College of Business

IT Audit Seminar

Performing IS Audits

Material is largely from ITAF standards and guidelines

ACTG 420/520
IT Auditing

https://mbkauditing.com/services/information-systems-audit/

IS Auditors need to understand:

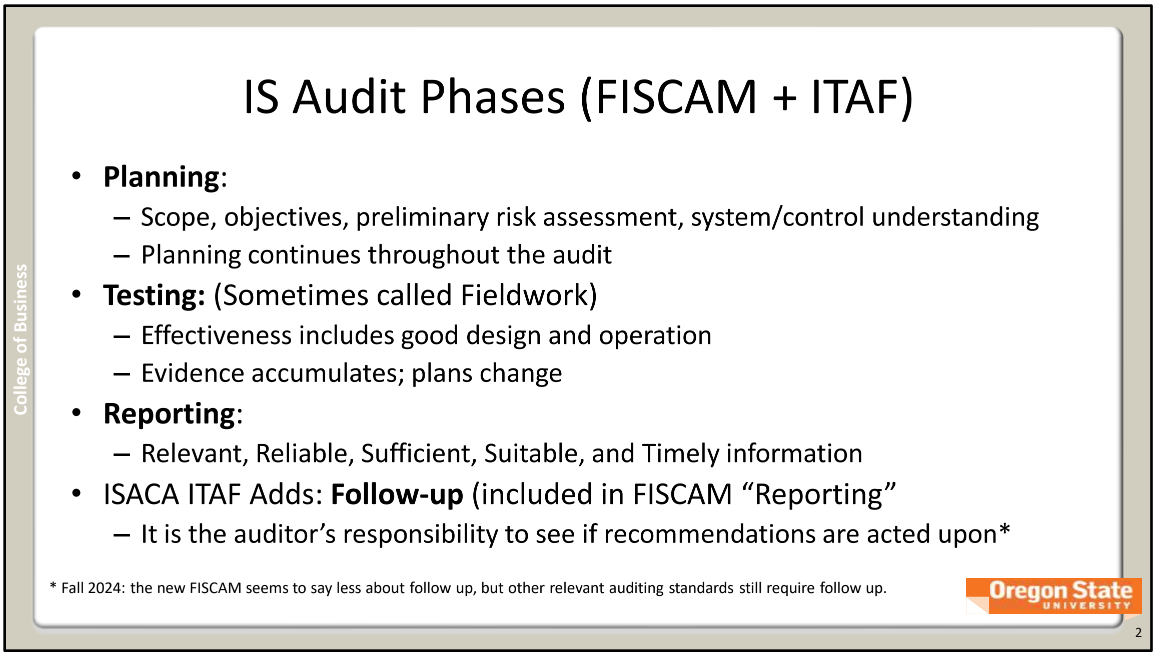
- The practice of information system auditing
- The substance of common information system risks and controls

Other IT professionals need to be able to see things from an audit perspective and communicate with auditors. What's more the very things an auditor looks for can be the difference between an ad-hoc IT risk management program and a systematic one that has a high probability of safeguarding against risks.

Previous modules have looked at:

- Internal controls
- IS audit resources that provide standards and guidance
- Risk management
- Audit risk

This module will go into more depth on conducting an audit. Although there is a good bit of information here, this still only scratches the surface. It combines approaches for IS audit with notions about commonly audited risks and controls.



College of Business

IS Audit Phases (FISCAM + ITAF)

- **Planning**:
  - Scope, objectives, preliminary risk assessment, system/control understanding
  - Planning continues throughout the audit
- **Testing:** (Sometimes called Fieldwork)
  - Effectiveness includes good design and operation
  - Evidence accumulates; plans change
- **Reporting**:
  - Relevant, Reliable, Sufficient, Suitable, and Timely information
- ISACA ITAF Adds: **Follow-up** (included in FISCAM "Reporting"
  - It is the auditor's responsibility to see if recommendations are acted upon*

* Fall 2024: the new FISCAM seems to say less about follow up, but other relevant auditing standards still require follow up.

Oregon State University

2

A well performed audit comes to well-justified conclusions; this is the key focus of all audit activities.
FISCAM notes three audit phases: Planning, Testing, and Reporting. "Testing" is often referred to as Fieldwork in audit frameworks.

When a plan is made. The auditor needs to arrange with the client so that the work that gets done looks at the right things and gathers the right evidence to confidently assess the effectiveness of the controls.

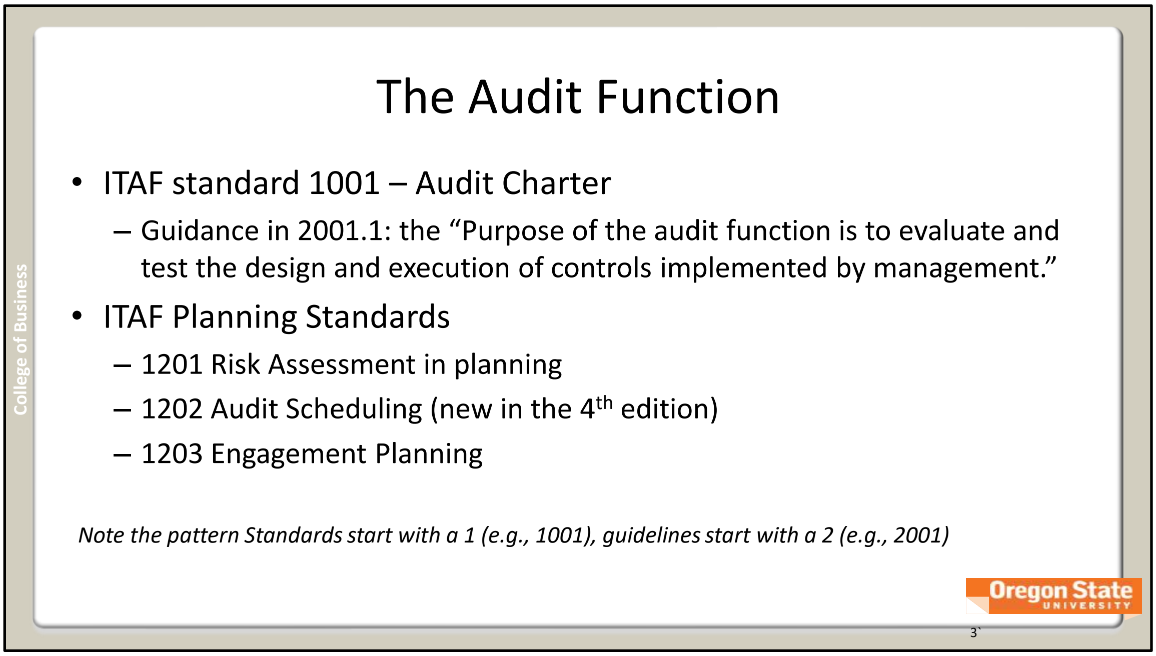
Scope is a big issue here. An auditor can be distracted by many unimportant controls. That is why auditing is risk-focused. If, for example, an organization does not do any financial transactions or important organizational business online, controls over the development and management of the web presence may not important enough to justify time spent reviewing them.

Experience is important in planning. An auditor may sit down with a client and discuss configuration management. If the ERP system is mis-configured, lots of risks ensue: errant reporting, bad decisions, or unauthorized release of data, for example. But which systems are "in scope"? There are lots of places to look including the database server that manages the information used by the ERP, the application server(s) that provide access to system functionality, the network that delivers information, and devices used by clients. It takes a lot of understanding to know which of those potential control points should be addressed.

Once the important systems and processes are identified, appropriate tests need to be planned.
Is any collectable control evidence generated? Could that evidence demonstrate that controls are effective?
Sometimes more testing is done because additional controls are needed to provide reasonable assurance. Other times testing is stopped because early failed tests indicate that some set of controls, taken as a whole, will be judged ineffective no matter how some future tests come out.

Report writing may be the most important part of all. A report has to be understandable for the audience and be convincing. Auditors don't say "It seems to me", they draw conclusions based on justified criteria and relevant, reliable, and sufficient evidence.

