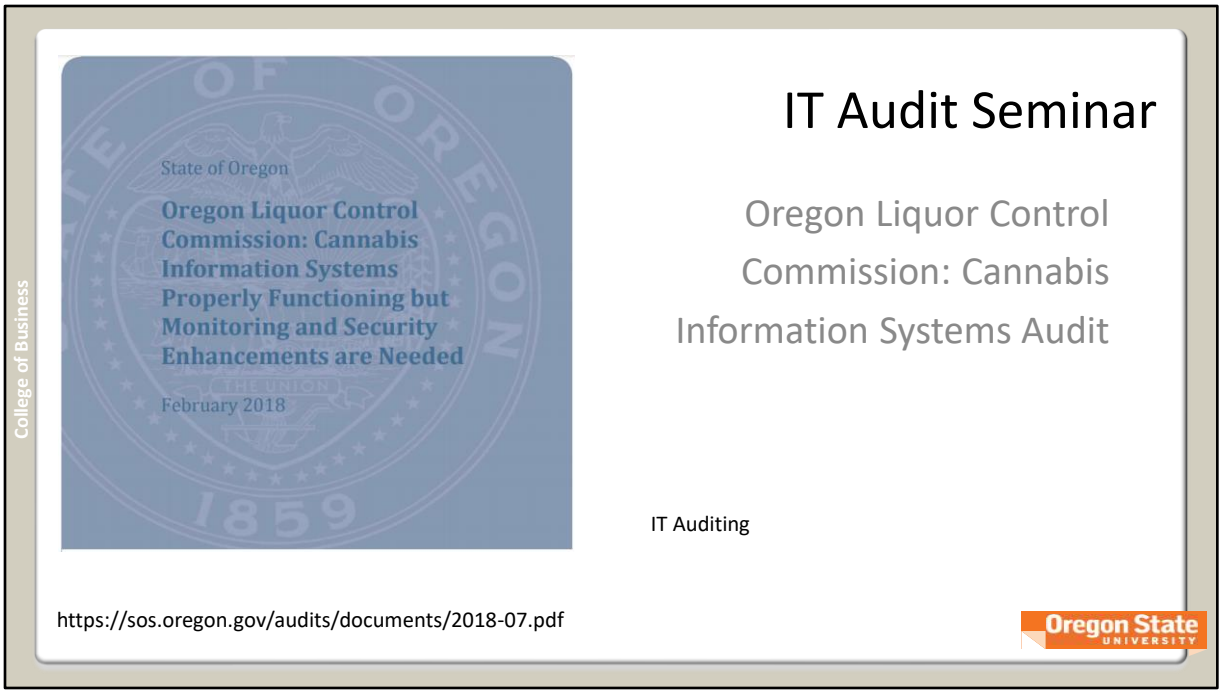
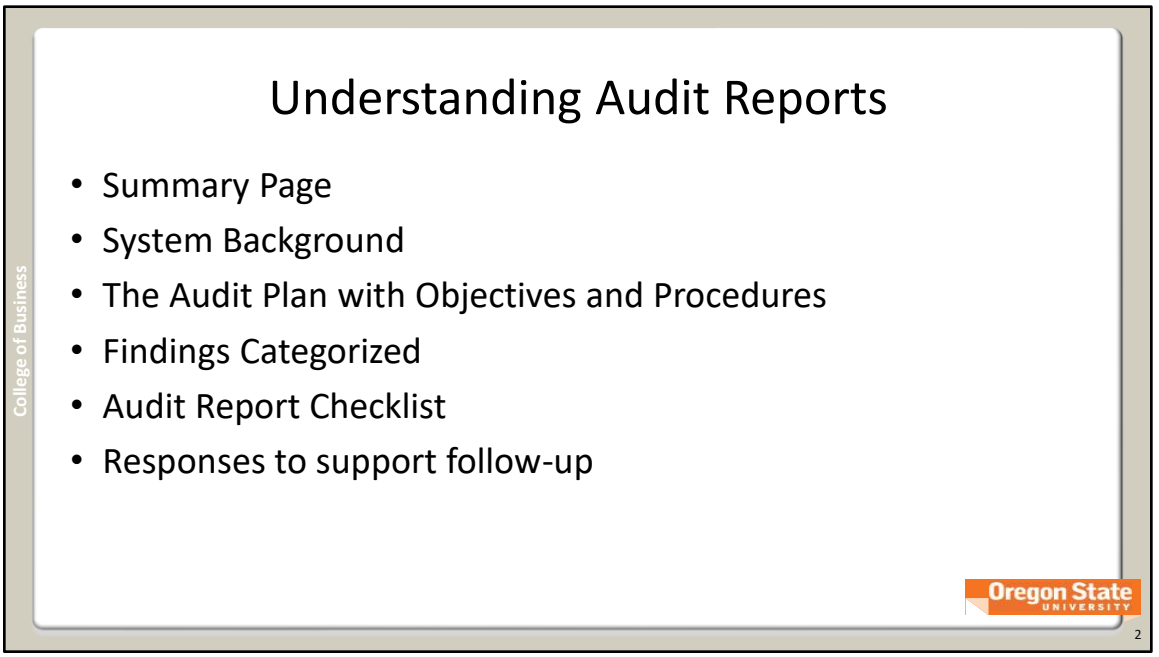


