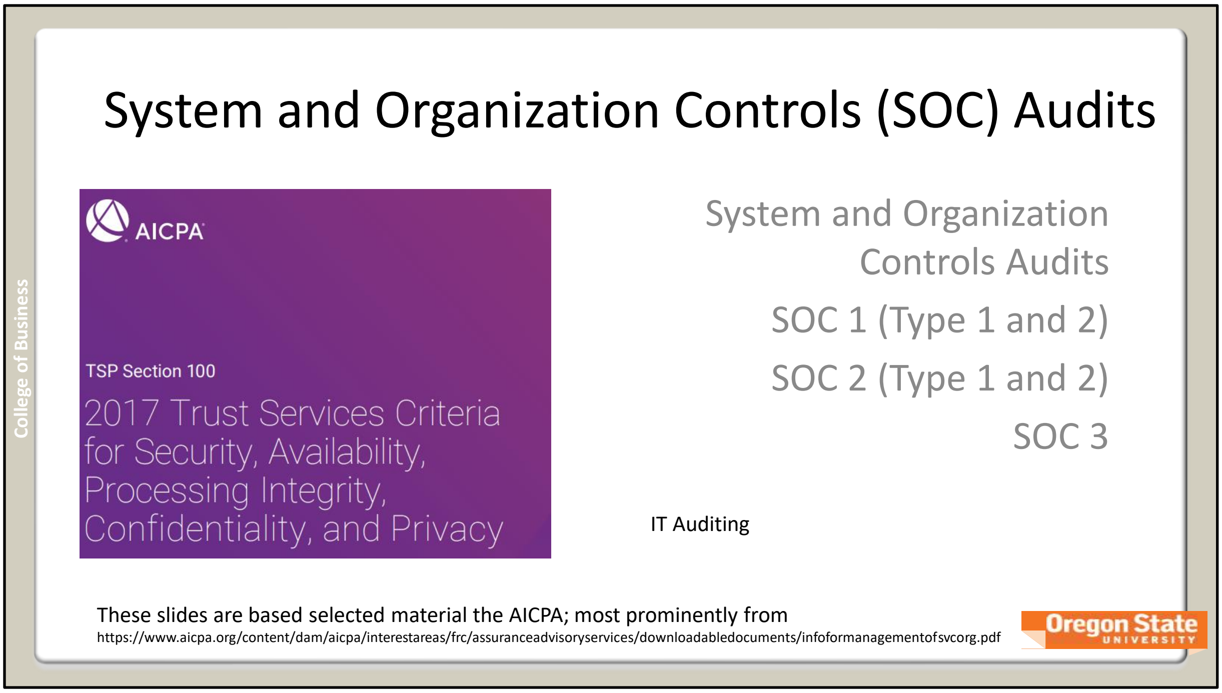


System and Organization Controls (SOC) Audits

College of Business

AICPA

TSP Section 100

2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

System and Organization Controls Audits

SOC 1 (Type 1 and 2)

SOC 2 (Type 1 and 2)

SOC 3

IT Auditing

These slides are based selected material the AICPA; most prominently from
https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/infoformanagementofsvcorg.pdf

Today's organizations are digitally interconnected. That's why we need SOC audits.

Service organizations support business processes for their clients. Examples:

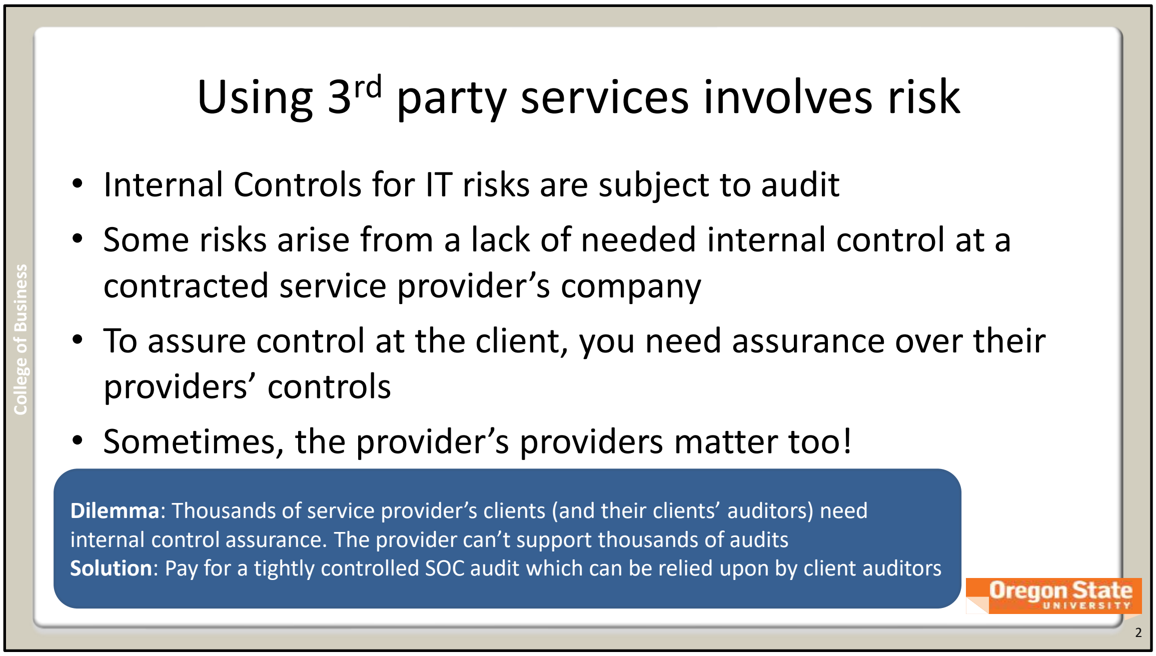
- Web hosting services
- Payroll processors
- Fulfillment service
- Shippers
- Supply chain partners (sometimes)
- Financial institutions
- Email hosting companies
- Web conference companies
- IT infrastructure providers, e.g., Amazon Web Services and Azure; Instead of having our own data center, we use yours!
- Application hosting companies (SAP or Oracle online, Sales Force, Office 365, Google Suite, etc…)

If you think a bit, you can see how problems at each of these categories of providers might result in risk for the client. Private information might be released resulting in client liability, computation or other processing may be incorrect resulting in inaccurate financial statements, operations may be disrupted, client reputation may be damaged, client legal obligations may not be fulfilled, or assets may be lost or misappropriated.

If you think about the objectives of internal control systems, all of them can be threatened by what our partners do.

Not all business partners are service organizations. If your caterer or landscaper do not have good internal control, there is not much risk. But if UPS can't deliver your packages because their computer systems go down, you might immediately face massive revenue shortfalls. Worse yet, if you cloud service provider is compromised, you may not be able to take, fulfill, or support orders. And your customers' data may be exfiltrated. Poor security practices by vendors are a problem.

By the way, the terminology "Service Organization Control" audits has become "System and Organization Controls" In this class, I will accept both/either. But some materials may still reflect the older (and more informative) name.



College of Business

Using 3rd party services involves risk

- Internal Controls for IT risks are subject to audit
- Some risks arise from a lack of needed internal control at a contracted service provider's company
- To assure control at the client, you need assurance over their providers' controls
- Sometimes, the provider's providers matter too!

