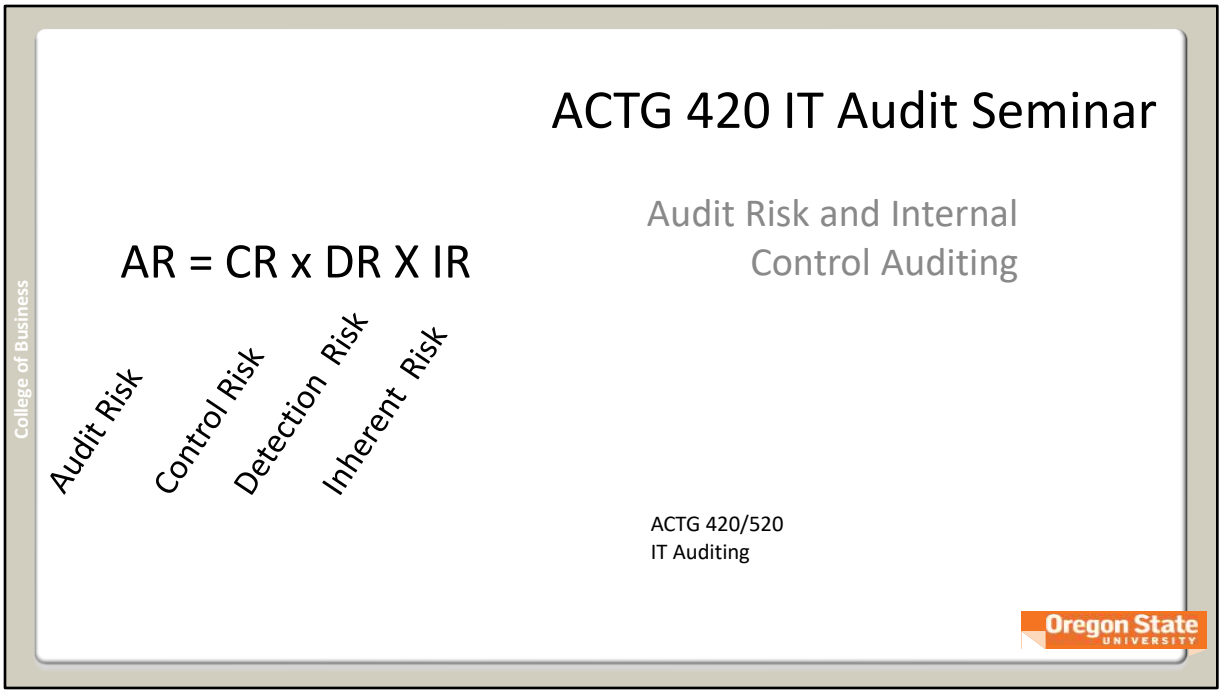


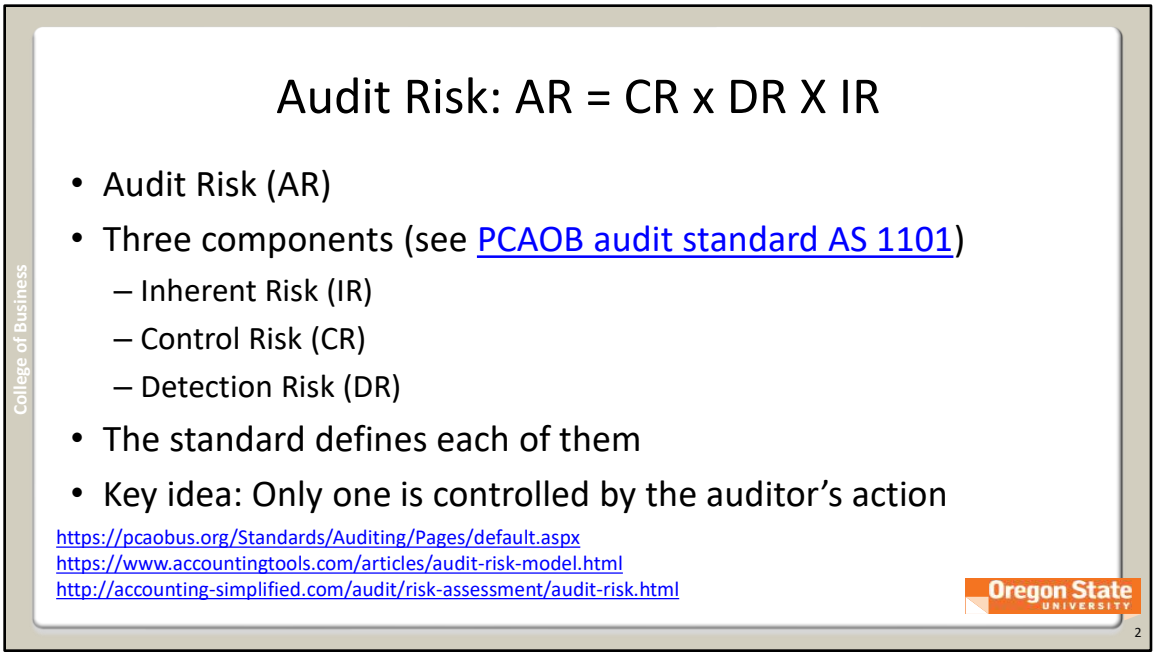
This slide deck expands on the Introduction to Internal Control Auditing Slide Deck.