The difference between theory and practice is a lot more in practice than in theory. Or so they say.

This exercise calls on you to review a real performance audit done by real auditors, some of whom are graduates of OSU's college of business.

The idea is for you to connect with concrete examples that relate to course materials on how audits are conducted. Notably:

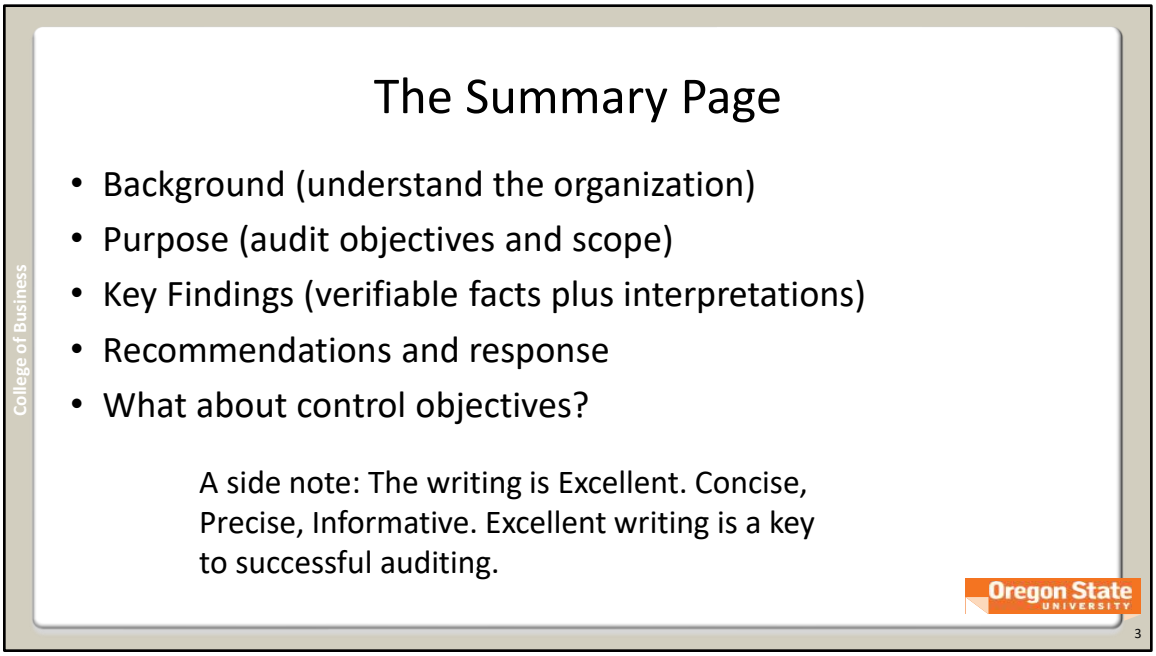
- Formulation of audit objectives and audit procedures
- Careful use of authoritative guidance to establish criteria
- Scope that starts with objectives and flows to systems
- Coverage of common IT audit topics
- Reporting content and structure
- The facilitation of follow-up activities
- Good writing: Precise, concise, and informative



This slide deck was designed to help students review material on conducting IS audits.