FISCAM includes follow up in the reporting phase. ITAF has a separate follow-up phase. In either case the auditor has a responsibility to follow up on reported control problems to see that risks are mitigated. These standards mean that hiring a certified auditor means hiring someone with a professional duty to follow up.



The Audit Function

- ITAF standard 1001 – Audit Charter
  - Guidance in 2001.1: the "Purpose of the audit function is to evaluate and test the design and execution of controls implemented by management."
- ITAF Planning Standards
  - 1201 Risk Assessment in planning
  - 1202 Audit Scheduling (new in the 4th edition)
  - 1203 Engagement Planning

Note the pattern Standards start with a 1 (e.g., 1001), guidelines start with a 2 (e.g., 2001)

College of Business

Oregon State UNIVERSITY

3`

Most large organizations have an internal audit function and many of the IT audit standards reflect this context. This function can involve employing an external audit firm to do the work but often includes internal staff. If little or no effort is put into ongoing internal audit, an external auditor has much more work to do as they conduct financial or internal control audits.

Audit departments (internal or external) operate under an audit charter which describes what they are supposed to do and accomplish. Standard 1001.1 says: "The IT audit and assurance function shall document the audit function appropriately in an audit charter, indicating purpose, responsibility, authority and accountability."

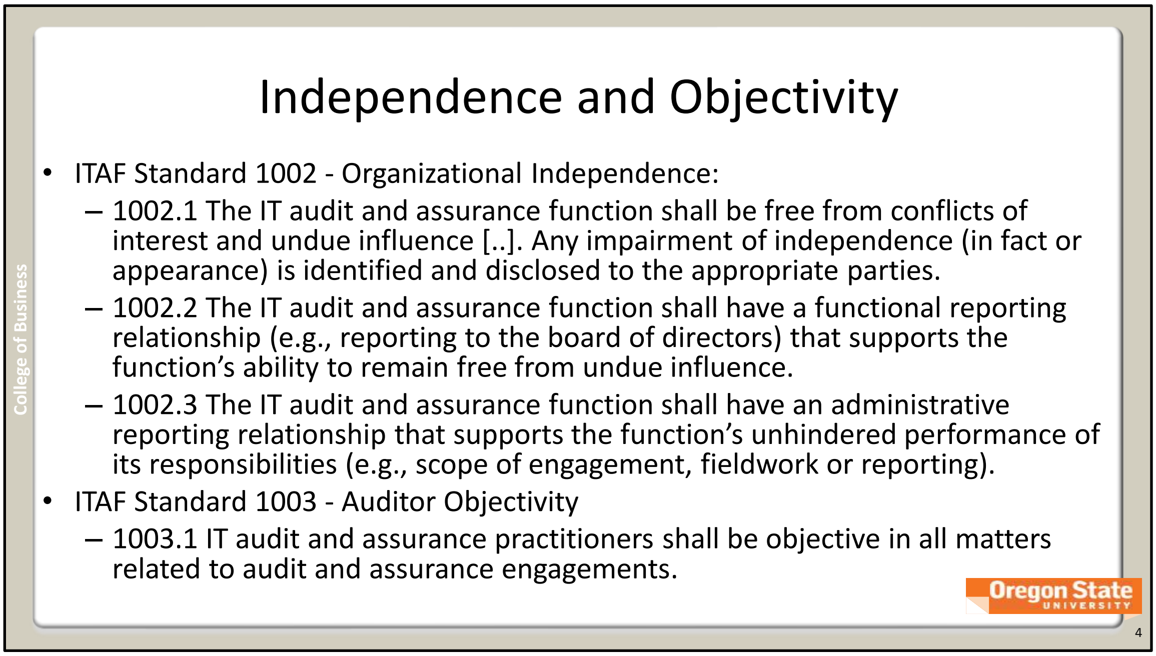
Further guidance says that the "Purpose of the audit function is to evaluate and test the design and execution of controls implemented by management." Both quotes from ITAF 4th ed. pg 17.

An audit charter covers a variety of issues about qualifications and independence, but for now, it is important to know that the charter guides the planning of an ongoing IT audit program.

The IT audit function matters!
- Findings are often reported to the board of directors.
- Financial auditors can rely on their work to ascertain the level of control risk (CR) to be used in planning the integrated audit.

Some key ideas:

- By now, it should not surprise you that risk assessment is the starting point for IT audit program planning.
- Long term planning within the audit function is important. Organizations can't test all their IT controls at once. For a variety of reasons including:
  - Such an audit would be expensive and disruptive. The IT people can't spend weeks talking to auditors; they have other work to do.
  - Controls are interrelated, what we learn in one audit impacts how other audits are conducted.
- In addition to long term planning for the audit program, auditors carefully plan each engagement.



Independence and Objectivity

- ITAF Standard 1002 - Organizational Independence:
  - 1002.1 The IT audit and assurance function shall be free from conflicts of interest and undue influence [..]. Any impairment of independence (in fact or appearance) is identified and disclosed to the appropriate parties.
  - 1002.2 The IT audit and assurance function shall have a functional reporting relationship (e.g., reporting to the board of directors) that supports the function's ability to remain free from undue influence.
  - 1002.3 The IT audit and assurance function shall have an administrative reporting relationship that supports the function's unhindered performance of its responsibilities (e.g., scope of engagement, fieldwork or reporting).
- ITAF Standard 1003 - Auditor Objectivity
  - 1003.1 IT audit and assurance practitioners shall be objective in all matters related to audit and assurance engagements.

College of Business

Oregon State UNIVERSITY

4

Perhaps the most important thing to understand about performing audits is the presumption of independent objectivity.

Internal control auditors are supposed to operate outside of influences that might skew the results.

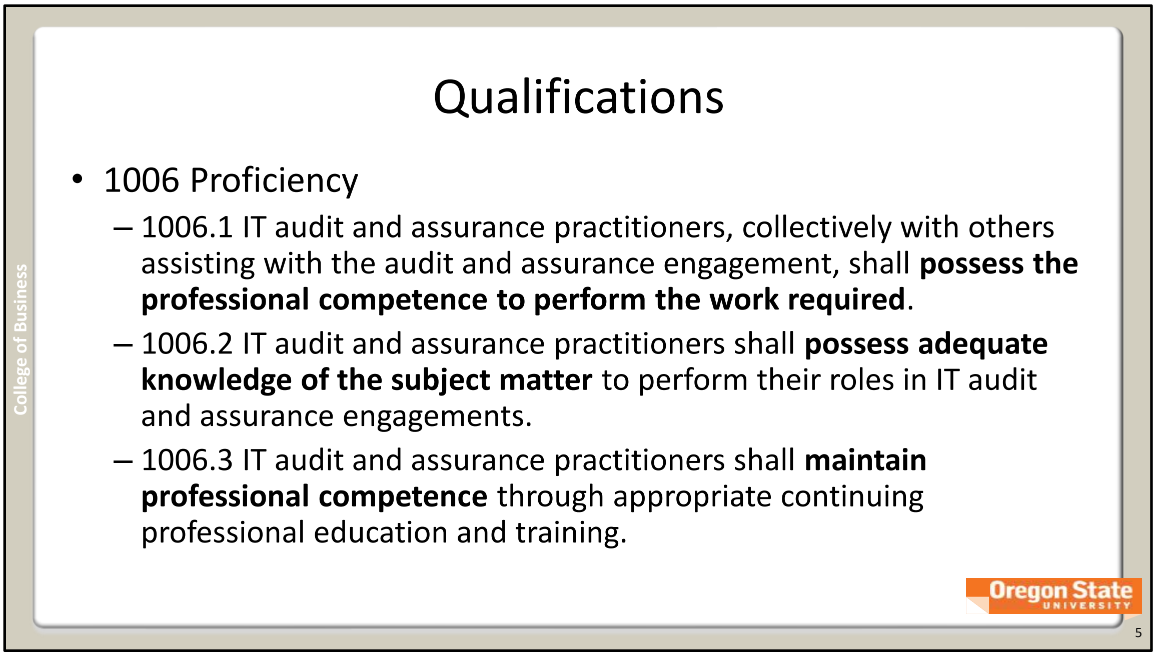
Auditors are to be independent in fact and appearance. This starts with making sure the auditor does not have a conflict of interest. If the audit function reports to management (instead of the board of directors) they may well be inclined to assess management's efforts in an overly favorable light. This is true both for internal auditors who work an organization and external auditors who are hired by the organization. They need to report to governance bodies, not to management. They also need to be administratively independent so that some administrative functionary cannot control the purse strings. Of course, spending and hiring are subject to administrative oversight, but priorities and allocation of resources to one audit effort or another need to be in independent hands. And the overall level of investment in audit is subject to board guidance.