External auditors charge for audits. Internal auditors have to prioritize.
They want to do a reliable audit, but they don't want to spend extra money on testing.

- If an external auditor plans and budgets to do more testing than necessary, a competitor may beat them out on the audit bid.
- If an auditor does more testing than necessary, they may spend more money on auditor labor and other expenses resulting in a less profitable engagement (external) or waste of resources (internal).

Sometimes doing more testing allows the auditor to charge more. Other times an audit is bid for a flat rate.
In flat rate audits, additional testing results in higher costs but not a higher fee.

Even when additional testing allows additional fees to be charged, it makes clients unhappy.



Risk also has a special flavor for auditors: Audit Risk.

In order to establish reasonable assurance that audited assertions are correct, an auditor targets a specified level of audit risk. This is only partly about risks the organization faces, its is mostly about the risk that the audit will result in an incorrect opinion.

For example, the auditor may decide that the audit should provide evidence that there is no more than a 5% chance that an assertion is materially incorrect (AR) – in essence, this is a practical expression of reasonable assurance.

To estimate the risk of failing to catch a misstatement, auditors need to consider why errors might occur:
Management's financial assertions could be incorrect because:

- Estimating the value of the underlying transactions may be difficult (inherent risk), or because
- the processes the organization uses to record the information may be improperly controlled (control risk).

Those two risks are outside of the control of the auditor, that is, nothing the auditor can do can change the inherent chance that a firm like this one might have an error (IR) or the chance that the control systems the organization had in place over the period of interest might fail to detect or prevent misstatements (CR).
Together these two components make up the risk of material misstatement of an assertion as described in AS 1101.07.
Think back to the idea of residual risk: (IR) x (CR) works much the same way as estimating the residual risk after controls are considered.

Auditors need to estimate the risk level for IR and CR, then they plan their audit to achieve the level of DR needed to achieve the targeted AR.

DR is primarily controlled by deciding which and how many transactions need to be reviewed so as to meet the desired level of Audit Risk – DR is selected to meet audit objectives and achieved by the actions an auditor takes.

Basically, if things are very risky and the control systems are weak, the auditor will have to review line items, GL entries, and accounting estimates very closely by verifying a relatively high percentage of the transaction records but if process controls make it very unlikely that an error would slip through, the auditor can do little or no testing of the transactions themselves.

College of Business

Inherent Risk

- AS 2110.05 “Risks of material misstatement can arise from [..] external factors, such as conditions in the company's industry and environment, and company-specific factors, such as the nature of the company, its activities […] For example, external or company specific factors can affect the judgments involved in determining accounting estimates or create pressures to manipulate the financial statements”
- Inherent risk is NOT tested – it is estimated

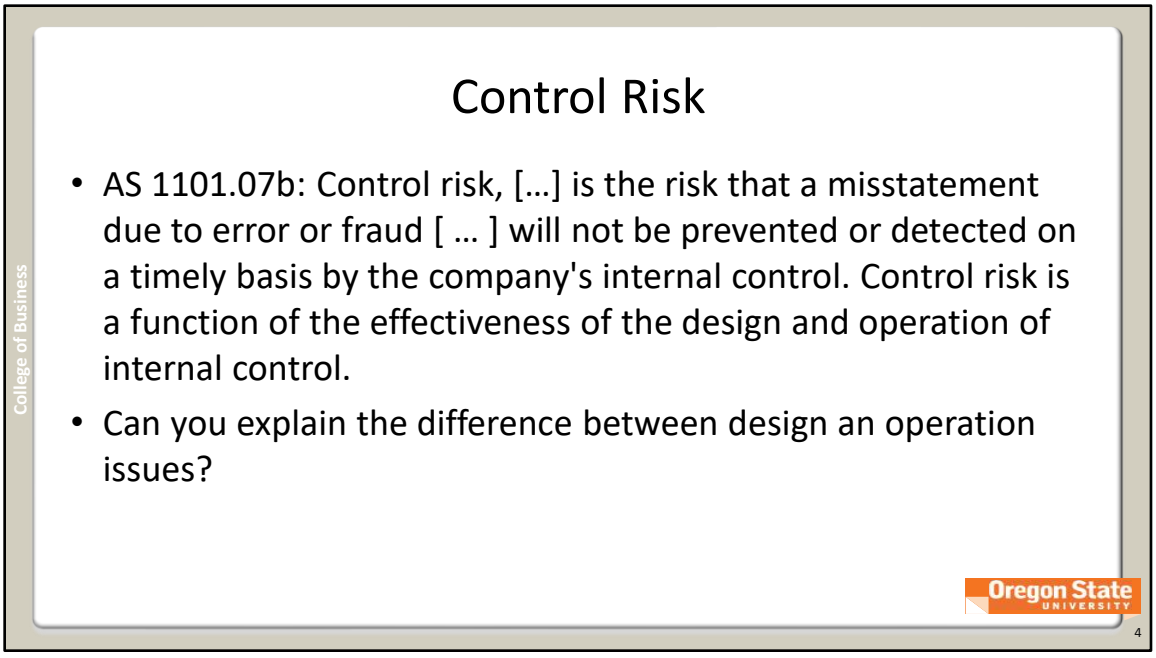
Oregon State University

3

Read that over a couple of times and think up examples:

- Perhaps a company is in an industry that faces challenges in estimating the value of financial transactions.
- Perhaps a company is in an industry with assets that quickly become obsolete.
- Perhaps a company recently went through a merger.
- Perhaps the firm has had misstatements in the past.
- Perhaps the company is finding it difficult to get financing and may have to pay more for loans in the future.
- Perhaps management bonuses or other factors make it lucrative for managers to estimate some value to be higher or lower.