Dilemma: Thousands of service provider's clients (and their clients' auditors) need internal control assurance. The provider can't support thousands of audits
Solution: Pay for a tightly controlled SOC audit which can be relied upon by client auditors

Oregon State UNIVERSITY

2

Why are SOC audits needed?
If you rely on a third-party service, you are exposed to risk.
IT risks related to internal IT processes are subject to audit:

a. In support of financial audits,
b. In connection with SOX audits as required by the SEC,
c. As part of compliance audits for many organizations, and
d. In connection with other risk management audits.

But what if risks arise not from your processes, your infrastructure, or your control environment, but instead from lack of needed internal control at a contracted service provider's company?

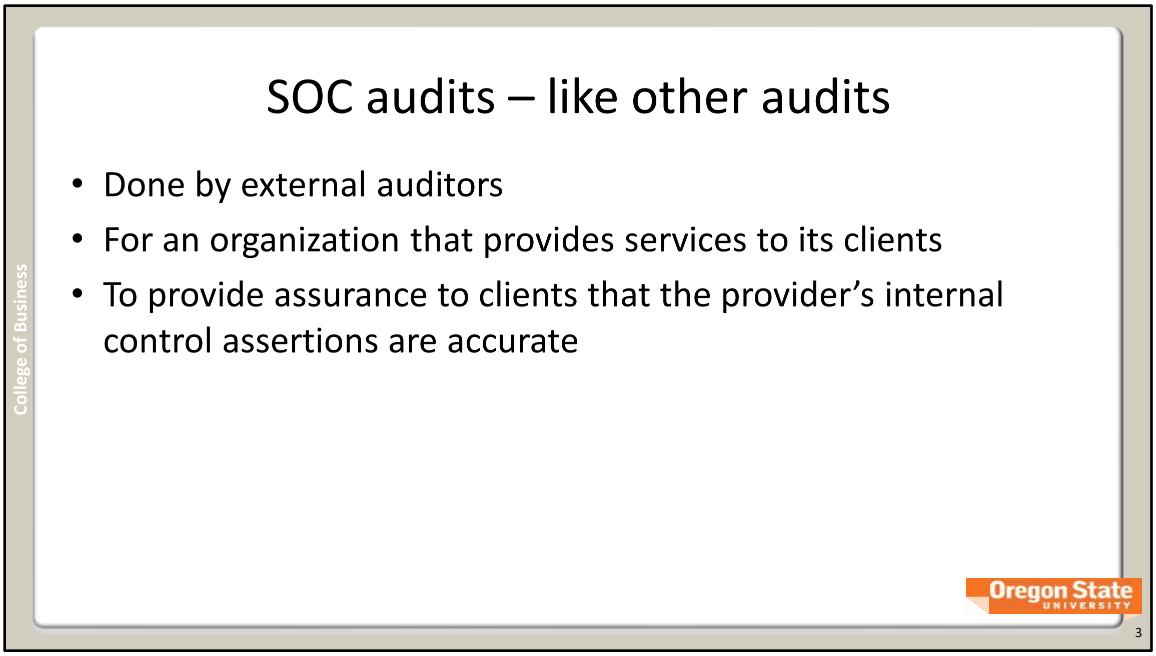
a. The provider might inaccurately process, protect, or provide financial information causing material misstatement in your financial statements.
b. The provider might expose your data to excessive risks resulting in various liabilities that become your problem.
c. The provider's internal control flaws might result in operational risk for the client who becomes unable to operate properly when a provider's systems fail.

What is an auditor to do? Let's say an auditor is charged with auditing internal controls in organization C (client) which relies on services provided by organization V (vendor).

a. C's auditors are concerned about risks arising from possible weaknesses in V's internal controls.
b. V cannot have dozens, hundreds, or thousands of auditors come in and directly assess their internal controls; they will not allow C's auditors to audit their operations.
c. But C's auditors cannot really provide assurance because if V's systems fall short, C may not meet its objectives.

When a service organization has relevant risk associated with its use of subservice providers, control audits of those secondary entities may also come into play.

a. These secondary risks are sometimes 'carved-out'. That is the auditor notes that such controls are expected to be in place and effective even though evidence to that effect is not collected.



College of Business

SOC audits – like other audits

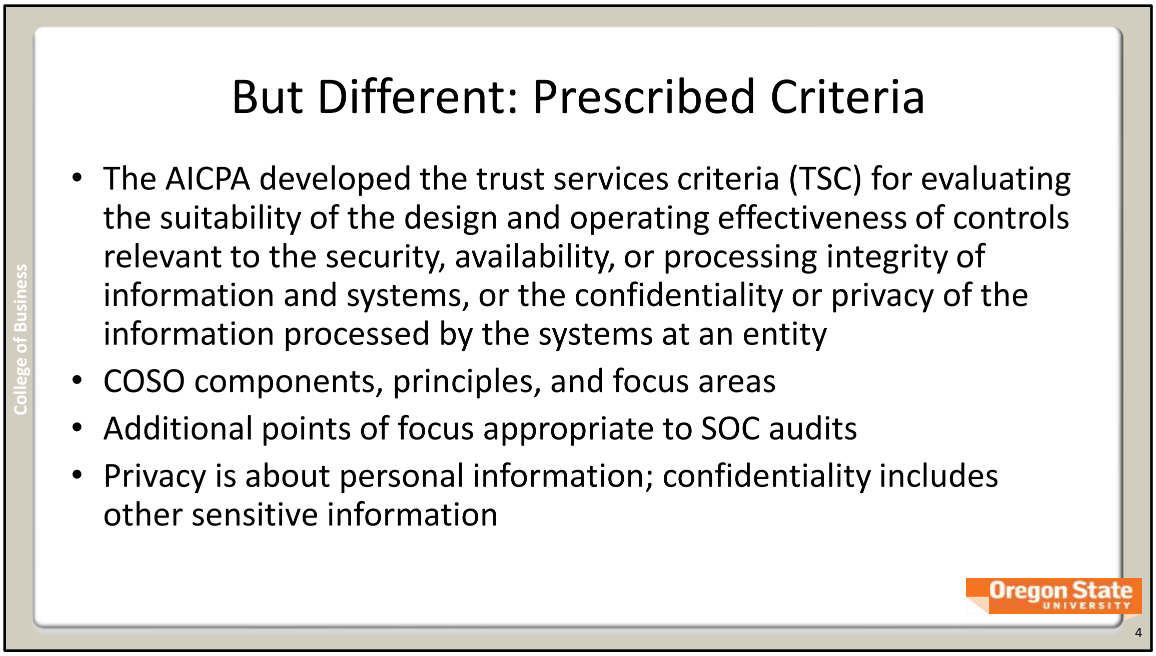
- Done by external auditors
- For an organization that provides services to its clients
- To provide assurance to clients that the provider's internal control assertions are accurate

Oregon State UNIVERSITY

System and Organization Control (SOC) audits are performed to allow a service provider's customers assurance over the Service Organization's internal controls.