Auditors are also supposed to be objective. It isn't about what the auditor thinks, it is about providing credible audit assurance that the internal controls provide reasonable assurance that objectives will be achieved.

Using authoritative standards to form criteria is an example of how this plays out. You will almost always see that a client "agrees" with audit findings even when they reveal shortcomings. This is not because auditors are thought to be especially insightful, it is because auditors create findings by comparing controls to authoritative sources. Its easy for a contentious manager to disagree with some auditor, but it is much harder for them to credibly say that NIST, COSO, or a CIS benchmark is wrong.

Still, it important for auditors to avoid creating unnecessarily adversarial situations. Good auditors talk with clients early about which standards are to be applied and try to take the position of verifying that what management says is true – with due skepticism – rather then starting out with a presumption that things are not as they should be.

These principles strongly influence how audits are planned and conducted.



College of Business

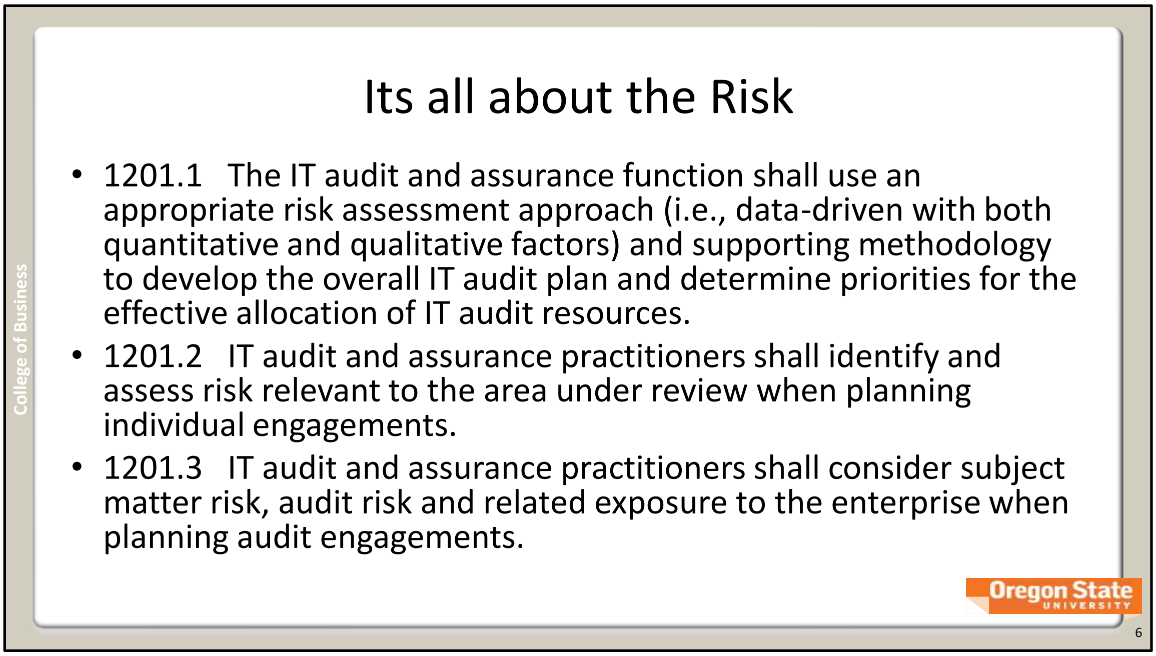
Qualifications

- 1006 Proficiency
  - 1006.1 IT audit and assurance practitioners, collectively with others assisting with the audit and assurance engagement, shall **possess the professional competence to perform the work required**.
  - 1006.2 IT audit and assurance practitioners shall **possess adequate knowledge of the subject matter** to perform their roles in IT audit and assurance engagements.
  - 1006.3 IT audit and assurance practitioners shall **maintain professional competence** through appropriate continuing professional education and training.

Oregon State University

5

Auditors need to take a good look in the mirror and consider whether or not they are qualified to do an audit. However, this could easily be taken too far. An auditor need not be expert, for example, in configuring cloud services to audit an organization’s cloud deployment. But the auditor should be up on standards for cloud deployments, be technically strong enough to understand related policy, and be familiar with cloud risks and controls generally. Since audits are driven by criteria from standards.



College of Business

Its all about the Risk

- 1201.1 The IT audit and assurance function shall use an appropriate risk assessment approach (i.e., data-driven with both quantitative and qualitative factors) and supporting methodology to develop the overall IT audit plan and determine priorities for the effective allocation of IT audit resources.
- 1201.2 IT audit and assurance practitioners shall identify and assess risk relevant to the area under review when planning individual engagements.
- 1201.3 IT audit and assurance practitioners shall consider subject matter risk, audit risk and related exposure to the enterprise when planning audit engagements.

Oregon State UNIVERSITY

6

We have talked a good bit about risk-based auditing already.
The ITAF 2201 guidelines that support this standard

- define audit, inherent, control, and detection risk,
- note the need for multiple forms of risk assessment,
- and emphasize the role or risk in audit planning.

This should be familiar ground by this point in the term.

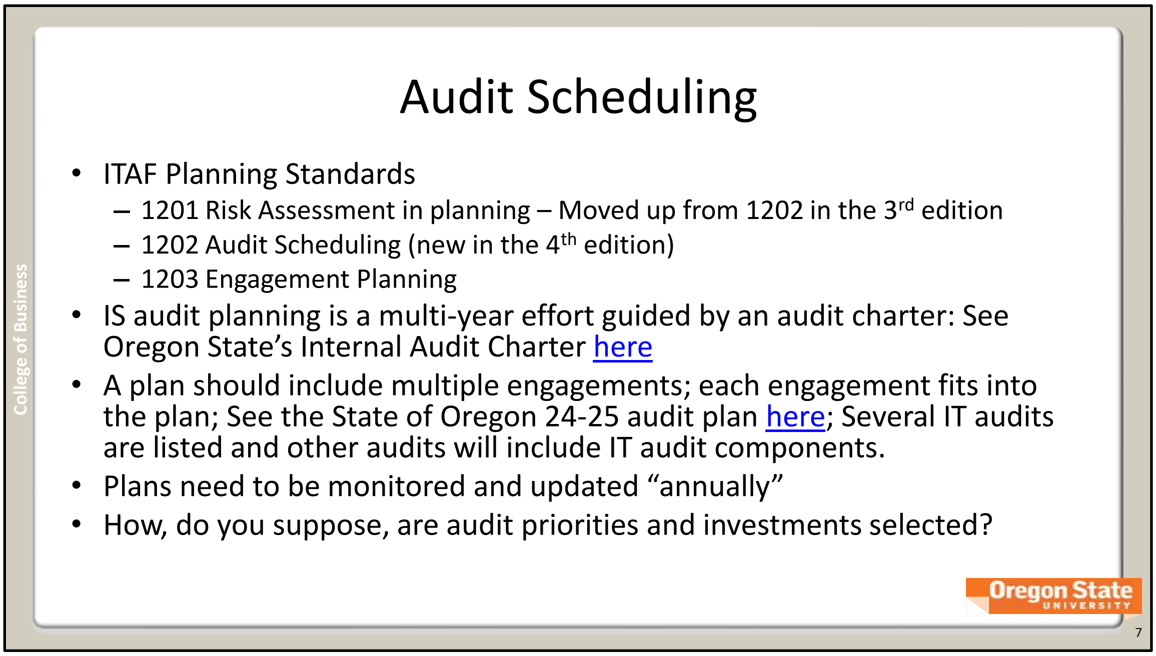
In addition to defining inherent risk guideline 2201.6.2 says: "*Since the IT auditor considers the scope of areas to be tested that affect major business systems, inherent risk is expected to be high*." ITAF pg 52
Indeed, information systems pose great risks to organizational success if they are not carefully safeguarded. Factors that influence inherent risk relevant to IT audits were discussed previously.