These kinds of issues increase the level of inherent risk.



Internal controls are supposed to protect the organization from inherent risks.
The AS1101 definition shown here notes that the problem can be that:

- the control is not properly designed
- or that the control is not properly operated.

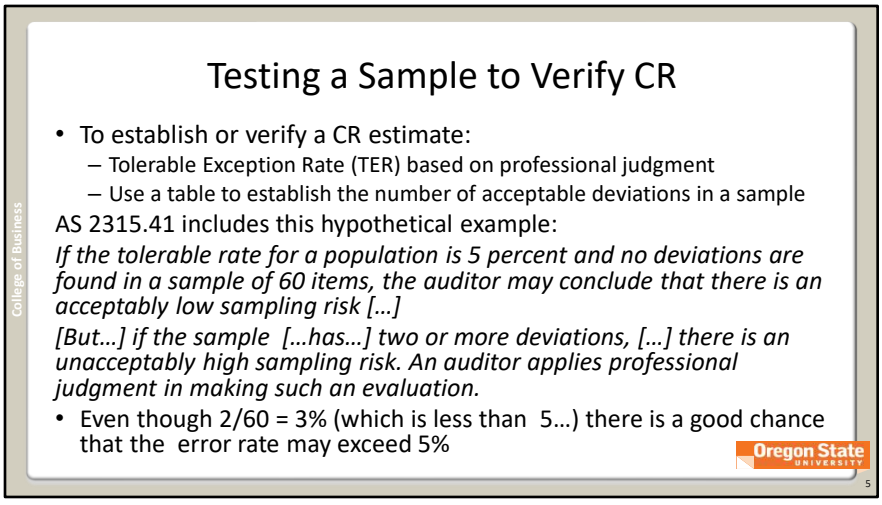
Consider a control where one individual enters a transaction into the system and a separate individual approves it before it can be processed.
By policy, the approver is expected to verify the date, amount, and customer against a paper document AND be familiar enough with the situation to judge this transaction to be legitimate.
This kind of control would affect the likelihood that the reported financial statement balance is accurate (CR in the Audit Risk formula).

Note that some of these things are automatically enforced by the system and others require action or judgment from the user.
Although the system won't process the transaction until the appropriate approval has been recorded, the person who approves may or may not have applied due care in checking things over.
This illustrates the difference between automatic and manual controls.

An example of design flaws might be an incomplete control, for example a control design could require that approval be recorded by only authorized individuals, intending to ensure that the person who approves knows enough to make a proper decision.
Perhaps the auditor, when checking over the design of the control, discovers that while the main screen for approval is restricted to selected individuals, a separate screen allows anyone to change the switch to 'approved': that would be a control design flaw.

An auditor might, at first, estimate, based on this control, that there was only a 5% chance that an errant transaction was entered or that fraudulent transactions have been processed; but after discovering this flaw, they would have to change their thinking.
In this case, they would be likely to decide that this particular control provides little assurance so CR would be 50%.
That is, there is a 50% chance that an errant transaction would not be prevented by this control – virtually no protection at all.

In contrast, an example of failed operation of the control might be that while the approver is supposed to check things over and be sure they can recognize legitimate transactions, in practice, people routinely approve transactions without reviewing them.
In the interview the approvers say that they trust their coworkers so they don't give a lot of thought before approving.
Despite a seemingly proper design, the control is found to not be properly in operation.



CR values are sometimes verified by testing the attributes of a sample of transactions.

Verifying the estimate of control risk is guided by professional judgement.

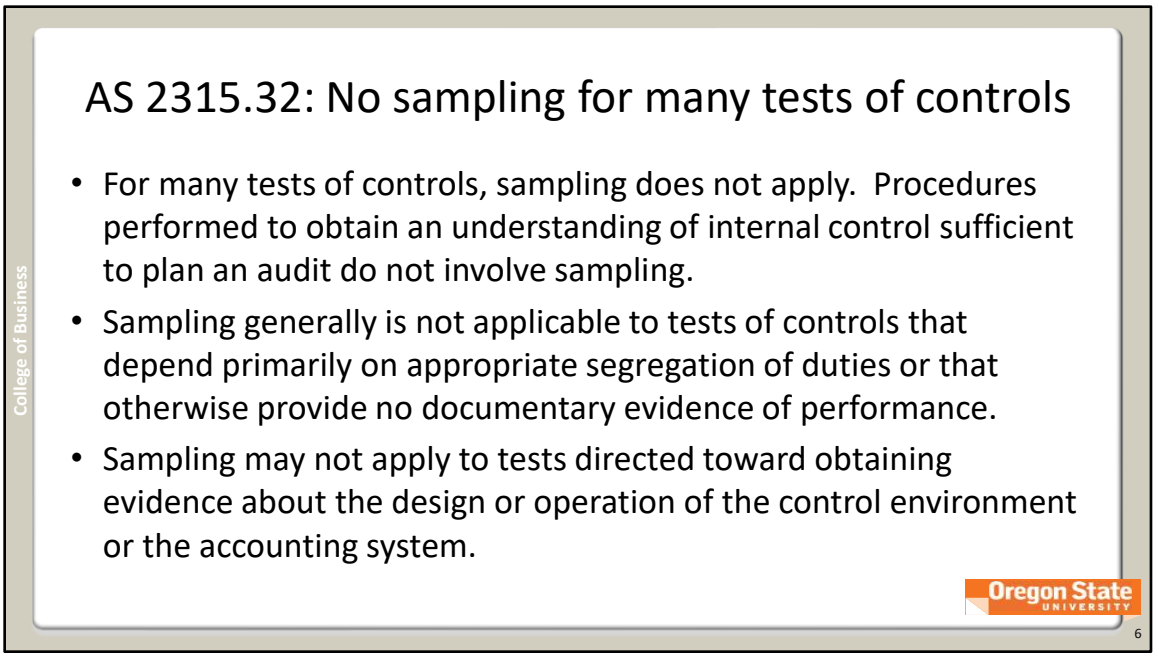
Multiple controls may impact relevant control risk.
For example, consider controls over the accuracy of the Accounts Payable account:
1. Computer software enforces that one person enters, and another approves each entered payable.
2. Computer software enforces that checks are written by one person and approved by another.
3. Due care by the approver is documented with initials and variations from PO amounts are justified.