In many ways, SOC engagements are like other internal control assurance engagements:

- Management makes assertions about their internal control
- Independent auditors formulate audit plans to test those assertions



But Different: Prescribed Criteria

- The AICPA developed the trust services criteria (TSC) for evaluating the suitability of the design and operating effectiveness of controls relevant to the security, availability, or processing integrity of information and systems, or the confidentiality or privacy of the information processed by the systems at an entity
- COSO components, principles, and focus areas
- Additional points of focus appropriate to SOC audits
- Privacy is about personal information; confidentiality includes other sensitive information

College of Business

4

In traditional attestation engagements, audit criteria are developed based on the internal control system implemented in the organization in light of relevant authoritative guidance. Internal control systems are often similar from one organization to the next because the systems are built using the COSO framework with its components, principles, and focus areas.

For SOC audits, COSO has been interpreted and expanded by the AICPA to support service organizations and to focus on:

- the security, availability, or processing integrity of information and systems

- and/or -

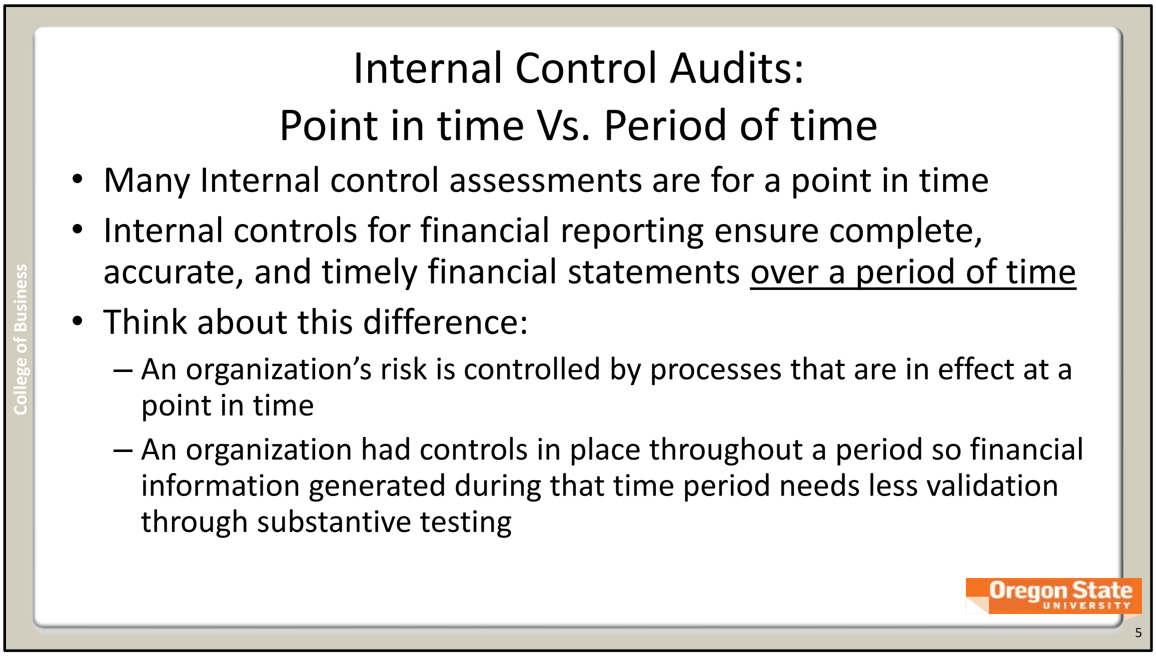
- the confidentiality or privacy of the information processed by the systems at an entity.

By now you should realize that risk assessments are closely related to the specific conditions for a particular organization. Certain risks are more pressing for one of several reasons. As a result, auditors do risk analysis and focus on risks of material misstatements or serious internal control failures. Different organizations, different control expectations and audit priorities.

The problem is that users of SOC audits can not become intimately familiar with the details of every service provider. They cannot know which controls are more or less important in protecting their interests.
To address this ambiguity, the AICPA Trust Services Principles (TSP) and Trust Services Criteria (TSC) are tailored to be usable in most any organization and focused on risks to clients rather than on risks to other of the service provider's stakeholders.

To put it simply, given that more nuanced judgements about a provider's specific risk situations would be hard to establish in a SOC audit environment, AICPA added numerous details to the COSO framework so that SOC audits will be more consistent across audited service organizations.

As we think about SOC reports, we should note that privacy and confidentiality are not the same thing. Actually, you can read lots of descriptions of the difference in different contexts. For SOC reports, privacy is about personal information while confidentiality is about other categories of sensitive information.



College of Business

Internal Control Audits: Point in time Vs. Period of time

- Many Internal control assessments are for a point in time
- Internal controls for financial reporting ensure complete, accurate, and timely financial statements over a period of time
- Think about this difference:
  - An organization's risk is controlled by processes that are in effect at a point in time
  - An organization had controls in place throughout a period so financial information generated during that time period needs less validation through substantive testing

One aspect of internal control auditing we have not really discussed involves whether or not internal controls have been in place and functioning throughout a time period.

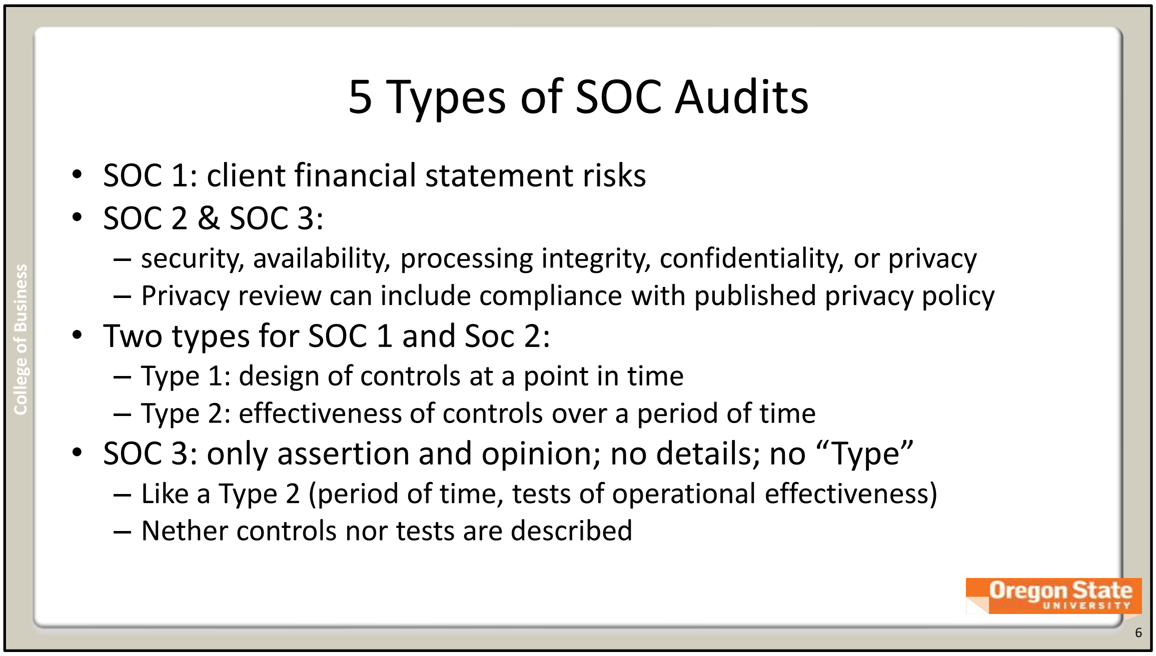
This seems like a trick. What if an organization "fixes" all its controls. They are working in late fall so that auditor can verify them. But what if the company then stops performing the activities in January after the financial statements have been issued. They aren't lying to the auditor about it, there's no fraud here. They want the auditors to say the controls are well designed as of the statement date as required for compliance even though they really don't think the controls are worth the ongoing investment of money and effort. You may think I am kidding. But this really does happen. Frequently!