Key themes from the course are illustrated. See if you can recognize them as we go along.

- Consider business processes and IS processes, audits focus on organizational risk.
- Auditors need to understand the system and organization to perform an audit.
- Audits are carefully planned to achieve identified objectives through identified procedures. These are driven by the chosen audit scope.
- Findings reflect established criteria and are closely connected to organizational objectives.
- Recommendations are communicated concretely. Responses are specified to support follow up.



This summary, all by itself, conveys a tremendous amount of actionable information in a single page.

Consider what it means to write well:
- Concise: don't use too many words
- Precise: Use terms exactly as per their meaning
- Informative: Include relevant details in support of meaningful conclusions

All the information on the summary page is important. First, think about audit objectives. The purpose statement is:

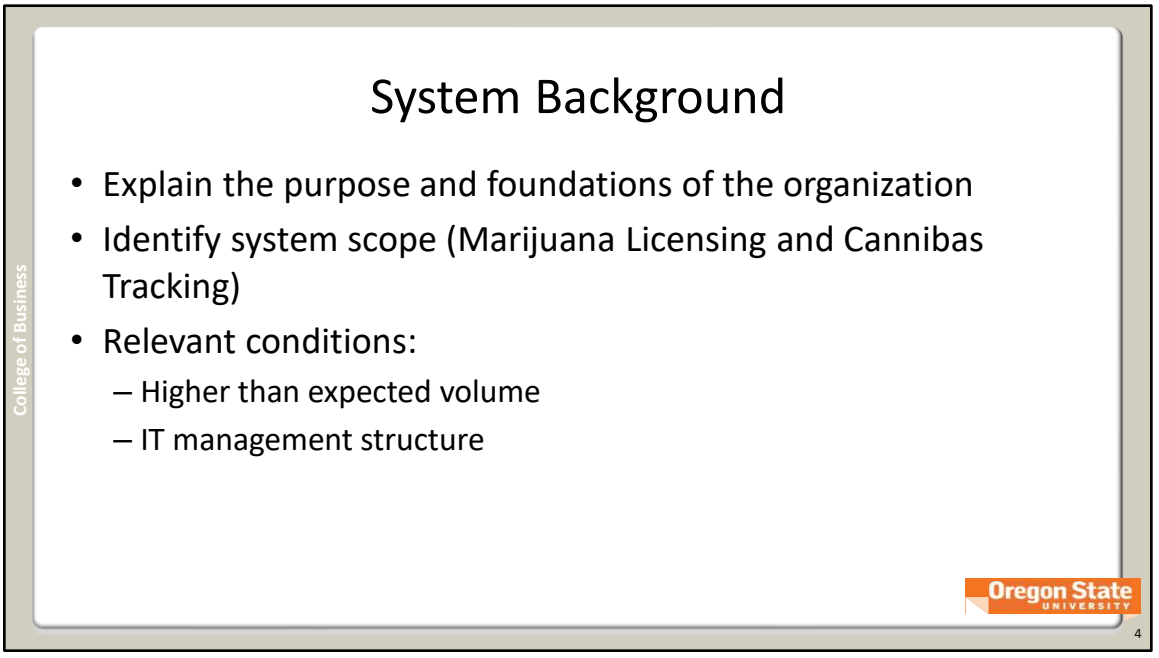
The purpose of our audit was to review and evaluate key general computer controls governing OLCC's IT security management program, and application controls over the Cannabis Tracking and Marijuana Licensing Systems.

This foreshadows what is to come in the statement of objectives on page 5 – the 9th page in the pdf document.

Our specific audit objectives were to 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.*

The purpose statement establishes auditor intent. The audit objectives are further specified to support action.
You may recall that audits test managerial assertions. Sometimes those assertions are implied. Here the State of Oregon is investigating whether management is living up to its responsibility. The purpose statement calls this out. The agency is supposed to have a *security management program* that includes *general computer controls*. Hopefully that makes sense in light of what we have learned so far this term.