First, the auditor estimates the rate of error for attributes.
For example, the software should never allow the same user id to enter and approve the same transaction as per controls 1 and 2. So, we expect to find no examples of that. We can easily check all recorded transactions using a database query.

For control 3 (due care in checking) let's say the auditor sets TER (tolerable exception rate) to 5%. People are not so good at this kind of thing so we shouldn't expect 100% of the items to show signs of effective review. Even so, the control provides some safeguarding: if employees know this is checked they may take more care, may be disinclined to commit fraud because they might well be caught, patterns of errors will be caught, and most errors will be corrected.
Those sorts of factors are built into auditor judgment in establishing TER.
The auditor then compares the recorded details to the paper backup for 60 transactions, finding that 2 out of the 60 items were not initialed – therefore we have no evidence that they were reviewed.

Even though the sample had only a 3% (2/60) error rate, and even though we decided that 5% was acceptable, there is a concern that the error rate might be higher in the population (all transactions) than it was in the sample (the 60 tested items).
Note that the "limits" (how many errors are allowed given a sample size) are determined statistically based on some assumptions about the distribution of errors across sample subsets. Limits are usually computed by specialized audit software or found in tables.
Key: if we want to be 95% sure that 90% of transactions are proper, our sample will have to have fewer than 10% exceptions.

If your tests do not come out as expected, you do not usually do more control testing.
If you have a reason to believe that the sample you chose was not representative of the population, you might try again.
Otherwise, you have no reason to expect that checking more transactions to see if the control was applied correctly will get you a better answer; more testing of the same control doesn't help much.
Usually, rather than going back and checking 60 more transactions for initials, you will increase the CR you were expecting; later slides will address what the auditor might have to do as a result.



PCAOB's audit standard number 2315 is all about audit sampling.

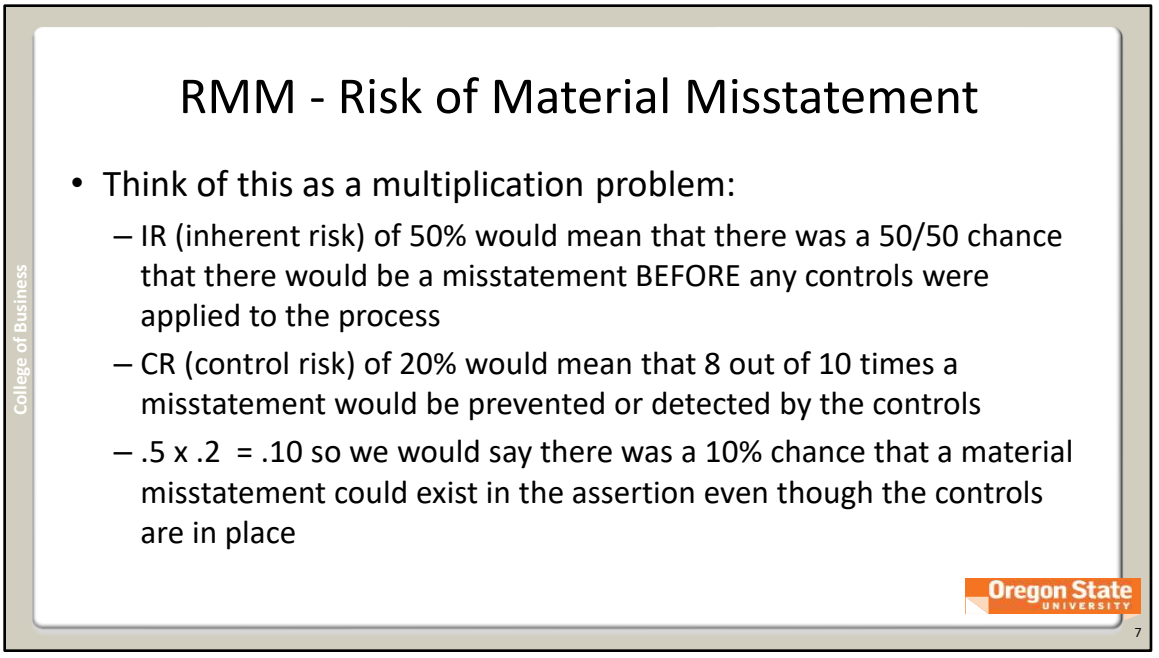
While financial statement facts are often tested through sampling, many internal control tests do not involve samples.