The 2201 guidance section includes this interesting (potentially misleading?) statement:
"*To reduce risk for higher materiality, compensate by either extending the test of controls (reduce control risk) and/or extending the substantive testing procedures (reduce detection risk) to gain additional assurance.*"

As previously discussed, additional control testing and additional substantive testing have different effects on audit risk. If we test additional controls, we may be able to support a lower level of control risk and by testing compensating (overlapping) controls we may be able to report reasonable assurance that risk is controlled even if one or more controls may be ineffective. But additional testing of the same controls does not increase assurance in the same way that additional substantive tests can.

Do you see why? If a TER of 5% is set, testing of 60 items is planned, and we might decide that the test of the control fails if we find 2 exceptions. While it is possible that a control is being properly operated and our sample wasn't representative or wasn't large enough, additional testing would only help in slightly increasing statistical power. MAYBE if we tested 240 items (4 times as many) 9 exceptions, instead of 8 (2x4) would be considered a passing score, but likely not. This is different from doing additional substantive testing of financial items. If we test 20% of all financial transactions vs 10%, we know for sure that there are not any undetected errors in the additionally tested 10%. That always lowers detection risk.

In that scenario, detection risk has definitely been reduced, whereas in the control testing scenario, CR is definitely NOT reduced, although our confidence in the CR estimate may be higher.



College of Business

Audit Scheduling

- ITAF Planning Standards
  - 1201 Risk Assessment in planning – Moved up from 1202 in the 3rd edition
  - 1202 Audit Scheduling (new in the 4th edition)
  - 1203 Engagement Planning
- IS audit planning is a multi-year effort guided by an audit charter: See Oregon State's Internal Audit Charter here
- A plan should include multiple engagements; each engagement fits into the plan; See the State of Oregon 24-25 audit plan here; Several IT audits are listed and other audits will include IT audit components.
- Plans need to be monitored and updated "annually"
- How, do you suppose, are audit priorities and investments selected?

7

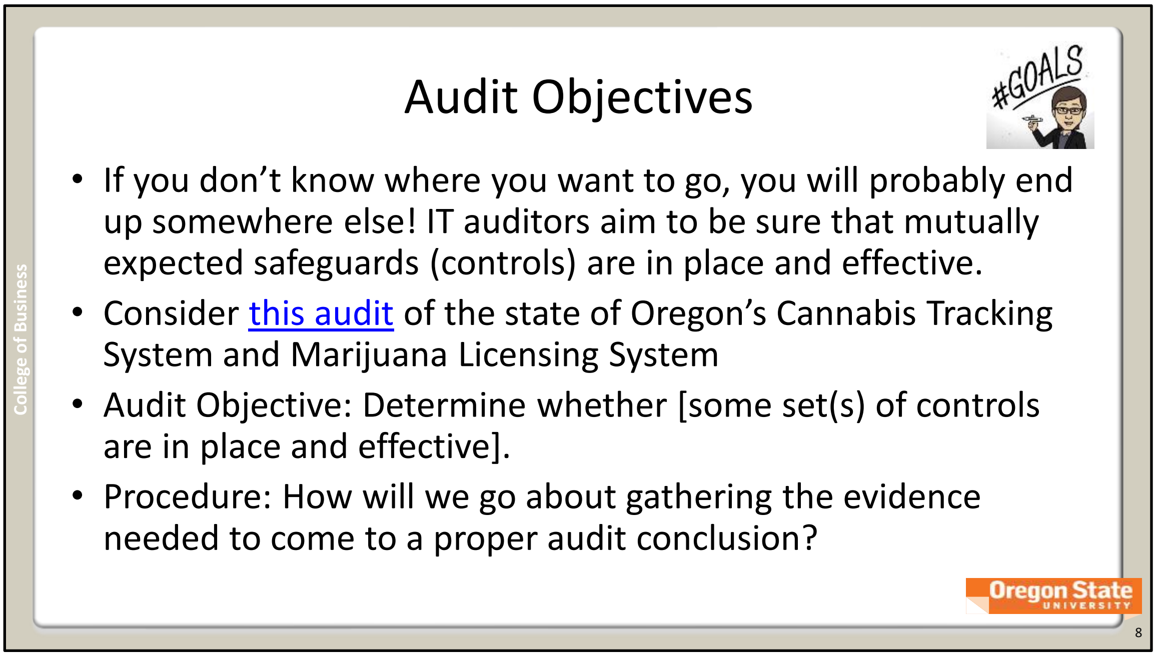
Standard 1202.: "*1202.1 The IT audit and assurance function shall establish an overall strategic plan resulting in short-term and long-term audit schedules. Short-term planning consists of audits to be performed within the year, while long-term planning is comprised of audits based on risk-related matters within the enterprise's information and technology (I&T) environment that may be performed in the future.*" 2202 guidance notes: "*IT audit [..] practitioners shall develop [..] an audit schedule that is based on an inventory of audit areas, often referred to as the audit universe*."

Organizational IS auditing needs to systematically cover the breadth of IS risk for the organization. This does not happen in one audit engagement. Instead, based on a variety of factors, auditors set a course to address the major areas of risk over time. IS is understood to be delivered by a series of controlled processes. And while organizations vary a lot, these processes are similar across most organizations. Here are some common examples: Identity and access management; System development lifecycle and change management; Configuration management; Security management; Contingency planning; and Business process controls.

How might an auditor decide which things to look at first? Judgement. Considerations:

- Risk! Having effective controls for the biggest risks is really important. Identify weaknesses sooner rather than later.
- Management: If an organization gets a new CISO (Chief information security officer) that might be a bad time to do a security program audit. It might be inefficient because security personnel are just figuring things out or the processes and controls might be changing. OR – it might be a good time to do the audit to help the CISO act on the biggest risks first.
- Organizational changes: Changing operations means changing risk profiles. If, for example, a University expands its online offerings, cybersecurity and network management processes might become more important. Both the likelihood and the impact of negative events would increase.
- Resources: It is not easy to hire good IS auditors – especially if they have skills in high-demand areas such as analytics or cybersecurity. Maybe the audit team has only one person capable of reviewing cybersecurity processes – or maybe they have none. You can hire external auditors – a common practice – but your budget probably does not allow you to cover all the areas at once and internal auditors – and the information system staff – can only coordinate so many things at any one time.
- Organizational priorities: Board members may become aware of hot button concerns in an industry. Managers may want to shine a light on particular concerns. Or negative events may spur awareness.

Do you see why the plan needs to be updated annually? These sorts of factors don't remain constant.
As noted in 2202.2: "*Long-term audit schedules should be reevaluated on a periodic basis (at least annually) to be responsive to organizational needs. This reevaluation allows the audit function to include any additional assurance and audit engagements that may be required in response to unexpected critical events or situations. Any replaced planned audits should be reassigned to a future period.*" All quotes from pg 55 of the ITAF



Audit Objectives

- If you don't know where you want to go, you will probably end up somewhere else! IT auditors aim to be sure that mutually expected safeguards (controls) are in place and effective.
- Consider this audit of the state of Oregon's Cannabis Tracking System and Marijuana Licensing System
- Audit Objective: Determine whether [some set(s) of controls are in place and effective].
- Procedure: How will we go about gathering the evidence needed to come to a proper audit conclusion?