For SOX reporting and some other compliance reporting, the organization needs to show it has good internal control in place. Let's say an auditor's opinion is dated Dec 31st. Their report would be focused on the state of internal control as of that date. This makes sense because internal control auditing is not about financial numbers, it is about efforts to mitigate risks related to important organizational objectives. Having a good process is important, individual events along the way are not. So, internal control opinions are generally about the state of the internal control system(s)/processes at a particular point in time.

On the other hand, if an auditor is estimating or validating CR (control risk) as part of a financial audit, controls that are only in place for a couple of months are not very effective in assuring the accuracy, completeness, and timeliness of financial records for the whole year.

Of course investors and other stakeholders are likely to expect that if controls are good on December 31st, they will likely be good when May comes around too. Auditors do eventually report if an organization repeatedly "turns controls on and off" to meet year end requirements. The protocol for that, however, is not all that clear.

This distinction is important in understanding SOC audits.
We will get back to this later when we talk about type 1 and type 2 SOC audits.



College of Business

5 Types of SOC Audits

- SOC 1: client financial statement risks
- SOC 2 & SOC 3:
  - security, availability, processing integrity, confidentiality, or privacy
  - Privacy review can include compliance with published privacy policy
- Two types for SOC 1 and Soc 2:
  - Type 1: design of controls at a point in time
  - Type 2: effectiveness of controls over a period of time
- SOC 3: only assertion and opinion; no details; no “Type”
  - Like a Type 2 (period of time, tests of operational effectiveness)
  - Nether controls nor tests are described

Oregon State UNIVERSITY

6

SOC 1 audits are created for auditors providing assurance for financial reporting for clients of the service organization. They do not cover some of the elements emphasized in SOC 2 and SOC 3 reports. Matters of security, availability, confidentiality, or privacy are of less importance in financial statement audits. But many elements do overlap. For example:

- If change management or system development lifecycle (SDLC) processes are not well managed, systems may crash (harming availability) but they may also be more likely to produce inaccurate numbers. So, most change management and SDLC controls matter for both SOC 1 and SOC 2/3 reports.
- Identity and Access Management (IAM) controls can also affect both financial statements and confidentiality concerns. There is a confidentiality problem if bad actors can read and release secret information. If they can change financial information, that’s a threat to information accuracy. Either way, familiar general IT controls are important in mitigating the risk.

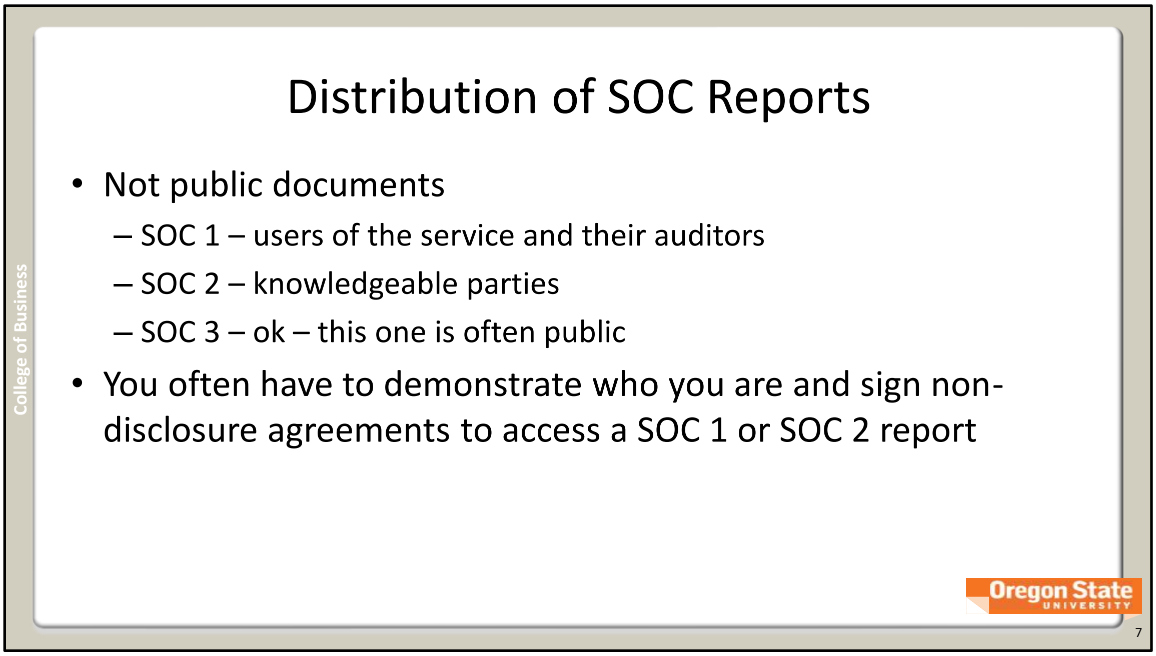
You could say that different objectives are of interest for SOC 1, but many of the same controls and criteria are used.

SOC 2 and SOC 3 reports are intended to address risks beyond financial reporting. Thinking back to the definition of internal control, complying with laws and regulations and supporting efficient and effective operations matter too. Consider, for example, the Canvas system used by many universities. Let’s say a university contracted with a service provider (a company called Instructure) to host its Canvas installation. The university would be concerned about complying with FERPA and generally with protecting student data and intellectual property. These concerns would not be very important from a financial statement perspective. But they would be VERY important from an internal control perspective.

Soc 2 and 3 reports can include privacy. Organizations often have published privacy statements. An organization that uses a SOC-audited service may not have its internal control system compromised if the service provider fails to comply with its own privacy policies, but the organization, or its users might still be affected. It isn’t reasonable for a user/client to be able to have their own audit done. SOC 2 and SOC 3 reports can address these concerns.

SOC 1 and SOC 2 reports include information about the controls in place in the service organization. For these two categories, there are Type 1 and Type 2 variants. The Type 1 reports are “point in time” reports. They look at the design of the controls. Type 2 reports provide additional assurance over the operational effectiveness of the controls over a time period.

SOC 3 reports do not include many details. They are intended to allow the general public to access an external auditor’s opinion on the overall state of internal control. This might give users, regulators, and business partners confidence in working with the service provider. But a SOC 3 is of no real use to an auditor. Perhaps it is better then nothing, but it is not specific enough to provide assurance that can be relied upon.



College of Business

Distribution of SOC Reports

- Not public documents
  - SOC 1 – users of the service and their auditors
  - SOC 2 – knowledgeable parties
  - SOC 3 – ok – this one is often public
- You often have to demonstrate who you are and sign non-disclosure agreements to access a SOC 1 or SOC 2 report

Oregon State UNIVERSITY

7

Most SOC reports are not public reports.