We don't take samples to understand controls.
We don't take samples when a control does not produce documentary evidence.
We don't take samples to assess the design of controls.

High level controls such as analysis of budget variations (which is supposed to catch overspending) do not require sampling. The auditor would observe and inquire.

- Were budget variances reported?
- Were they reviewed?
- Did any exceptions arise?
- How do we know someone looked into the exceptions?

These factors all play into an auditor's verification of the estimate of CR used in initial audit planning.



IR and CR make up the basic Risk of Material Misstatement (RMM).

If this is confusing, think back to our discussion of residual risk.
There was a chance a bad thing would happen.
But when we added the control, some of those negative events would be prevented or detected and corrected.
The risk that an error happened and was NOT caught by the control was the residual risk.

Residual risk has a more narrow application to auditing: RMM
RMM focuses on the chance that a material amount is misstated before the auditor looks things over.
RMM is a function of the inherent risk of misstatement as it has been mitigated by the controls the organization has in place.

Generally and theoretically, the auditor cannot change IR or CR.
RMM levels result from the business and its environment, not from the actions of auditors.

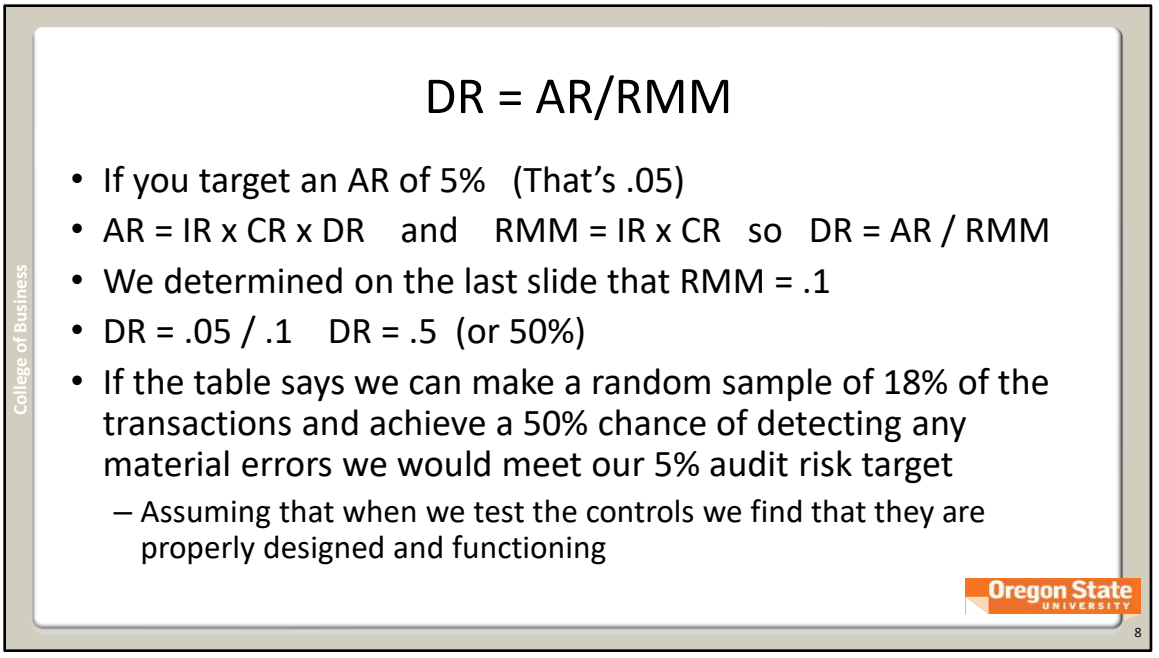
The word "determine" has two meanings:
- "cause (something) to occur in a particular way; be the decisive factor in"
- "ascertain or establish exactly, typically as a result of research or calculation"

Consider the difference between determining CR and estimating CR.

CR is determined (caused) by management. If they implement good controls, CR is low.
Auditors ascertain the CR level. They review the controls and identify the CR level resulting from the implemented controls.
Importantly, the auditors start with an estimate of CR. But that estimate may change as control testing is performed or as new evidence comes to light.

Similarly, IR is not driven by the actions of auditors, it is estimated by the auditor when they do their audit planning.

This is an important distinction in making sense of audit planning.



In our previous example RMM for the chance of material misstatement was 10%, resulting from an IR estimate of 50% and a CR estimate of 20% Got that? .5 x .2 = .1

Let's say an auditor decides that 5% AR means reasonable assurance for this audit.
This is a matter of professional judgment. But choosing a target risk level is the first step in audit planning.