College of Business

Oregon State University

8

Because audits are supposed to result in justified and useful results, the auditor needs to be clear on what the audit is supposed to accomplish. As stated in 2203.2.1: "*Practitioners should define the audit engagement objectives and document them in the audit engagement project plan. In addition to confirming an understanding of the enterprise's goals, operations and challenges, documentation of the audit engagement objectives ensures that testing lends assurance that controls are in place and operating effectively.*" ITAF pg 57

Think about the difference between the terms "accomplish" and "perform".
Audit objectives (what is to be accomplished) come before Audit procedures (what we are to do).
Examples of audit objectives from an Oregon Secretary of State Audit Division review of the Cannabis Tracking System and Marijuana Licensing System (https://sos.oregon.gov/audits/documents/2018-07.pdf) include:
Determine whether management has implemented:

- *a security management program with supporting policies and procedures to ensure that computer resources are protected against known vulnerabilities and physical threats; and*
- *sufficient computer controls over the Cannabis Tracking System and Marijuana Licensing System to support the regulation of the recreational marijuana programs according to current law.*

Then they summarize the audit procedures performed:
To fulfill our audit objectives we conducted interviews with department personnel, observed department operations, and examined available system documentation. We also evaluated or tested:

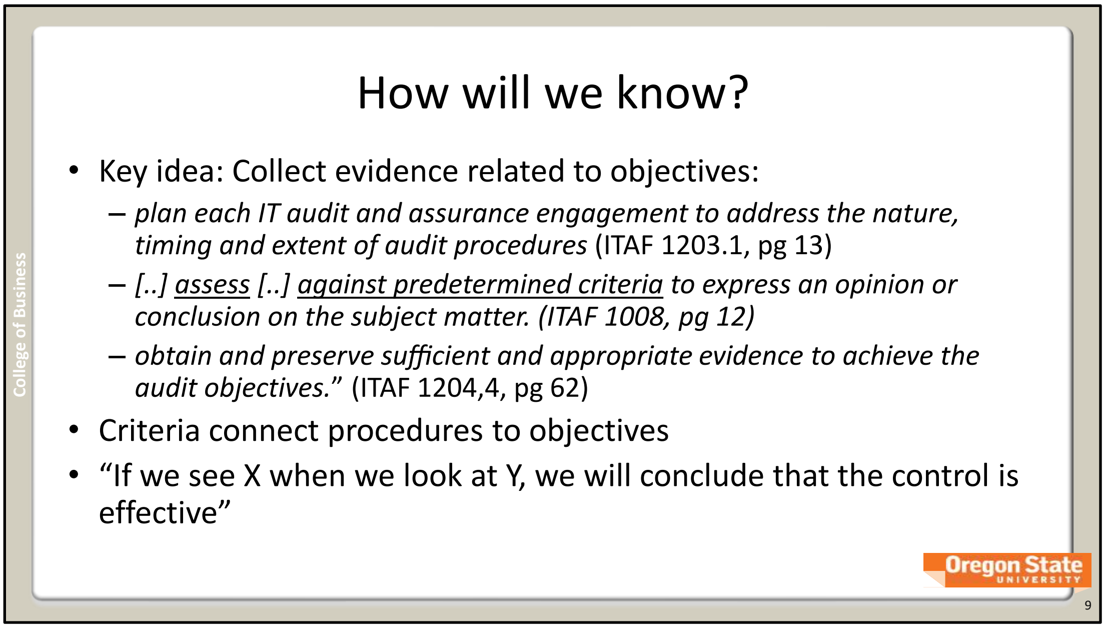
- *policies and procedures governing security management; and*
- *policies and procedures over contingency planning, disaster recovery, and system and data backups;*
- *and more.*

Compare the two lists and think a bit.

- Objectives here begin with "Determine whether" – it's about making determinations. There are lots of way to say this, but the main idea is about interpreting appropriate evidence so as to come to a reliable conclusion.
- Procedures are more diverse and active: interview, observe, examine, evaluate, test, review.

Management controls, auditors verify. Do you see the connection here? Audit objectives generally aim to see if identified control objectives have been met. Auditors don't come in to look around for problems so much as they come in to see that known problems are appropriately addressed.

** Audit objective language on the slide was altered/improved 10/31/2023 after reviewing student work*



How will we know?

- Key idea: Collect evidence related to objectives:
  - *plan each IT audit and assurance engagement to address the nature, timing and extent of audit procedures* (ITAF 1203.1, pg 13)
  - *[..] assess [..] against predetermined criteria to express an opinion or conclusion on the subject matter. (ITAF 1008, pg 12)*
  - *obtain and preserve sufficient and appropriate evidence to achieve the audit objectives.*" (ITAF 1204,4, pg 62)
- Criteria connect procedures to objectives
- "If we see X when we look at Y, we will conclude that the control is effective"

Given objectives (Determine whether…), an auditor needs to design audit procedures (things to do) that will result in appropriate evidence. Auditors need to be systematic. They don't just snoop around till they feel convinced. They identify, in advance, what it would mean for evidence to be sufficient and appropriate.

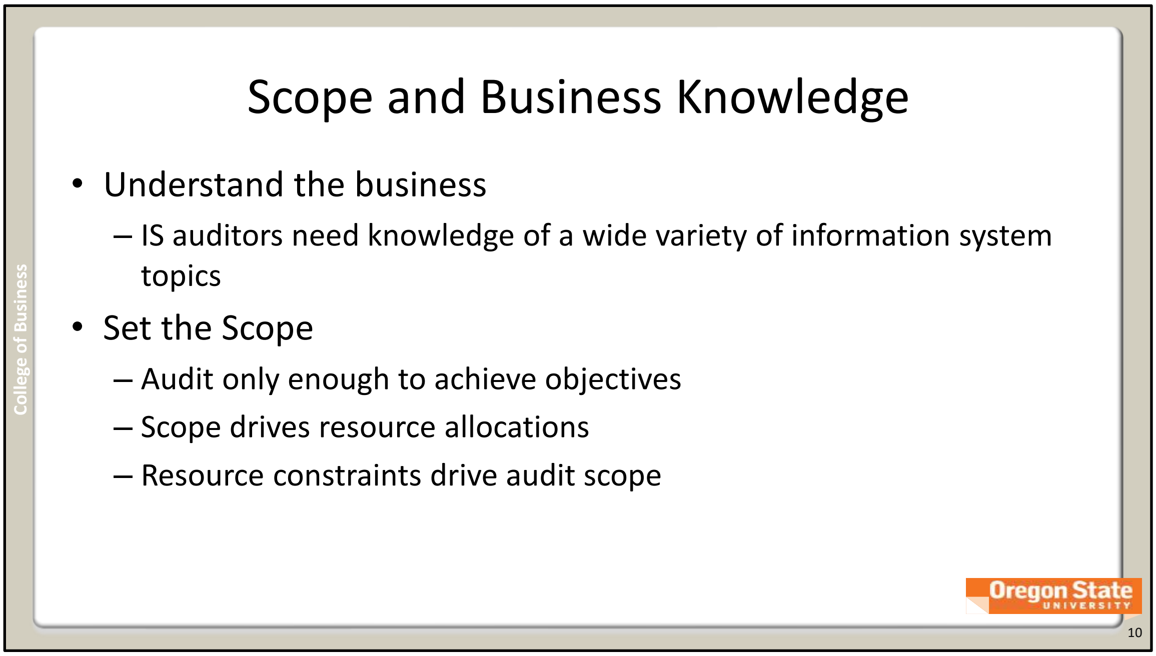
What would the auditors in the Cannabis audit need to observe in the "policies and procedures governing security management" to provide appropriate and sufficient evidence to conclude that they "ensure that computer resources are protected against known vulnerabilities and physical threats"? Although the policies and procedures are a key source of evidence, the evidence would come from multiple sources.

While we do not have access to all the details of the security audit, the SOS (Secretary of State) audit team found that "*OLCC lacks an up-to-date security plan*". Why would they call out that particular detail?

1. SOS relies, in part, on FISCAM and related NIST documents to describe how systems are to be controlled. If FISCAM says a particular practice "should" be in place, that constitutes a compelling audit criterion. FISCAM refers to NIST 800-53.
2. FISCAM (starting on page 155) lists expectations (standards) required of security management programs in support of the audit objective "*determine whether…*" "*the security management program is adequately documented, approved, and up-to-date*". In the following pages, the text of FISCAM mentions "*security plans*" dozens of times.
3. So, because FISCAM (and, by reference, NIST 800-53) is deemed authoritative here, and because it specifies requirements for security plans, a system without a security plan would be considered to be deficient.
4. Of course judgement also applies.
   1. An auditor would need to consider the risk; maybe a security plan would be considered unnecessary in some cases.
   2. Or maybe a different standard (something besides FISCAM) would be more appropriately authoritative.
   3. Or maybe less formal document would suffice as a 'security plan'.