The audit objective captures high level control objectives:
- *computer resources are protected against known vulnerabilities and physical threats*
- controls are *sufficient* to *support the regulation of the recreational marijuana programs according to current law*



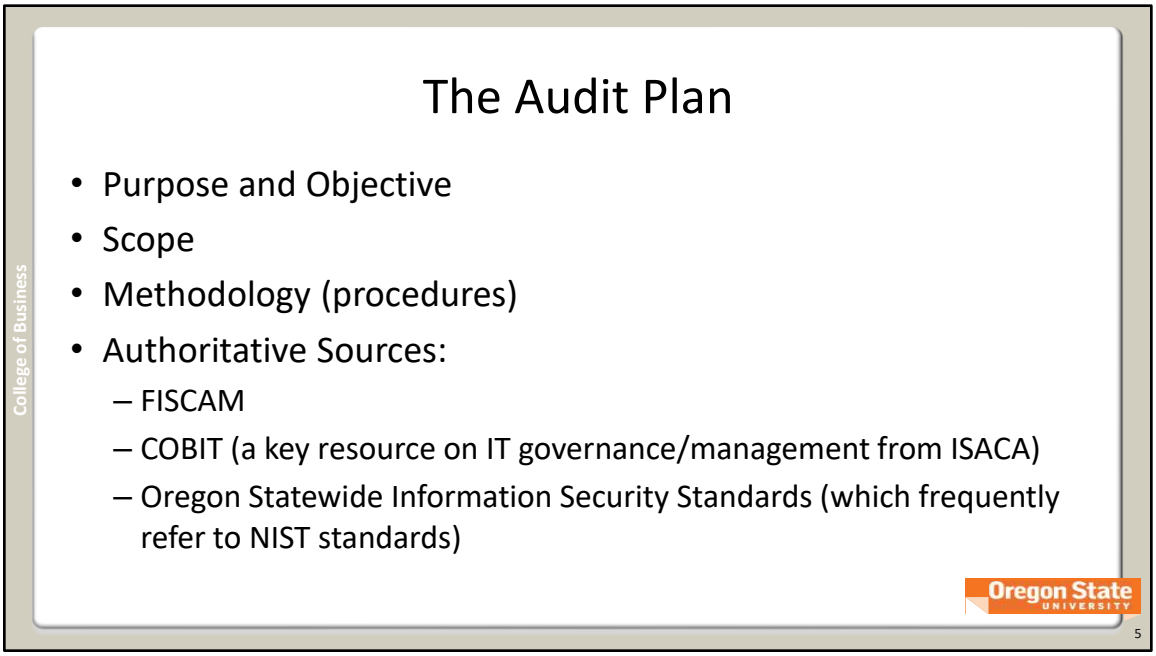
The background information reinforces several course themes:

1. To do a good job auditing, you have to understand the organization and its systems. This background section explains how the organization came into existence and what the law charges it with accomplishing. This is a special thing for governmental auditing – you can trace back to laws and regulations. This helps clarify organizational mission and objectives.
2. To establish scope, you need to do risk assessment. Risk assessment requires an understanding of the specific technology components. The report lists specific components of both of the systems under review.
3. You need to understand the environment in which the organization operates and relevant characteristics.
    a) It might have been enough to just characterize system volume. But by explaining that volume was higher than expected, perhaps the auditors create a bit of sympathy for the organization. It is important that auditees feel that they are treated fairly. And auditor can't fudge their findings, but they can provide a nuanced narrative.
    b) It is clear that OLCC has experienced IT management leadership challenges. This is made clear while also listing the areas of responsibility.

An older ISACA framework specifies "subject matter risk". Even in this short audit report, several relevant areas are partially addressed.

- Business Risk (market size and positioning relative to legislation)
- Contract Risk (relationship with NIC-USA)
- Country Risk (lots of governmental issues – e.g., funding for a CIO)
- Project Risk (turnover in the IT department)
- Technology Risk (this is, at least, introduced in describing the systems)

Perhaps this brief mapping makes a big idea clear: The auditors didn't just write about things they found interesting in the organization, they focused in on background elements that can be directly mapped to system-related organizational risks.