To get to a 5% AR target for an audit we do a little algebra: DR = .05 / .1 = .5 (50%)

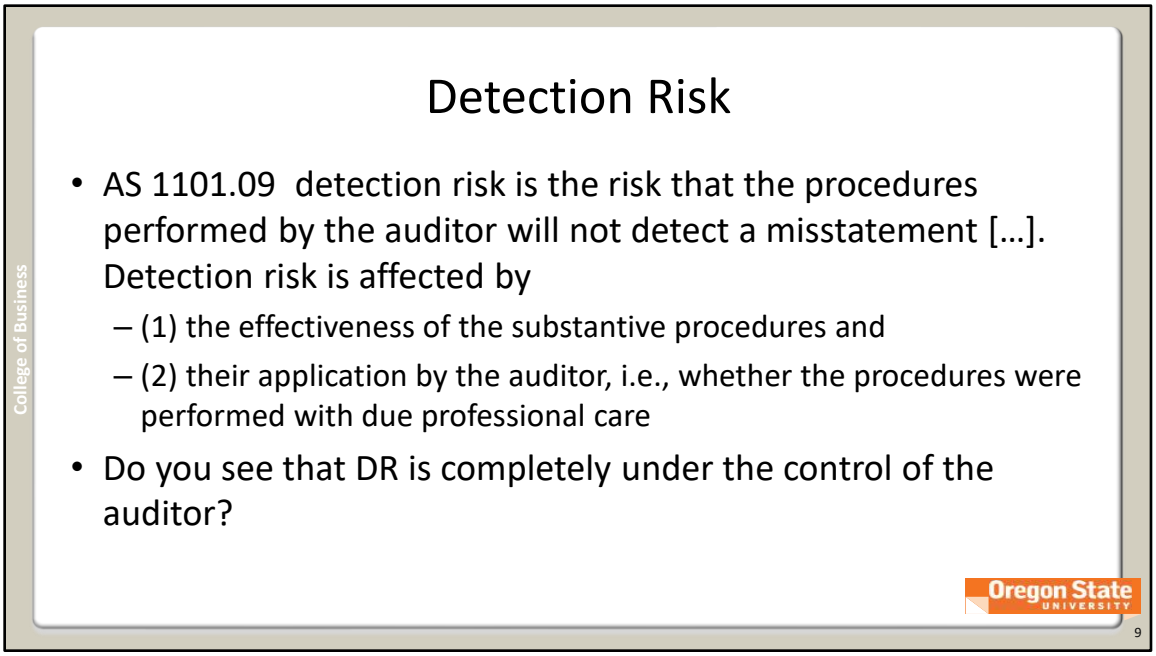
So, in planning an audit activity to get to the desired AR of 5%, we would look at a table and choose a number of items to substantively test so that it would result in a DR of 50%.
In words this means that we allow a 50% chance that a material errors would slip through the transaction testing done by the auditors. But, because we already know that there is only a 10% chance that such an error exists, this results in a 5% chance that the statements are materially incorrect.

However, this DR is often computed while planning the audit BEFORE the effectiveness of the controls has been tested.
If the controls subsequently fail their tests, the CR estimate will be higher, so DR will need to be lower to achieve the target AR.
This is the key point of connection between the financial and internal control parts of an integrated audit. Better controls mean less financial testing.

In practice, this computational approach is often not what really happens.
Instead of using percentage values, auditors often think of high, medium, or low inherent risk or control risk.
The values, instead of numbers for IR, CR, or RMM are used to determine the number of items to test. This is no problem if the software or tables you use are based on high/medium/low instead of percentages.

As with control testing, choosing the number of items to achieve the desired DR level is complex and is often done using specialized audit software or pre-computed tables. And that relates more to the financial part of the audit then the internal control part. But it is important for everyone involved to understand this relationship.

These fundamental relationships hold:
More substantive testing lowers DR.
Less effective controls or higher inherent risks means that more substantive testing is needed to achieve the same AR.



The essence of planning a financial audit is deciding which transactions, estimates, and entries need to be verified.

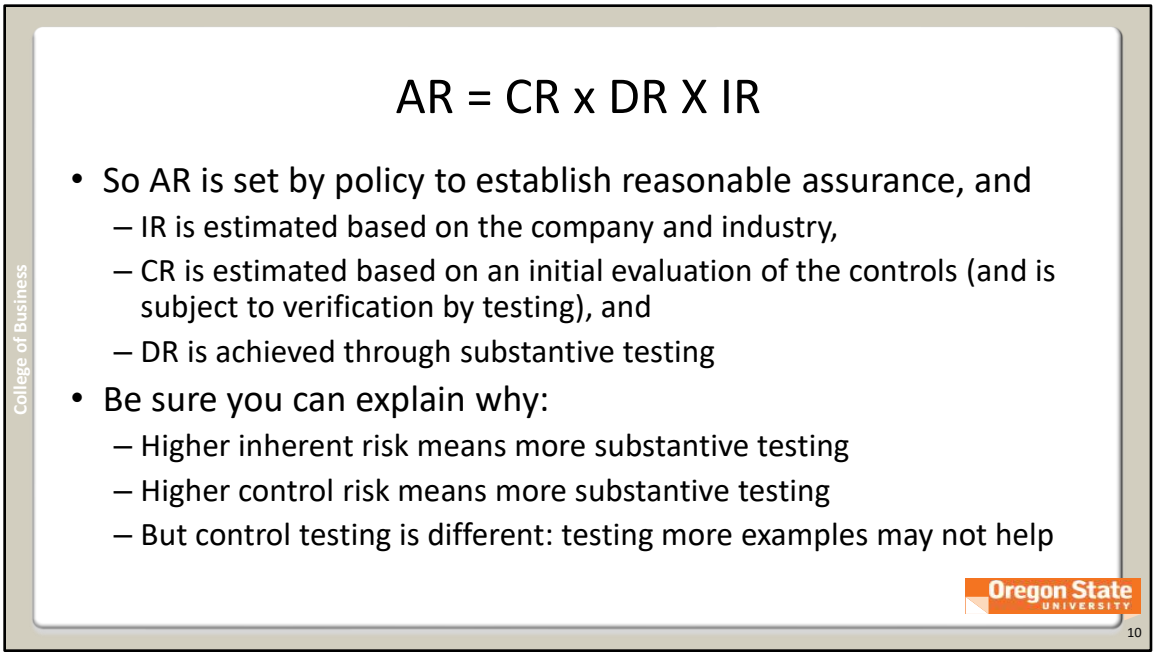
While RMM, IR, and CR are generally ascertained by the auditor, DR – Detection Risk results from the actions an auditor takes. This is important because while increased audit effort can lower DR, CR is verified by testing , and IR is not affected by testing. At the risk of repeating: more substantive testing will lower DR and AR, but more control testing does result in a lower CR and has no bearing on DR.