SOC 1 reports are only intended to be reviewed by user entities and auditors conducting audits of the provider's clients.

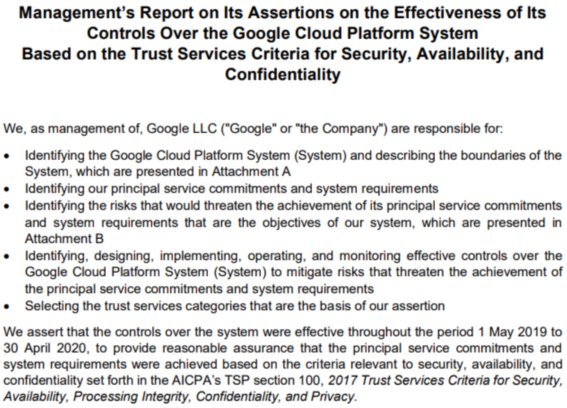
SOC 2 reports should be reviewed only by 'knowledgeable' parties who understand internal control in general, the provided services, and the client's use of the service.

SOC 3 reports tend to be much shorter. For example, SOC 3 reports for groups of Google services can be found on their web site. One was "only" 22 pages. https://services.google.com/fh/files/misc/gcp_soc3_report_spring_2020.pdf

SOC 3's have the least information, so let's start by looking at one of them.

College of Business

SOC 3 Example



Management's Report on Its Assertions on the Effectiveness of Its Controls Over the Google Cloud Platform System Based on the Trust Services Criteria for Security, Availability, and Confidentiality

We, as management of, Google LLC ("Google" or "the Company") are responsible for:

- Identifying the Google Cloud Platform System (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and system requirements that are the objectives of our system, which are presented in Attachment B
- Identifying, designing, implementing, operating, and monitoring effective controls over the Google Cloud Platform System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements
- Selecting the trust services categories that are the basis of our assertion

We assert that the controls over the system were effective throughout the period 1 May 2019 to 30 April 2020, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

This shows the assertion made by Google and assured by its auditor for one set of services

https://services.google.com/fh/files/misc/gcp_soc3_report_spring_2020.pdf

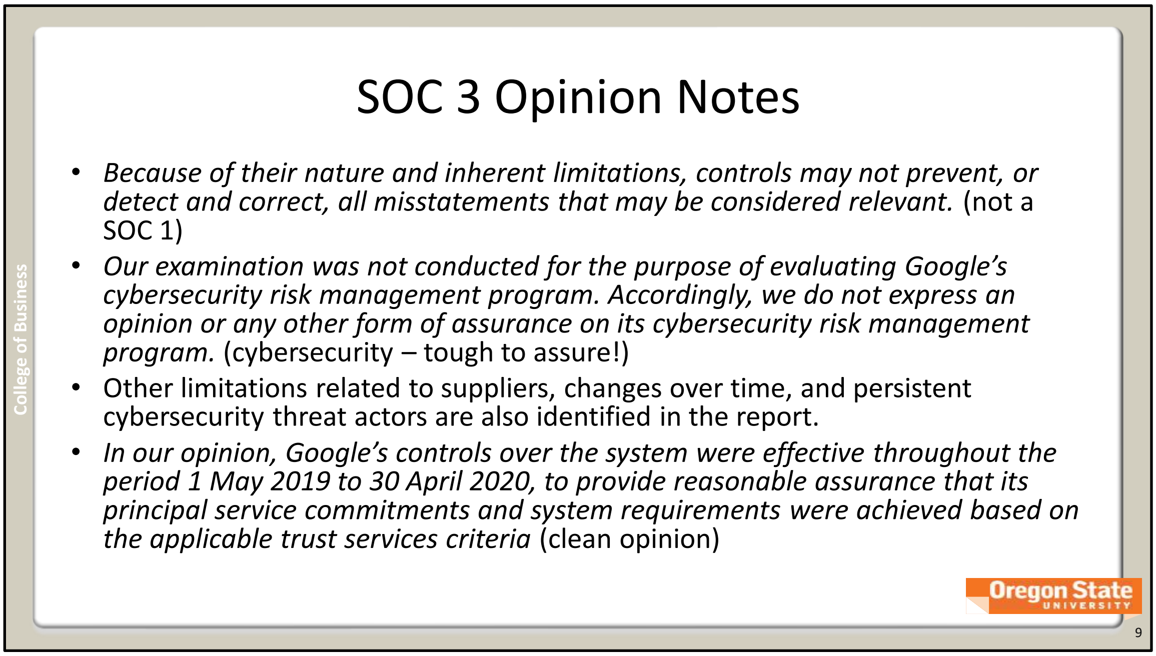
Retrieved Oct, 2020

Oregon State UNIVERSITY

As with other attestation agreements, the audit begins with management assertions.

This being a SOC audit, however, the assertion shown here refers specifically to the Trust Service Criteria (TSC). Perhaps you can see why this is important. Without common criteria, Google and the auditor could have developed their own criteria. While auditors tend to stick to well known sources and most all organizations build on COSO, most audits are prepared for people who can know enough about the company to assess the validity of what was audited. In SOC audits, clients will not have access to the level of information needed to know if the audit nicely covered the risks they were concerned about. Using the TSC helps increase the usefulness of the report. This is especially true for SOC 3 audits which do not describe many details of controls or methodology.

However, you also may see that Google decided which systems were in scope, which risks to be worried about, and which TSC categories were applicable. You always have to read the details provided in that audit and rely, to some degree, on the judgment of the auditor!



College of Business

SOC 3 Opinion Notes

- *Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant.* (not a SOC 1)
- *Our examination was not conducted for the purpose of evaluating Google's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.* (cybersecurity – tough to assure!)
- Other limitations related to suppliers, changes over time, and persistent cybersecurity threat actors are also identified in the report.
- *In our opinion, Google's controls over the system were effective throughout the period 1 May 2019 to 30 April 2020, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria* (clean opinion)

Oregon State UNIVERSITY

9

Here are some things included in the report:

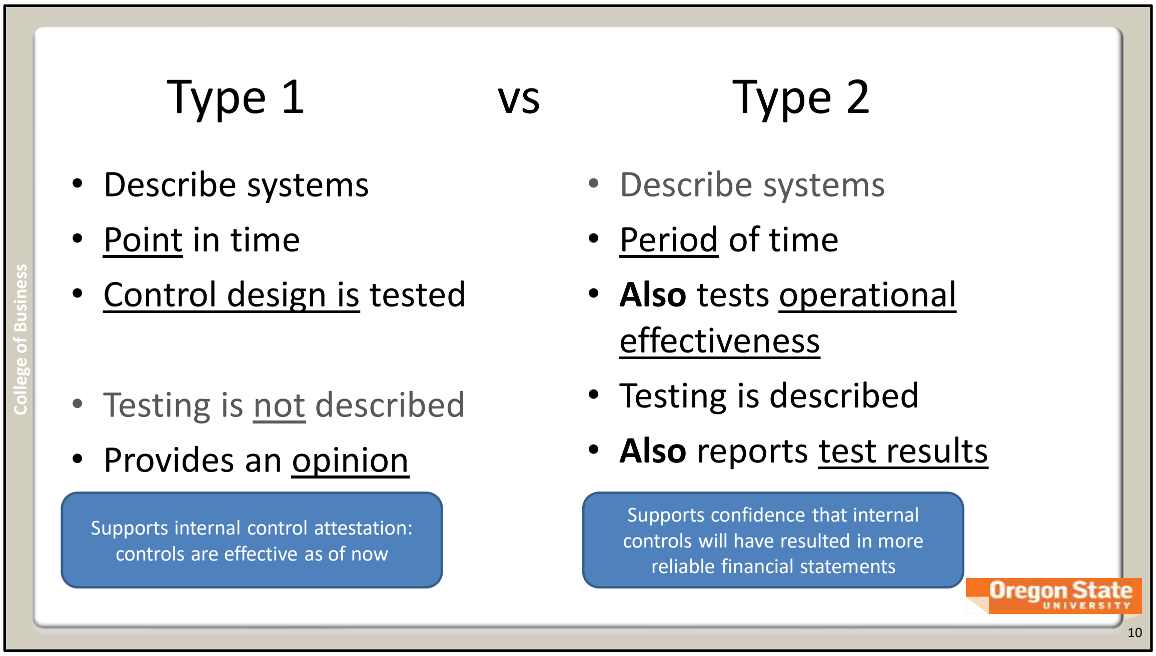
Scope
We have examined management's assertion, contained within the accompanying "Management's Report on Its Assertions on the Effectiveness of Its Controls over the Google Cloud Platform System Based on the Trust Services Criteria for Security, Availability and Confidentiality" (Assertion), that Google's controls over the Google Cloud Platform System (System) were effective throughout the period 1 May 2019 to 30 April 2020, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in the AICPA's TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Inherent limitations
Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Google's principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion
In our opinion, Google's controls over the system were effective throughout the period 1 May 2019 to 30 April 2020, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria.

The SOC 3 document also includes other information about audit methodology.

I'd encourage you to read that carefully, several times. Take note of how it addresses many concepts from previous concepts.



College of Business

Type 1 vs Type 2

- Describe systems
- Point in time
- Control design is tested
- Testing is not described
- Provides an opinion

Supports internal control attestation: controls are effective as of now

- Describe systems
- Period of time
- **Also** tests operational effectiveness
- Testing is described
- **Also** reports test results

Supports confidence that internal controls will have resulted in more reliable financial statements

Oregon State UNIVERSITY

10

Both SOC 1 and SOC 2 reports come in Type 1 and Type 2 variants. While SOC 3s do not come in types – they cover a period of time and test operational effectiveness but do not describe controls and do no report on testing.
Annual statements for SEC companies include attestation of assertions about internal control. This requirement stands apart from reliance on internal control as part of the assurance process for audited financial statements. These two uses, internal control assessment and reliance on internal control for financial auditing, are echoed in Type 1 and Type 2 audits.

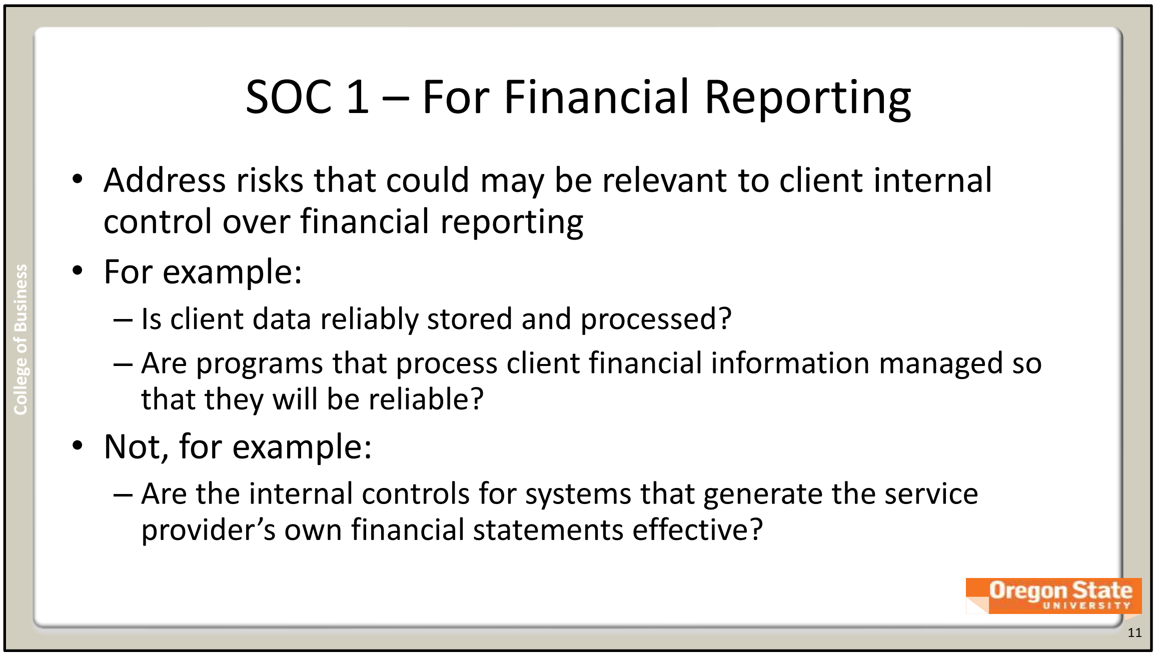
Companies need to file their SOX internal control assertions and have them validated (audited) to remain listed on major stock exchanges. This can also impact other organizations in health care and finance who are subject to regulatory frameworks besides SOX. Assertions and attestations for these purposes are point-in-time assessments. Management says the controls are designed and implemented for effectiveness as of the date of the statement. As you can see in the description above, Type 1 audits are sufficient for this purpose.

On the other hand, an auditor may hope to rely on internal controls existent at a client's service provider in order to decrease CR in audit planning and thereby allow for a higher DR which translates in to lower audit costs resulting from less substantive testing. Whew – that was a long sentence. Let's make a word flow chart: Audit costs are lower because:
Clean SOC report → supports organizational control assessment → lowering CR → Allowing higher DR → without raising AR

A Type 1 report doesn't help with CR. For example: An organization relies on a database managed by a server deployed in the cloud. Controls over that server are found to be reliable as of Dec 31st. But the auditor is not sure if the controls were working back in February. The financial statements include invoices recorded in February. Since the auditor cannot be confident that privileged access was not misused to alter the invoice records, CR is higher. They need to do more testing of financial transactions before obtaining reasonable assurance that the resulting revenue figure is complete and accurate.

If, on the other hand, they had a Type 2 report, they could check to see if privileged access controls for the server in question were effective throughout the entire reporting period. To come to this conclusion, they check the system description – to see if the database is covered, check the control descriptions – to see if privileged access was tested, and check the testing methodology and results – to see if the controls were tested correctly and proved to be effective. Now they have enough evidence to use a lower estimate for CR because they are more confident that material errors would be prevented by the provider's internal controls.

You may have noticed that dates matter. Sometimes supplemental work needs to be done because reporting dates differ. If the service provider's SOC report is dated Dec 31st and the client report is for June 30th, additional information may be needed.