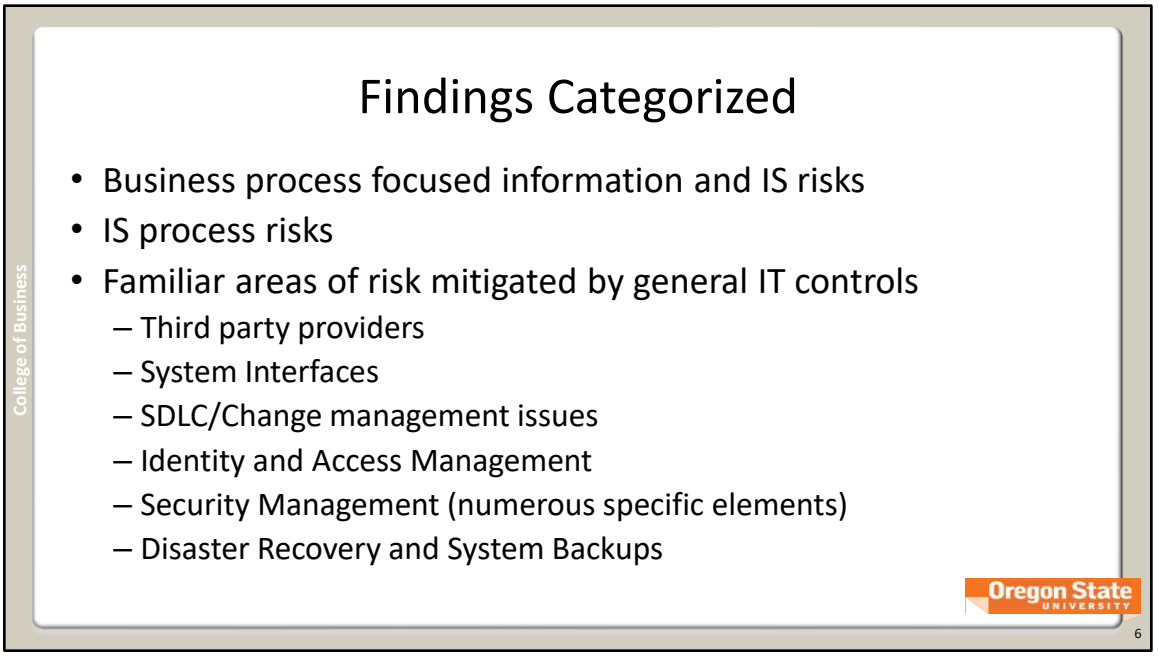


In one short page, the report authors covered the highlights of an extensive audit plan.

A few things to notice:

- The objectives begin with "determine whether". If you can't state something in that form, it is probably not an objective. But be careful, many things that are audit procedures (not objectives) could also begin with those words.
- The audit objectives closely track control objectives.
    - The security management program (a control or set of controls) is supposed to protect against known vulnerabilities and physical threats. The audit aims to see if it does that.
    - The systems are supposed to have sufficient and effective controls so as to ensure compliance with the laws. The audit seeks to determine whether they have such controls.
- The scope of the audit is specified in two ways: As IT processes and procedures for security management and as business processes for a given time frame. These specifications provide useful boundaries for decisions about what to audit.
- Audit procedures are indicated:
    - Interview personnel
    - Observe operations
    - Examine documentation
    - Test controls:
        - Security policies and procedures
        - Contingency planning policies and procedures
        - Vendor management practices
        - Access management processes

Note the call out to authoritative standards. While the report itself does not refer to these items very often, you can be sure that the working papers that support the findings sections carefully document how criteria and evidence are grounded in these source documents.