Detailed coverage of sampling and DR computations is out of scope for our class, but a number of sampling methods exist. They consider:

- How likely an error is thought to be.
- How many transactions there are.
- How the sample is to be selected (random?).
- The dollar amount of the transactions.
- How confident they want to be that an error will be detected by a test.

Accountants often use tables prepared by statisticians.

The answer to this decision process is something like:
We need to verify 30 of the transactions in the list to achieve a DR of 20%.
We call this kind of transaction testing “substantive testing”.



Hopefully this equation makes sense now.
The initial risk of misstatement (RMM) is estimated by considering IR and CR.

Then the audit is planned to do the following:
- Test the controls to see if the CR estimate holds up
- Perform substantive testing to achieve a DR that will result in the desired AR. If IR x CR is lower (low risk organization and strong controls) then less substantive testing is needed.

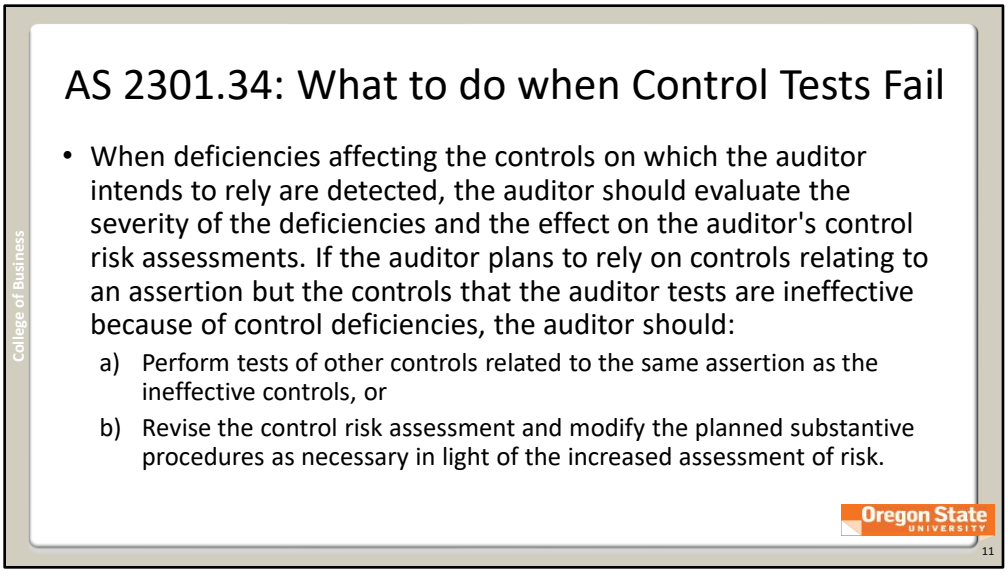
Different firms use different methodologies to establish levels and compute risk.
For our purposes, we want to understand:
- What things auditors do to establish the risk levels,
- How these factors relate to each other, and
- What happens when control tests succeed or fail.

We have already covered what these risks consist of and how they are estimated and determined.
We can talk a bit more about how they related to each other.

Most importantly for IT auditing: Audit planning cannot result in a lower actual CR value for the organization.
Beyond a certain point, more testing of the same control does not lower CR for the audit, the controls are what they are.

Why is that so? Once the auditor has estimated CR, they are testing to see if the estimate is supported by evidence.
If you look at 50 documents that were supposed to be initialed and all but one was, you have evidence that the control is in operation. But checking 100 documents and finding that all but two were all initialed would not be evidence that the control is more effective. For example, it would not prove that people did a better job checking or that there was not some other way error could creep in.

This is different from establishing DR with substantive testing – if you review the dollar amount accuracy of 100 transactions instead of 50 there is a higher chance that you would catch a material error so more testing changes DR, but more control testing may not change CR



Let's say we are testing to see if the amounts of various expenditures are accurate, this has at least two important implications: Financial statements may be inaccurate and weak internal control over expenditures may not ensure that funds are spent as authorized by the appropriate people in the company.

Accounts Payable process details:
- Deposits are done through a bank lock-box arrangement and monitored.
- Checks are written only though a computerized AP (Accounts Payable) system.
- Amounts from these systems are automatically posted to the GL.

Audit objective: Determine whether expenditure amounts are accurately transferred to the GL.
The audit plan uses a CR of 3%. It was estimated that there was a 97% chance that the controls in the systems would prevent materially inaccurate amounts from being posted from the AP system to the GL. This was based on auditor experience with similar companies with similar systems. As a result, little substantive testing is planned to verify the completeness and accuracy of AP data.

Application Control Audit Objective: Determine whether approved AP amounts will be accurately posted to the GL.