A reader should be able to see why the auditor called out a particular control weakness, and then, why these particular criteria were used to plan the audit and arrive at conclusions. The head of the administrative department, the governor, and the legislature is likely to conclude that FISCAM/NIST is an appropriate source of criteria.

In this case, additional security audit procedures might have been cancelled if a mere yes or no answer was all that was to be provided. The lack of a security plan means that no matter what other activities are happening, the criteria have not been met. The lack of a plan is, by itself, sufficient evidence to determine that adequate protection is NOT in place. However, IT audits also seek to help an organization improve safeguards. Maybe the plan exists informally. They can look to see if some activities that would be called for in a security plan are being done to provide additional useful evaluation.



Scope and Business Knowledge

- Understand the business
  - IS auditors need knowledge of a wide variety of information system topics
- Set the Scope
  - Audit only enough to achieve objectives
  - Scope drives resource allocations
  - Resource constraints drive audit scope

College of Business

10

Processes use organizational assets intending to achieve goals.

We have talked a lot about risk. Risk is different in different organizations, even for similar processes.

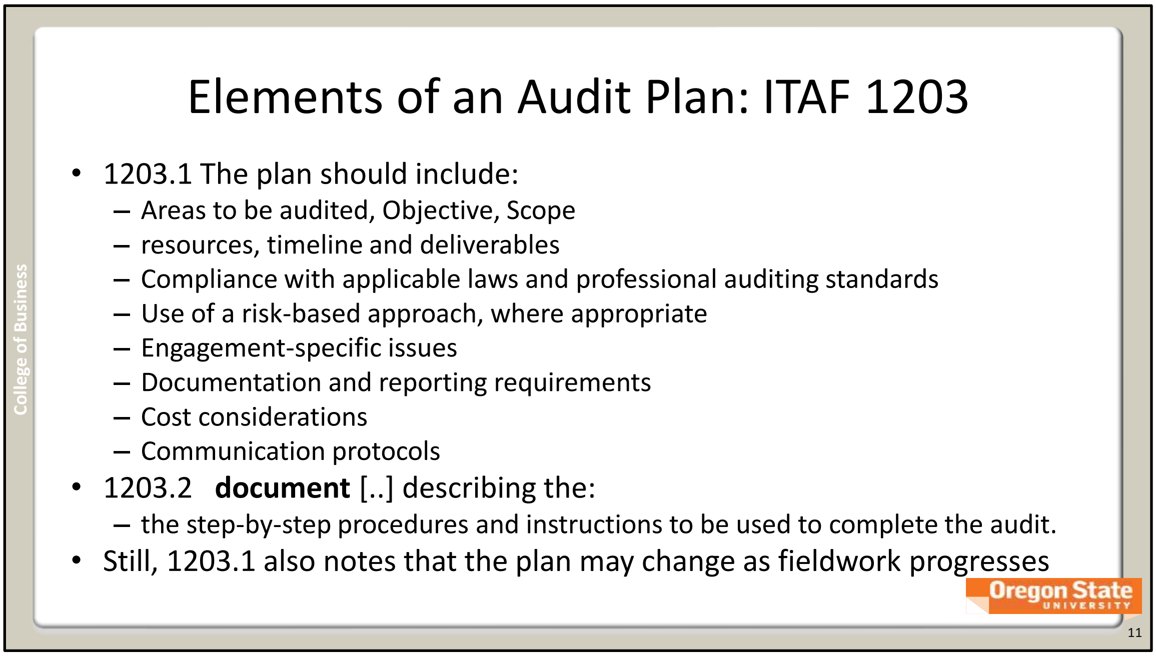
So, auditors need to understand how the process fits into the organization.
For example:

- If you are looking at cybersecurity or identity and access management, you need to know what systems are protected and what, in those systems, is worth protecting.
- If you are looking at configuration management, you need to understand what kinds of traffic goes through a network and what kinds of business systems are run on the configured devices.
- If you are looking at acquisition or decommissioning of information systems or system components, you need to understand what those systems and components do. How crucial are response times, reliability, privacy, and integrity?
- And so on.

This is why IT auditors need to develop knowledge of a wide variety of information systems.

This understanding is important in assessing scope.
Perhaps for our purposes it is enough to say that:

- Determining scope is crucial – you can't decide what resources (this often means people assigned to the audit) you need to deploy if you don't know what needs to be tested.
- Determining Scope is hard. Experience helps a lot.
- Audit objectives drive scope. Audit only what we need to audit to obtain reasonable assurance over the tested assertions.
- Audit scope is sometimes driven by resource constraints. Some things may have to wait till next year.



College of Business

Elements of an Audit Plan: ITAF 1203

- 1203.1 The plan should include:
  - Areas to be audited, Objective, Scope
  - resources, timeline and deliverables
  - Compliance with applicable laws and professional auditing standards
  - Use of a risk-based approach, where appropriate
  - Engagement-specific issues
  - Documentation and reporting requirements
  - Cost considerations
  - Communication protocols
- 1203.2 **document** [..] describing the:
  - the step-by-step procedures and instructions to be used to complete the audit.
- Still, 1203.1 also notes that the plan may change as fieldwork progresses

Oregon State UNIVERSITY

11

ITAF standards address audit plans. These statements are from ITAF 1203. (p56 in the 4th ed.)

Previous slides covered objectives and scope. And they mentioned deployment of auditing resources (usually people).
You are beginning to become familiar with auditing standards and the centrality of risk assessment.

Each engagement will have its own details as you can see from the audit report mentioned earlier.

It is crucial that these elements be documented in the plan.

While we hope that audits are happy experiences, the reality is that many clients feel threatened by audits. Being able to work with nervous clients is a key skill for a successful auditor. Don’t channel Darth Vader.

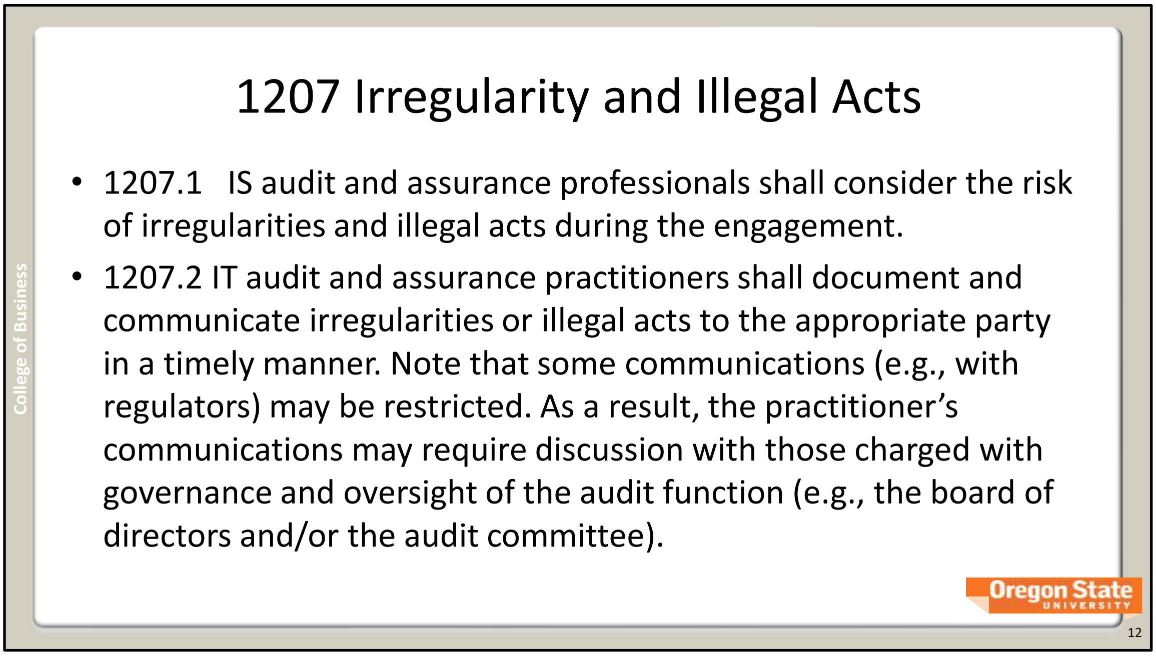
- Audits often reveal control weaknesses that have implications for people’s jobs. Managers who do not effectively control risk may be sanctioned. Employees in ineffective departments may fear the result of negative findings. Nevertheless, audits need to provide meaningful reports with well-supported conclusions.