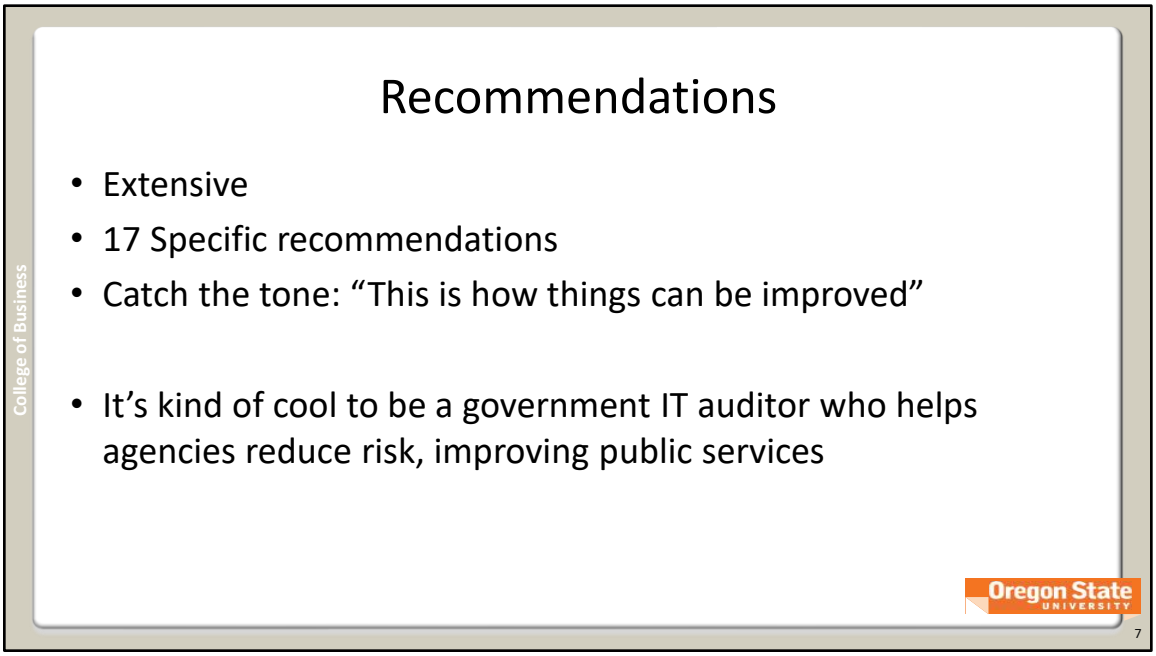


We are reviewing how audits are conducted more than the specific areas and findings of this report.

However, this audit covers a wide range of typical audit topics. This is really a performance audit, not an IS audit. Even though several of the findings focus on business process controls that are not directly system focused, it is not surprising that the noted internal control limitations are often related to IS. For example, data quality concerns that can lead to organizational problems are cited as causes of potential negative outcomes. The data capture and management processes are IS intensive.

Take a moment to look at the list on the slide. Many of these topics will come up later in the course.

In particular, you might take note of the following findings:
- OLCC lacks processes to monitor some third-party service providers (p 12)
- Interface reconciliation processes non-existent (p 13)
- Test data in Marijuana Licensing System production environment (p 13)
- User account management processes lacking (p 14)