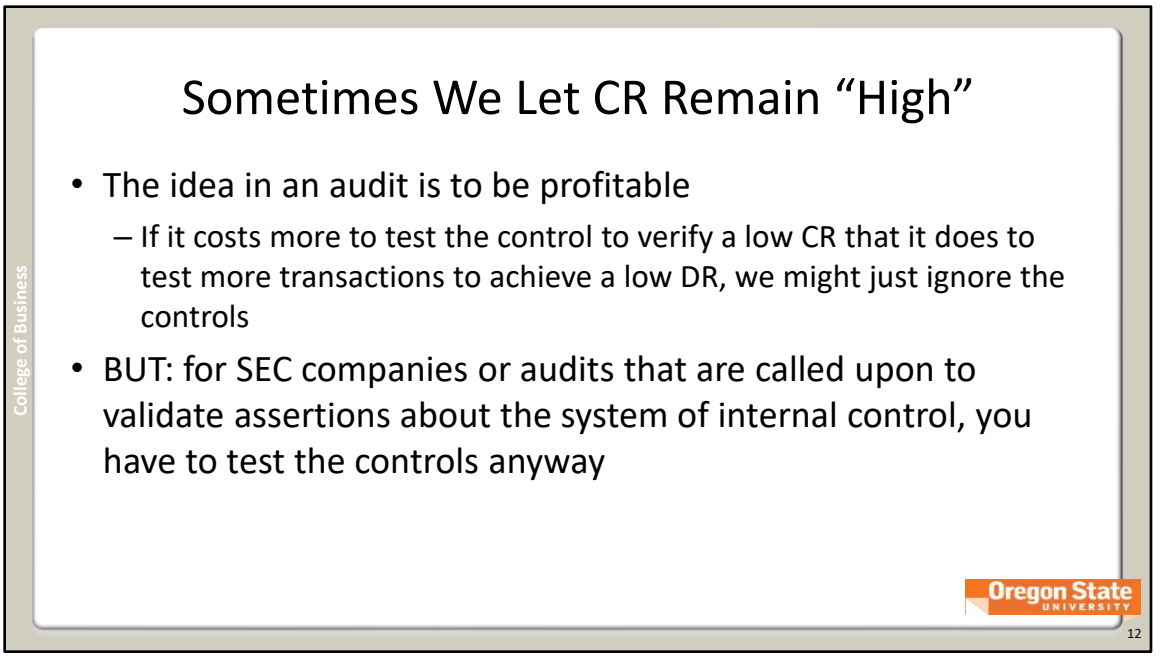
The first audit procedure is a walkthrough of the AP system:
- Identify risk points in the AP process.
- identify and assess the effectiveness of key control features or activities.
- identify control-function evidence generated by the system.

Then the auditor reviews generated evidence to ensure proper operation of the controls.
In the walkthrough, you learn that only selected individuals are to be allowed to make changes to approved checks but when you check the configuration, you discover that every AP clerk has the needed access rights to change approved checks. Oops!

At first, you think you will need to do much more substantive testing because the tested control failed.
But instead, you talk with the client and discover that there is a compensating control: Any changes to approved checks are posted to a log and that log is reviewed.
You now test that control:
- Verify that all such changes are logged.
- Verify that only system admins can change the log.
- Verify that a manager reviews the log and checks up on any changes listed in the log.

You find that there is a control deficiency that management needs to address, but you don't need to do additional substantive testing to verify the financial statement amount because you stand by your original CR estimate despite the control deficiency.

We didn't do more testing of the approval control. We decided to test the compensating control to keep our CR estimate intact.



Hopefully by now it is clear that RMM (Risk of Material Misstatement) is not fundamentally driven by what the auditor does. It is a function of the business, its environment, and its controls. The auditor cannot change those things. However, in completing an attestation engagement, auditors don't look at everything, they only want to look at enough to form opinions about assertions made by management. And those opinions are to be based on a standard of reasonable assurance.

Consider Accounts Payable. Expense and liability line items on the financial statement are generated based on the output of an Accounts Payable module in a financial reporting system.
The auditors could achieve reasonable assurance by:
- Verifying a significant number of transactions (substantive testing),
- By verifying the effectiveness of the controls over the systems that generated the reports (control testing),
- Or through some combination of the two.

Let's say AR is set at 5% and IR is assessed to be 50%
- If CR is 100% (no effective controls) DR would need to be 10%.
- If CR = 20% can be used, DR would need to be only 50%.

Remember: lower numbers mean more likely to avoid a mis-statement and it takes more testing to achieve a lower DR.

For a large organization, perhaps a government agency or SEC-regulated company, the internal controls have to be validated anyway to meet regulations. But for small private firms, the internal control assessment is only important for the financial statement audit. If regulations allow, the auditor can conduct their financial audit assuming all CR values are 100%. This is unlikely to be the 'true' level of control risk because most every organization has some control system with some level of effectiveness. But the auditor can ignore the controls if they choose to. If it costs $10,000 dollars to validate a CR of 20% but only $5,000 to achieve DR of 10% if controls are ignored, it would clearly be better to do the audit without looking at internal controls. As previously noted, this may actually mean using a level of "High" for control risk when percentages are not used, but the idea is the same.

Setting controls to 'high' can make sense when:
- Many controls are thought to be weak or poorly documented,
- The audit firm lacks expertise to do needed IT control audits, or
- Circumstances result in high control audit costs.

In general, however, it is less expensive to validate good controls than to do extensive substantive testing.