SOC 1 – For Financial Reporting

- Address risks that could may be relevant to client internal control over financial reporting
- For example:
  - Is client data reliably stored and processed?
  - Are programs that process client financial information managed so that they will be reliable?
- Not, for example:
  - Are the internal controls for systems that generate the service provider’s own financial statements effective?

College of Business

SOC 1 audits are about financial statement risks.

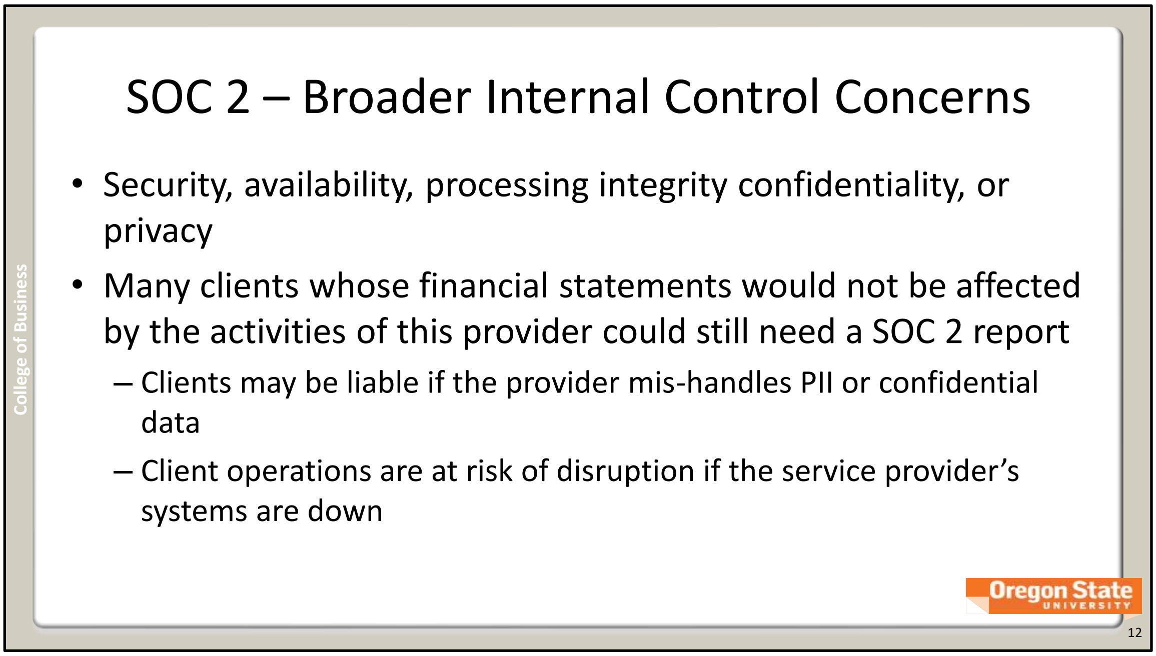
But they are not so much audits of the internal control risks for the service organization as they are audits of controls that safeguard against client risks in using the service.

Depending on how the service organization is set up, some may overlap. For example, privileged access controls for systems that support clients and support the provider’s internal processes need to be secure.

SOC 1 reports are rarely shared with anyone except potential clients, clients, and client’s auditors.

It is not clear how useful a SOC 1, Type 1 report would be. Since it focuses on risks to the client’s financial statements, it would be important to know if controls were in place throughout the time period covered in the client statements. A point-in-time audit would be of limited value. Maybe they would be good for a new organization seeking to do business with the provider. They might feel good about the audit, knowing that they won’t have issues later if they use the service.

Just as control assertions and attestations for internal controls within a company need to cover the entire reporting period if they are to by used to lower CR, relevant controls at the service organization also need to have been in force throughout the time period.



SOC 2 – Broader Internal Control Concerns

- Security, availability, processing integrity confidentiality, or privacy
- Many clients whose financial statements would not be affected by the activities of this provider could still need a SOC 2 report
  - Clients may be liable if the provider mis-handles PII or confidential data
  - Client operations are at risk of disruption if the service provider’s systems are down

College of Business

Oregon State University

12

Internal control is concerned with objectives well beyond financial statements.

When an organization depends on a service provider in a way that poses important organizational risks that are supposed to be addressed by internal controls, that organization’s auditor will need to consider the effectiveness of those controls.

Consider, for example, the impact on a university if:

- … their learning management systems (e.g. Canvas) was down for a week
- … their banking interface was down so employees did not receive direct deposits
- … their external recruiting system had flaws that allowed competitors to access applications filled out by potential students

SOC reports can be requested by clients or potential clients of the service organization.

- They can be used before contracts are written with a service provider either to select a vendor or to influence the content of service level agreements.
- They are needed as part of regular audit processes. The auditor can match services provided to service organization controls and see if the controls were deemed effective by the SOC auditor.

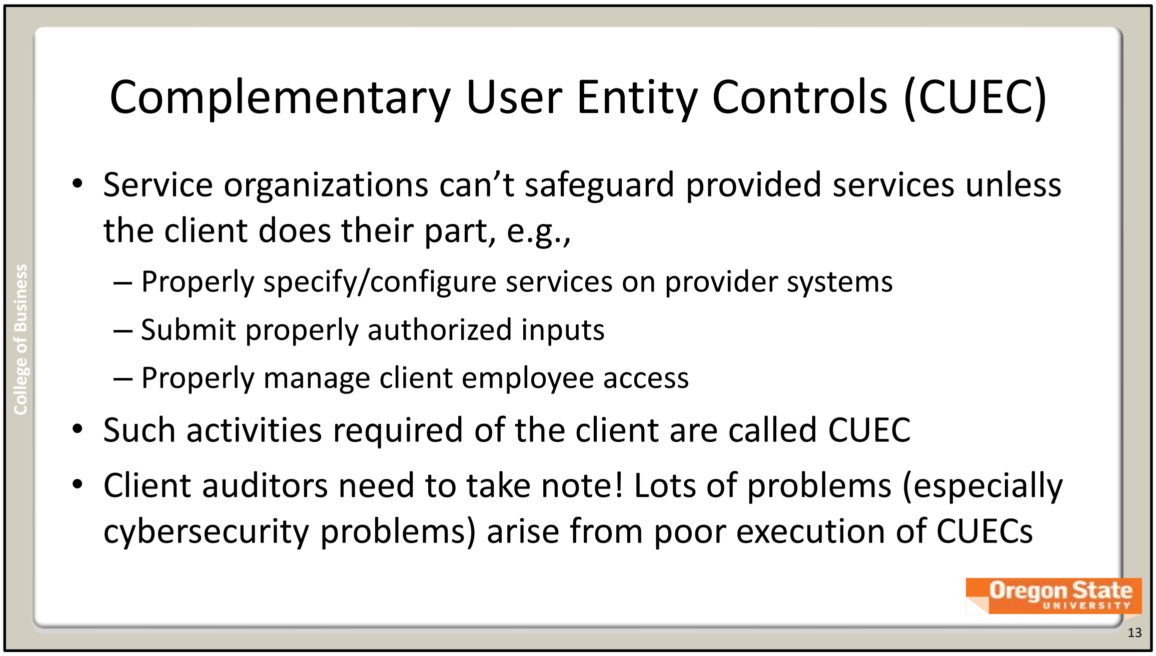
SOC 2, Type 1 reports may be sufficient for SOX reporting and other similar point-in-time control reports.