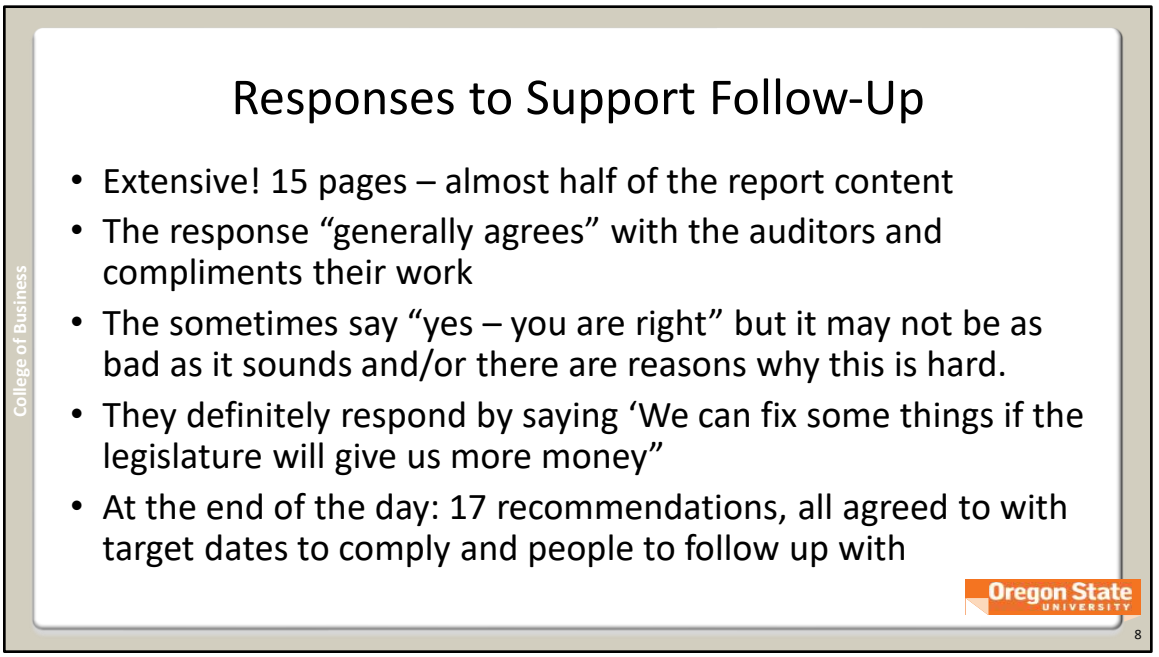


We won’t talk about these in detail at this point.

But please note that, like most performance and internal audits, the auditor lists concrete things that can be done to better mitigate real risks. IS auditors provide valuable service by helping organizations get better.

Of course, external audits can sometimes be a bit less congenial. If managers in a public company have made control assertions that the auditors cannot verify, stock prices can drop and personnel changes may ensue. But that is not how it works out most of the time. Usually, when auditors identify important control weaknesses, IT departments are glad to get support to ask for additional resources or training. That certainly happened in this case. And, even more often, control deficiencies are identified and organizations improve controls.

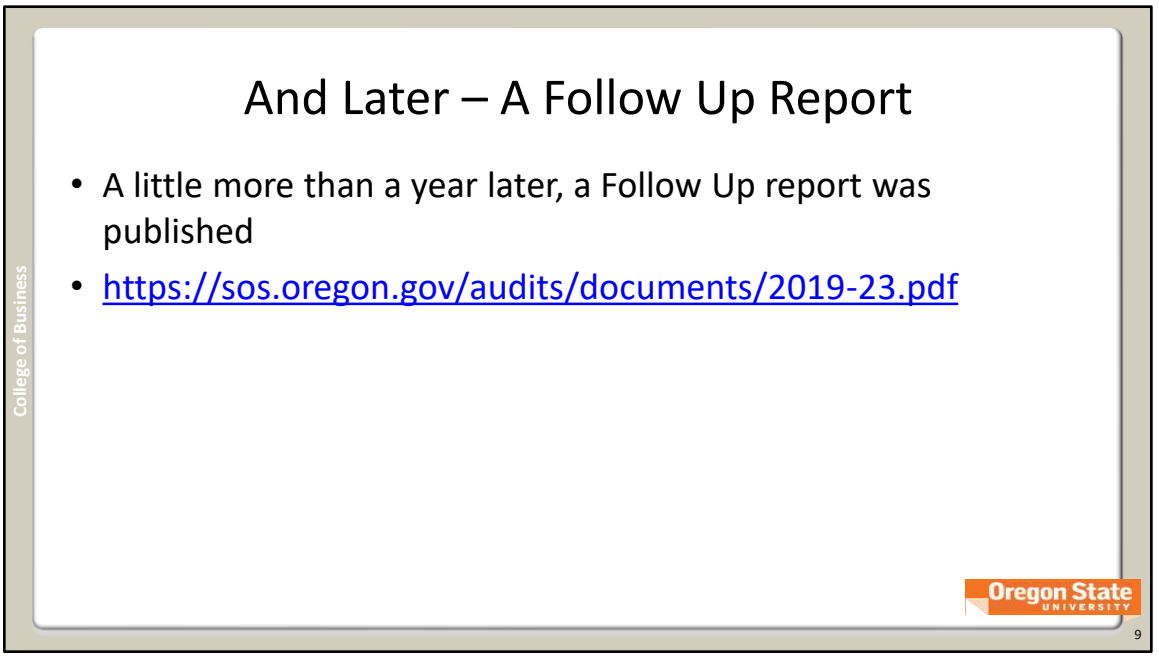
This might be a good moment to put in a good word for government auditing. Over the last few years, the Oregon Secretary of State’s Audit Division has done a lot to improve operations in state government. The information systems audit group has identified a number of areas for improvement and lawmakers and administrators have helped make some useful changes happen – all to the public good. Of course, IS problems in the state continue to exist, but I am proud of the auditors who work for the state. They are doing well (IS auditing is a pretty well paid profession) and they are doing good. Some also report a different work-life balance as compared to practitioners in public accounting firms. Maybe these factors are attractive to you as a student. Please consider the many paths to rewarding careers in IS audit.