- Managers get to respond to audit findings. Good audit documentation leads to good responses. The 15 page response at the end of the Oregon Liquor Commission audit report include: “We agree with the conclusions and are implementing…” instead of bickering “The findings are not right or not relevant…” It hard to argue with a well-written report from a properly done audit.

The point here is that good documentation can help the audit lead to process improvements rather than squabbles. Recalling the Star Wars metaphor, an auditor would rather be Princess Leia (striving for a bright future) than Darth Vader.

Further, engagements need to be documented to facilitate macro audit planning. For example, large organizations such as Intel may have a dozen IS auditors flying all over the world in support of its multi-annual audit plan. Getting auditors to the right place and having the clients properly prepared to provide needed information involves lots of logistics. Well documented reports this year can mean more efficient and effective audits in future years.

Despite the best efforts of experienced auditors, plans are changed as audits proceed. The guidance provided in ITAF addresses this noting that the plan should be updated. The planning process is continual and iterative (steps repeat), and should allow for unexpected events. Changes are to reflect risk-based priorities.



1207 Irregularity and Illegal Acts

- 1207.1 IS audit and assurance professionals shall consider the risk of irregularities and illegal acts during the engagement.
- 1207.2 IT audit and assurance practitioners shall document and communicate irregularities or illegal acts to the appropriate party in a timely manner. Note that some communications (e.g., with regulators) may be restricted. As a result, the practitioner's communications may require discussion with those charged with governance and oversight of the audit function (e.g., the board of directors and/or the audit committee).

College of Business

Oregon State UNIVERSITY

12

Auditor responsibility to detect fraud is an important consideration in terms of auditor liability.
The standards can't really address all of that and we will not go deeply into this topic in this course.

Guidance element 2207.6.1says: "*Practitioners have no explicit responsibility to detect or prevent illegal acts or irregularities, but they should design procedures for the audit engagement that take into account irregularities and illegal acts that have been identified*"

A few things are clear:

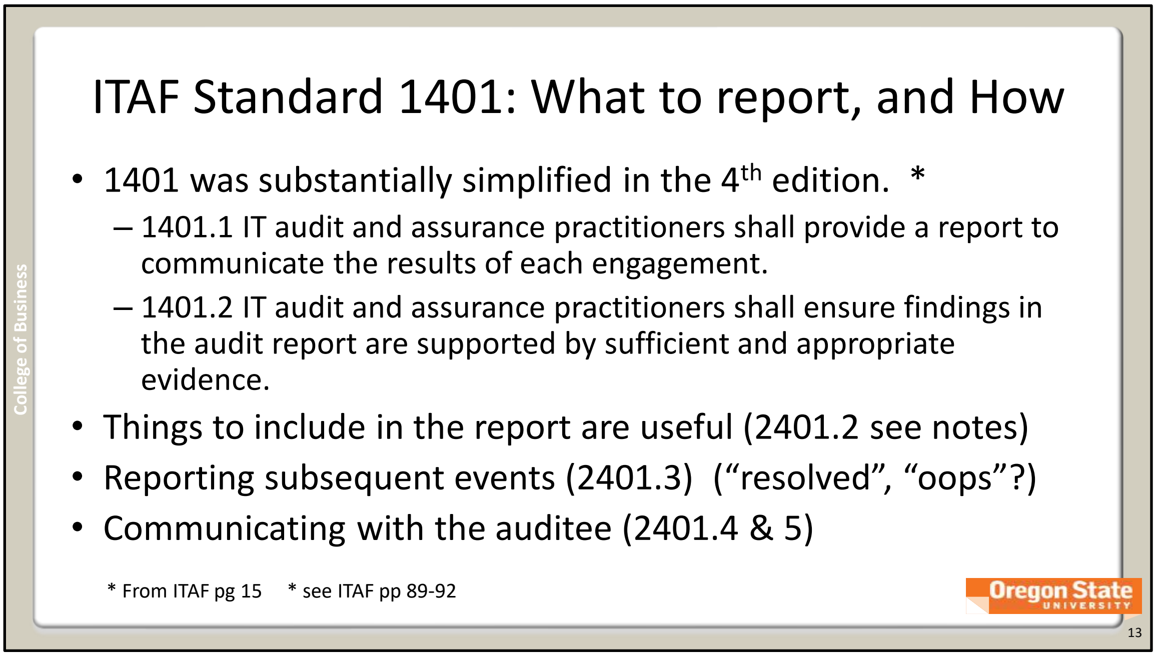
- The auditor should be thinking about how a nefarious person might commit fraud as they plan and perform audit procedures.
- The auditor should be skeptical. Be professional, but also inquisitive.
- If illegal acts or irregularities are discovered in the course of an audit, they have to be reported.

This can get tricky:

- Even properly-planned audits can fail to catch issues in the face of collusion or other systematic deceptions.
- Figuring out who to report to can be tricky when your audit client is involved.

Auditors can and should withdraw from an audit if they cannot achieve reliable findings because of material errors, control deficiencies, misstatements or illegal acts. "*Consider withdrawing from the engagement if material errors, control deficiencies, misstatements or illegal acts affect the continued performance of the engagement.*" (2207.10.1 - p.87) However, this does not mean that audits can never be completed if fraud was present.

The 4th version of the ITAF standards had a couple of changes in this area. In the 3rd edition the need for "professional skepticism" was called out in its own standard item (1207.2) and the standard item about communicating irregularities (see 1207.2 above) was much shorter. But these are not big changes. The reality is that coming across fraud or other irregularities is a somewhat ambiguous area for an auditor. They can't be expected to catch all possible carefully planned deceptions, but they need to plan so that many would come out during the audit. And, they need to respect the people involved AND report to appropriate authorities.



College of Business

ITAF Standard 1401: What to report, and How

- 1401 was substantially simplified in the 4th edition. *
  - 1401.1 IT audit and assurance practitioners shall provide a report to communicate the results of each engagement.
  - 1401.2 IT audit and assurance practitioners shall ensure findings in the audit report are supported by sufficient and appropriate evidence.
- Things to include in the report are useful (2401.2 see notes)
- Reporting subsequent events (2401.3) (“resolved”, “oops”?)
- Communicating with the auditee (2401.4 & 5)

* From ITAF pg 15 * see ITAF pp 89-92

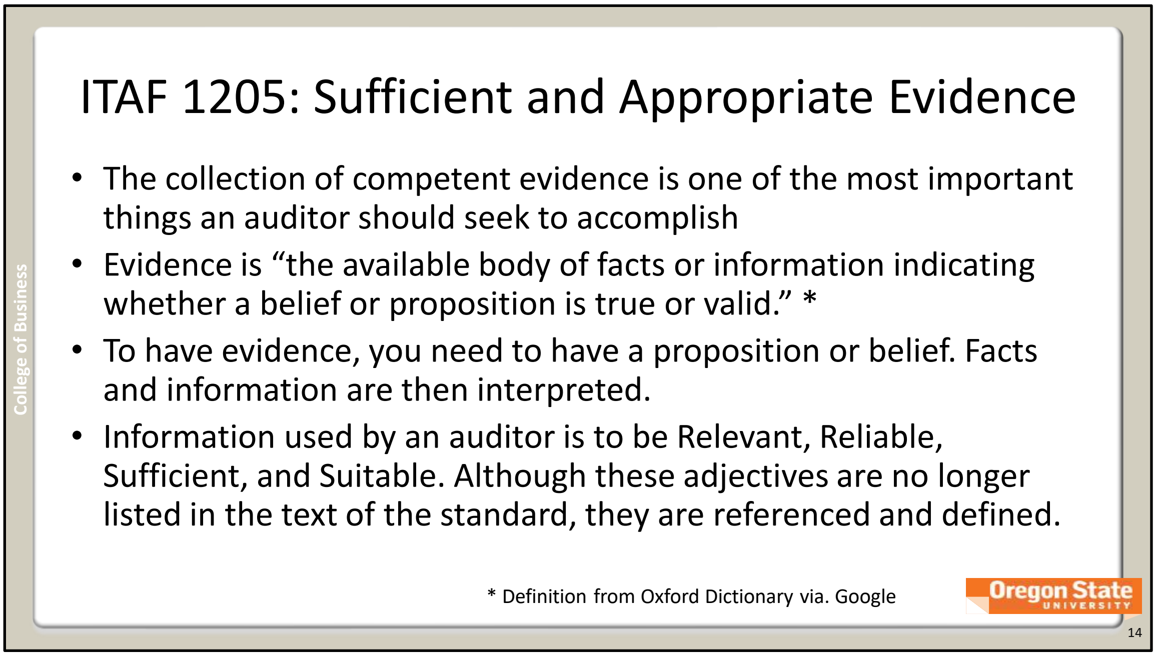
13

These reporting standards seem pretty obvious.
But it is nice to have specific guidance. You don’t need to remember which item number goes with each item, but you should have a good idea what is to be included in a final report.