However, if a service organization only had important controls in place for part of each year, a client should be worried. If the part time controls are additional controls added this year, maybe that’s fine. But if, for example, a provider put change management control in place for a month or two each year but did not follow through on the activities throughout the year, the client organization’s system of control is not in line with the kind of expectations expressed in COSO and other control frameworks.

Over multiple years of audits, auditors have to think about what it means if an organization needs to remediate the same control several times over several years. Auditors are aware of this dynamic, and it is of concern.

Further, if the provider’s statement’s point in time and the client’s statement date do not align, problems can arise.

So, in practice, SOC 2, Type 2 reports, which cover a time period instead of a point in time, are often needed even though client internal control assertions are point-in-time assessments.



College of Business

Complementary User Entity Controls (CUEC)

- Service organizations can't safeguard provided services unless the client does their part, e.g.,
  - Properly specify/configure services on provider systems
  - Submit properly authorized inputs
  - Properly manage client employee access
- Such activities required of the client are called CUEC
- Client auditors need to take note! Lots of problems (especially cybersecurity problems) arise from poor execution of CUECs

Remember that control systems are integrated.

A service provider's systems usually need to interact with client systems to accomplish their purpose.

For example, a university that used a cloud version of a learning management system such as Canvas:

- Uploads lists of students and courses
- Authenticates users
- Authorizes instructors to access selected resources
- Routes email messages under certain conditions
- Allows university administrative access to configure services and monitor activity and performance
- And more

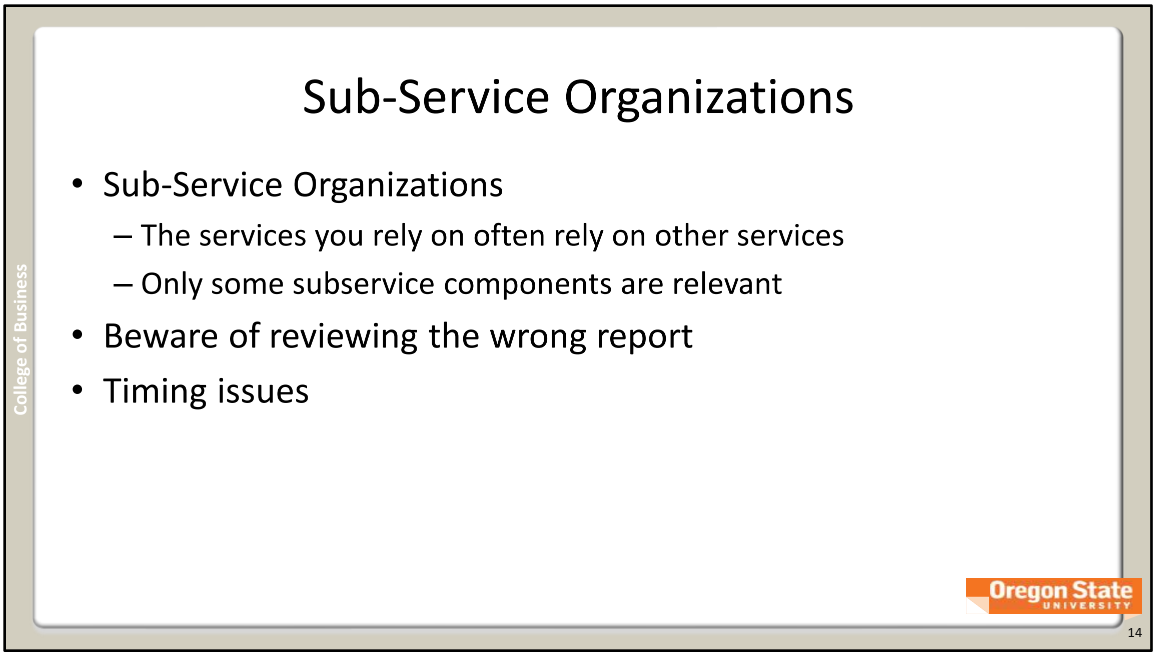
If the university does not take proper care to protect its side of things the provided services may be insecure or may not operate correctly.

The trust service criteria are actually written to try to keep things separate. For example,

> *CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.*

Do you see how this audit criteria side-steps an issue? The SOC auditor is specifically allowed to ignore any concerns related to incorrect user lists provided by the client entity. This distinction is nice from an audit perspective, but it does not mean there is no risk. A client auditor looking at the internal controls for this system would certainly review the SOC report to be sure the provider is doing what it should. But they must also take note of things the client has to do. It would be easy to ignore such risks thinking "that system is covered by the SOC report". But that could be a big mistake unless the audit report is thoughtfully reviewed.

Many many cybersecurity breaches have been caused because an organization uses a service such as Amazon Web Services (AWS) without properly securing things as per AWS guidance or best practices. There isn't much the provider can do about this. The client and its auditors must be ware.



College of Business

Sub-Service Organizations

- Sub-Service Organizations
  - The services you rely on often rely on other services
  - Only some subservice components are relevant
- Beware of reviewing the wrong report
- Timing issues

Today's interconnected digital world means that not only does an auditor need to think about service organizations, they need to think about service organizations used by their providers. IT is common for one service to use another "sub-service." For example, a company may use an online portal which uses a systems integrator, who then uses a cloud service. Risks to the end user can come from poor internal controls at any of the sub-services in this chain.

When conducting a SOC audit, you hope that the service auditor has covered subservice risk in its report. But sometimes auditors need to read the supporting reports to be sure that shortcuts were not taken or to be sure that relevant risks have been addressed rather than carved out.

They may also have to worry about issues such as timing. If the client's reporting period ended in Dec, and the service organization's SOC reporting period ended in November, the auditor may be able to gather some interim information and conclude that reasonable assurance is in place. But what if the service's SOC audit was partly based on a subservice audit with an end date in June?

The fine details of such decisions is outside of the scope for this course. But pay attention to these two important points:
(1) Auditors sometimes need to review SOC reports of subservice organizations.
(2) When doing a SOC audit, auditors may well need to review subservice SOC audits very closely.

Be sure you are looking at the right report. For example, let say a university learning management system (LMS) is hosted by a third party. An internal auditor assessing controls for the university, or a purchase agent deciding on a new system, should review the hosting services SOC report. But if a potential service provider has not had a SOC audit and may send a subservice's report instead.

Many services use Amazon Web Services (AWS) or Microsoft Azure. They outsource their data centers to these well-resourced companies. If you asked the LMS company for a SOC report, they may provide the AWS SOC report instead of one for their own systems. While the LMS company may be much more reliable and secure because its systems are hosted by these tech titans, the data center only represents a small portion of the risk for the university. If the LMS system has poor change management controls, poor internal cybersecurity practices, or a weak control environment, it won't help much that they host their systems at AWS.

Auditors who rely on SOC audits have a responsibility to carefully think through risk and be sure they match client risks to provider controls that have been properly tested.