Time does not allow for a detailed look at the artfully crafted response letter from the OLCC Executive Director.

One point to pay attention to:
The format of the response letter's last 9 pages includes specific agreement with recommendations, target dates for action, and the names (and phone numbers!) of people who can be contacted for follow-up.

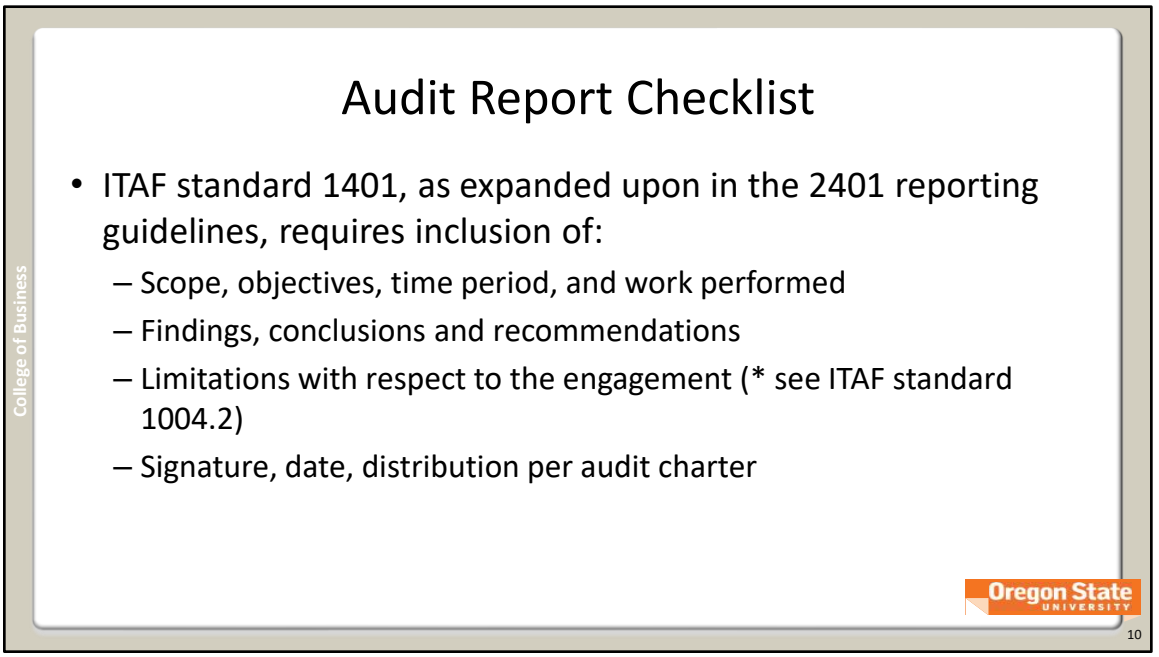
This facilitates the kind of follow-up required in ITAF standards.



We won't look at this follow up report in detail.

Three things to note:

1) Follow- up was done and documented
2) The resolutions, even when done, are far from perfect. This is part of the reality of internal control systems. Organizations work on them, but they are never done and never as good as the auditor might hope.
3) Disaster recovery plans are often neglected.



Not surprisingly, many of the specific items called for in ITAF 1401 are included in the one-page summary.

Note the verbiage on the page after the summary. It establishes the authority of the auditor and includes a public web link to the report.

While there does not seem to be any specific reference to “limitations” there are comments about risk in the environment related to personnel changes and adapting “business” conditions. Given that this is a government agency, the Secretary of State’s Office’s biggest real limitation is the number of resources (people) available to conduct audits.

The paragraph on page 6 (at the end of the Objective, Scope, and Methodology Section) provides some fundamental information regarding how the audit was planned and conducted.

“We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained and reported provides a reasonable basis to achieve our audit objectives.”
This paragraph highlights several themes also found in the Performing IS Audits materials.