- 2401.2.2 Summarize the work that was done
- 2401.2.3 Include a section with the opinion of the auditor, based on evidence, as to whether the design and/or operation of control procedures in relation to the area of activity were effective.
- 2401.2.4 Say that internal control is management’s responsibility and where management assertions are documented
- 2401.2.5 Identify the audit objectives
- 2401.2.6 List criteria, or at least the source of the criteria
- 2401.2.7 Recipients and distribution of the report
- 2401.2.8 Signatures and locations of the individuals or entities responsible for the report
- 2401.2.9 The date the report was issued and when the work was done
- 2401.2.11 Findings, conclusions, and management response.

2401 also talks about issues such as:

- 2401.3 Subsequent events (Things that happen after the work was done but before the report was issued)
  - You don’t want an audit report that is already obsolete before it is published.
- 2401.4 and .5 What to communicate to the auditee
  - Show the auditee the results before you publish, maybe you have something wrong, at least they get to respond.



College of Business

ITAF 1205: Sufficient and Appropriate Evidence

- The collection of competent evidence is one of the most important things an auditor should seek to accomplish
- Evidence is "the available body of facts or information indicating whether a belief or proposition is true or valid." *
- To have evidence, you need to have a proposition or belief. Facts and information are then interpreted.
- Information used by an auditor is to be Relevant, Reliable, Sufficient, and Suitable. Although these adjectives are no longer listed in the text of the standard, they are referenced and defined.

* Definition from Oxford Dictionary via. Google

Oregon State University

14

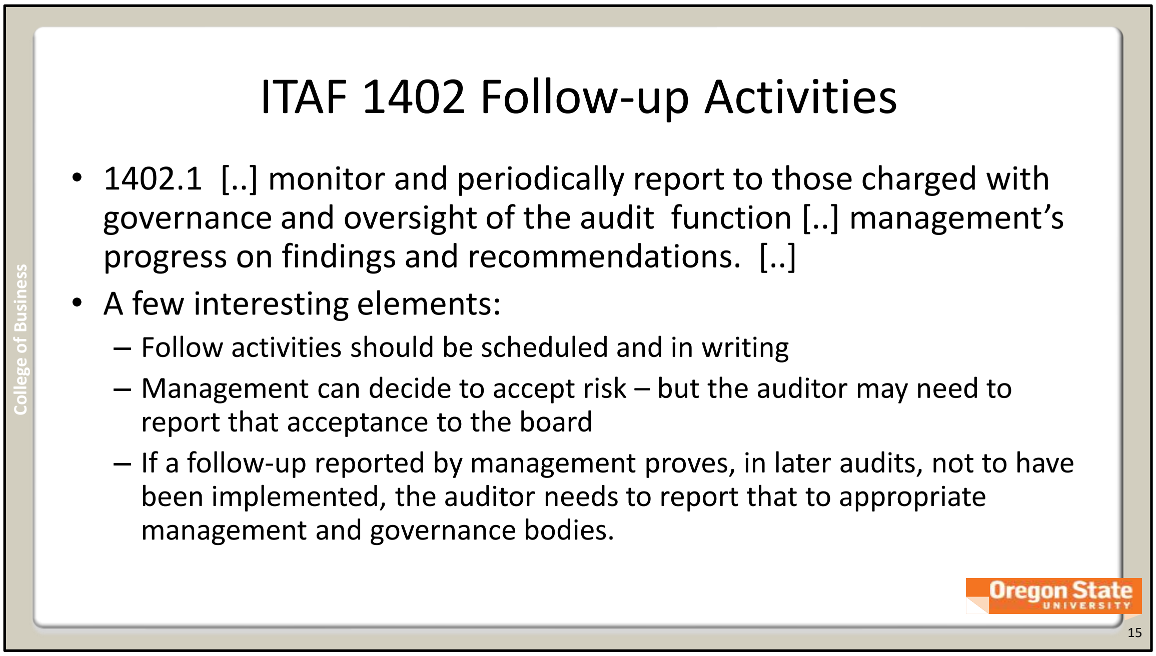
Societies have always struggled to interpret the world around them in ways that are accepted as true and valid. I am not sure people are actually good at coming to such conclusions. Auditors need to take special care to exclude bias and conjecture from their work.

Solid evidential logic starts with relevant, reliable, sufficient, and suitable information. Such information needs to be collected. The information is interpreted as evidence that a control objective has or has not been met. This interpretation achieves the audit objective.

Various parts of the ITAF document discuss qualities that supporting information is to have. Some definitions are in Appendix C: Terms and Definitions. Some of these are from COBIT 2019.

- Relevant information: Relating to controls, tells the evaluator something meaningful about the operation of the underlying controls or control component. Information that directly confirms the operation of controls is most relevant. Information that relates indirectly to the operation of controls can also be relevant, but is less relevant than direct information.
- Reliable information: Information that is accurate, verifiable and from an objective source.
- Sufficient information: Information is sufficient when evaluators have gathered enough of it to form a reasonable conclusion. For information to be sufficient, however, it must first be suitable.
- Suitable information: Relevant (i.e., fit for its intended purpose), reliable (i.e., accurate, verifiable and from an objective source) and timely (i.e., produced and used in an appropriate time frame) information.

Controls are then judged to be as strong as expected in the audit plan, or not as strong based on systematic interpretation of this kind of solid evidence.



ITAF 1402 Follow-up Activities

- 1402.1 [..] monitor and periodically report to those charged with governance and oversight of the audit function [..] management's progress on findings and recommendations. [..]
- A few interesting elements:
  - Follow activities should be scheduled and in writing
  - Management can decide to accept risk – but the auditor may need to report that acceptance to the board
  - If a follow-up reported by management proves, in later audits, not to have been implemented, the auditor needs to report that to appropriate management and governance bodies.

Auditors have an ongoing responsibility to follow up on internal control problems.

If you take on an audit and there are previous audit findings related to weak controls, you need to find out about it. Findings don't just go away because you bring in a new auditor. As an auditor, it is your responsibility to ask questions of the client. If answers are not forthcoming or are deceptive, you may have to withdraw and report your findings to the appropriate level within the organization.

Sometimes management may decide not to fix some control weakness. "Accepting" a risk is a legitimate response. But it should be done by the right people – often the board. It should be documented. And, if the auditor thinks the risk is excessive, that, too, should be reported. This was elevated to a standard in the 4th edition (see 1402.3, ITAF pg 15)

Here is some discussion or perhaps musing on this topic.
Standards (such as 1402 shown here) are supported in the ITAF by corresponding guidelines. 2402 guidelines relate to 1402 standards.
I found the 2402 guidance to be especially detailed – they are four pages long.
Perhaps it is because it is entirely too easy for a client to pressure an auditor to move on. We know that an auditor must maintain their independence and report their findings. But perhaps it is harder for the auditor to keep following up or to take on concerns noted by previous auditors. Because expectations are listed so clearly in the standards, an auditor has a solid reason to persist in follow up activities. They can say "My duty as a CISA requires that I follow up. If I don't, I am violating specific and recognized professional standards and am subject to having my certification revoked."
In a way, this puts the auditor "on the side" of encouraging strong internal control despite management's inevitable temptation to cut corners.