITAF and PCAOB standards tell us more about how audits are to be conducted.

ITAF from ISACA provides guidance on things certified information systems auditors (CISA) are to do as they conduct audits.

More generally, the **PCAOB (Public Company Accounting Oversight Board)** works with other agencies including the SEC (Securities Exchange Commission) to establish what it means to properly conduct audits. The extensive documentation linked here is 725 pages long, but it formulates many of the key concepts we will use this term.

12

# ITAF VERY briefly

- The Code of ethics (See ITAF page 10): Supports good practices, Be professional, Report properly
- IS Auditing standards talk about auditing not about IS
  - What does a proper audit include?
  - What does it mean to be professional?
  - How do you support things you report on?
- Guidelines describe what an auditor can do to meet the standards

Here is a very brief ITAF introduction

The ISACA code of ethics is short: 7 points, half a page.

- It requires that IS Audit professionals are to support good practices for the effective governance and management of enterprise information systems.
- It requires that auditors are professional: diligent, lawful, respectful of stakeholder interests, careful with information they handle, and competent.
- It requires appropriate transparency in reporting.

The IT audit standards do not talk about IS, they cover things an auditor must do:

- Required elements of an engagement
- Expectations for the skill, qualifications, and conduct of an auditor
- Boundaries for reporting and follow up

Guidelines are a bit different: they are not mandatory, but they explain things an auditor can do to meet the standards.

They refer to them as “things to consider” as audits are performed.

They may not be mandatory, but if an auditor doesn’t follow them, they better have a reason.

## Some more vocabulary

- Audit procedures collect evidence
- Standards and Criteria
- Testing phases
  - Test of design
  - Test of operation
  - Test of effectiveness

The next few slides cover these concepts.  
Snippets from ITAF and PCAOB AS will be included.

# Audit Procedures

- We seek to provide reasonable assurance that our processes and controls are working
- Usually we think of this as “testing the controls”
- Audit procedures collect evidence for assurance/attestation

*ISACA standard 1205.1 - IS audit and assurance professionals shall obtain sufficient and appropriate evidence to draw reasonable conclusions ITAF page 14*

Audit procedures gather audit evidence.

Procedures are designed to collect evidence that will be useful in assessing the effectiveness of controls.

This is harder than it looks – you have to have a plan so that you don’t waste all your time finding out things that don’t, in the end, result in audit evidence.

The slide shows an audit standard from the

Do you see how the listed ISACA ITAF standard contributes?

It tells us a few things about what our audit procedures are supposed to accomplish:

- Evidence is to be sufficient – while this is not specified in detail in this standard, auditors learn about how to consider various elements of audit risk and learn about sampling methods to support the sufficiency of collected evidence
- The evidence is to be obtained by IS audit and assurance professionals, not by just anyone
- Results are to be connected to collected evidence

These things may seem obvious, but actually, given that audits could be done a number of ways by various people to various ends, these few words sketch out part of how an audit is to be evaluated

# Standards and Criteria

- Two kinds of standards:
  - IT Audit standards: how to conduct an audit: be independent, be competent, reports should be as expected....
  - Compliance and best-practice standards speak to IS processes or controls to help auditors develop criteria

## ITAF Standard 1008.1

*IS audit and assurance practitioners shall select criteria, against which the subject matter will be assessed, that are objective, complete, relevant, reliable, measurable, understandable, widely recognized, authoritative, and understood by, or available to, all readers and users of the report.*

ITAF page 12



16

At this point it is important to distinguish between two kind of standards:

- Standards related to business, IS, and control processes
- Standards on how to conduct an audit

We have already talked about FISCAM the Federal Information Systems Controls Audit Manual. IT is one source of audit-related standards, but it also includes lots of information about control systems that ought to be in place in a well-controlled organization. We will talk about other sources of IT auditing standards (that is guidance on how to conduct audits rather than guidance on how to design, implement, and operate controls) later in the term. The quote on the slide above is from the IT Assurance Framework (ITAF). This resource provides guidance on how IT auditors are to go about doing their work.

Read over ITAF 1008.1 on the slide. It is guidance on how to conduct an audit. It says that criteria need to be identified. Criteria are targets or thresholds an auditor will use to decide whether or not an organization's controls or control processes are acceptable. 1008.1 does not say anything about any particular risk or control. It doesn't say, for example, that system users lists need to be encrypted and should only be accessible to authorized people. Those would be audit criteria. Standard 1008.1 merely says that criteria will be formed. And says that those criteria should be "*objective, complete, relevant, reliable, measurable, understandable, widely recognized, authoritative, and understood by, or available to, all readers and users of the report*". The material on a previous slide on managing security services was taken from COBIT, a "widely recognized and authoritative" source. Criteria (such as "encrypted") are only appropriate for an audit of they are supported by such a source. Note however, that the user list might be encrypted in a way that does not really protect it from intrusion; judgement is still required. The point of this audit standard is to say that the auditor cannot just make up their own targets/thresholds (criteria) they need to use recognized and accepted criteria.

Often organizational policies include standards, and those standards are used to form criteria.

The point is that auditors rely, whenever possible, upon authoritative criteria so that conclusions are stronger than mere opinion. No one really cares if the auditor thinks things are too risky; they care if the auditor is applying approved criteria that are know to assess the level of risk.

Can you see the difference between auditing standards that say how to audit and standards that form the basis of criteria? This is an important distinction.



# Internal Control Testing Phases

- Three kinds of internal control testing:
  - Test of design: Is the internal control designed appropriately so that it would be effective when functioning properly?
  - Test of operation: Is the control operating as it should?
  - Test of effectiveness: Is it having the intended effect?
- This is an important distinction:
  - Some audits only test the design of controls
  - Many properly-designed controls prove to be incorrectly implemented or incorrectly executed
  - The control may be ineffective because of poor design, or because it is not being properly executed

Actually, the first two kinds of testing listed on this slide are the main focus of most auditing procedures

Still, auditors are interested in results

For example, a cybersecurity training program might be intended to train people in the organization and reduce organizational problems resulting from individuals who click on phishing links in email

An auditor could make sure the training includes the right information to help (test of design) and make sure that the right people have actually participated in the training (test of operation) or learned what they should (test of effectiveness)

But since some organizations have security incidents despite solid efforts to prevent them and since other organizations just get lucky and don't happen to have been effectively attacked during the review period, auditors generally focus most of their efforts on the design and operation of controls

Still, if, after training, the number of successful phishing attacks rises, the auditor might include that the controls are ineffective