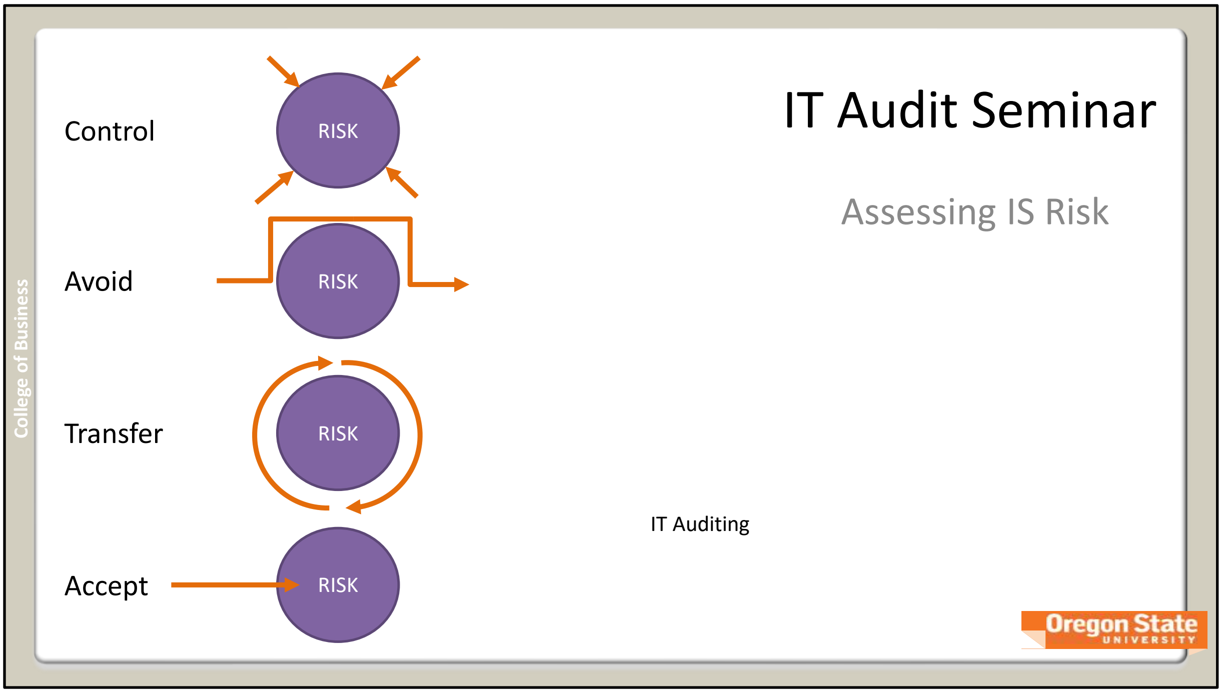


IT Audit Seminar

Assessing IS Risk

Control RISK

Avoid RISK

Transfer RISK

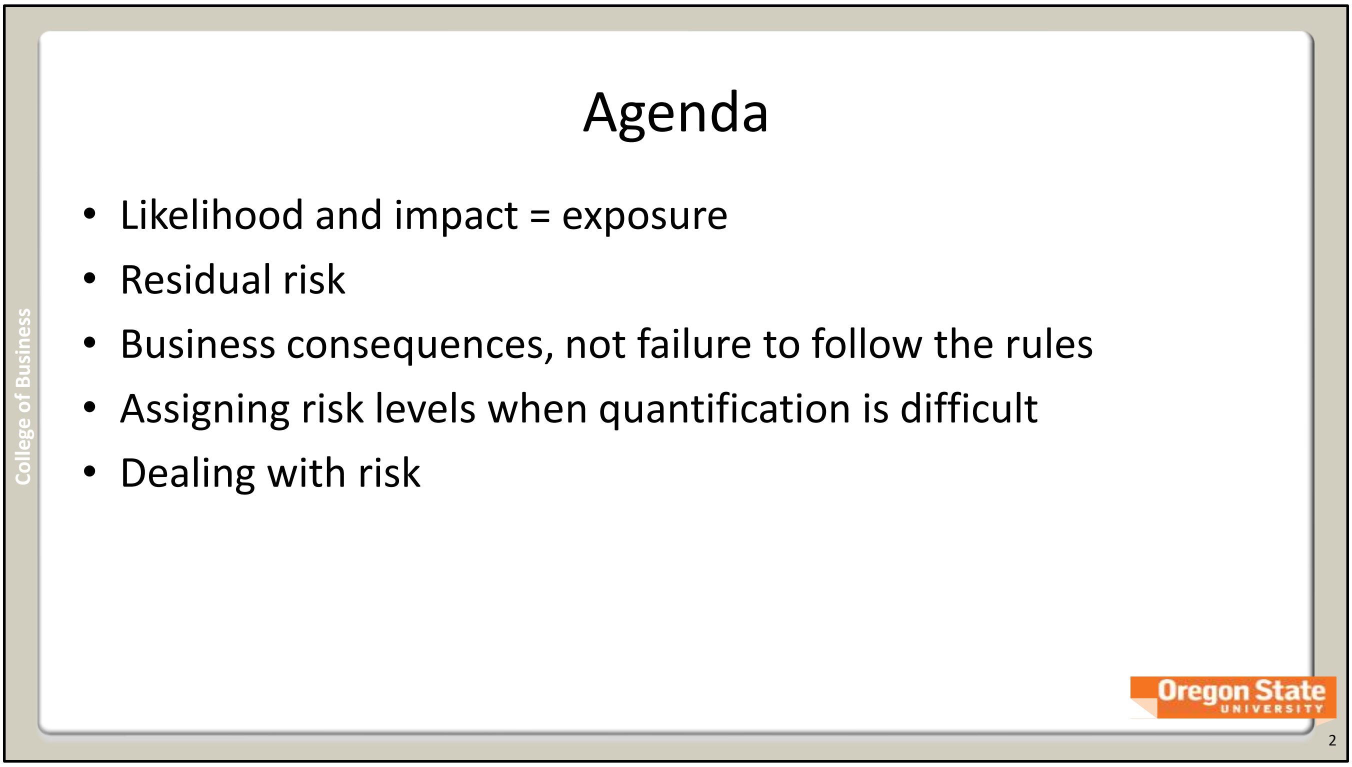
Accept RISK

College of Business

IT Auditing

Oregon State UNIVERSITY

This slide deck discusses IS risk.



Agenda

- Likelihood and impact = exposure
- Residual risk
- Business consequences, not failure to follow the rules
- Assigning risk levels when quantification is difficult
- Dealing with risk

College of Business

Oregon State University

Auditing is all about risk.

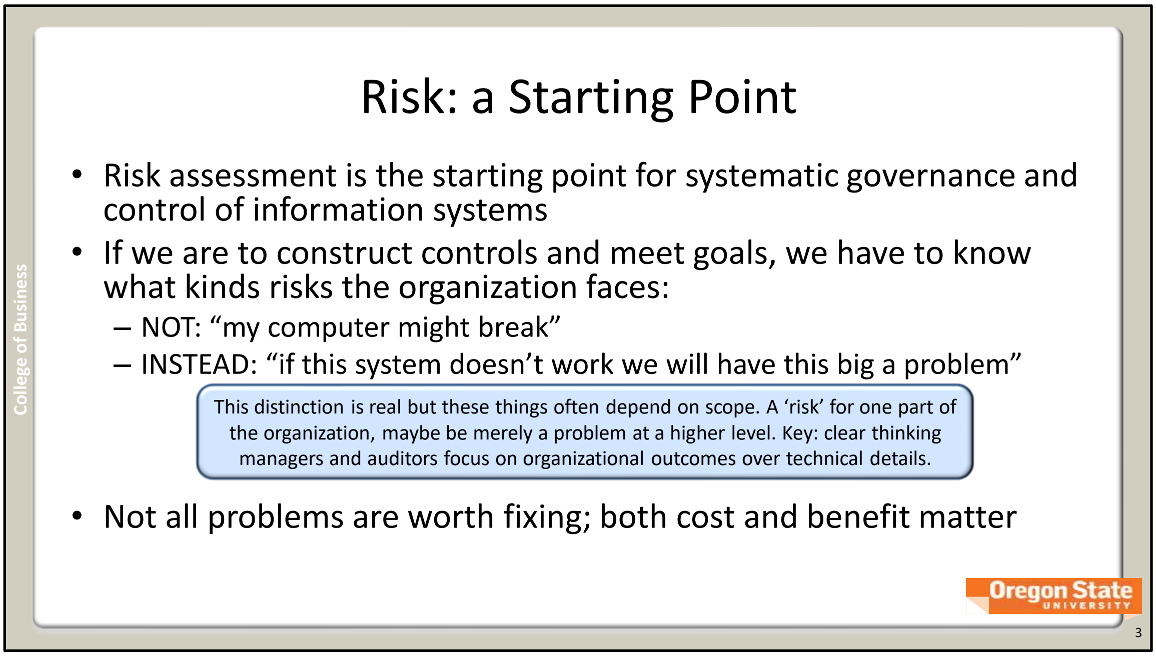
This deck will explore risk from an auditing perspective.

First we will talk about risk, emphasizing the kinds of risks faced by Information Systems.
Assessing IS risks is a central component of the internal control paradigm.

In later materials we will talk about audit risk which is all about the chance an internal audit will fail to identify material risks to the organization.

Most of the terms will be familiar:
Likelihood (probability or frequency), impact (loss or consequence), and residual (left over).
You will see how these terms are used in a risk computation.

But take a moment to think about the word residual in a risk context.
Residual risk is left over risk. We know a bad thing can happen, but we do things to keep it from happening. The chance that it will happen despite our efforts is the residual risk.



College of Business

Risk: a Starting Point

- Risk assessment is the starting point for systematic governance and control of information systems
- If we are to construct controls and meet goals, we have to know what kinds risks the organization faces:
  - NOT: “my computer might break”
  - INSTEAD: “if this system doesn’t work we will have this big a problem”

This distinction is real but these things often depend on scope. A ‘risk’ for one part of the organization, maybe be merely a problem at a higher level. Key: clear thinking managers and auditors focus on organizational outcomes over technical details.

- Not all problems are worth fixing; both cost and benefit matter

Oregon State UNIVERSITY

3

The starting point for governance of properly controlled operations is risk assessment.

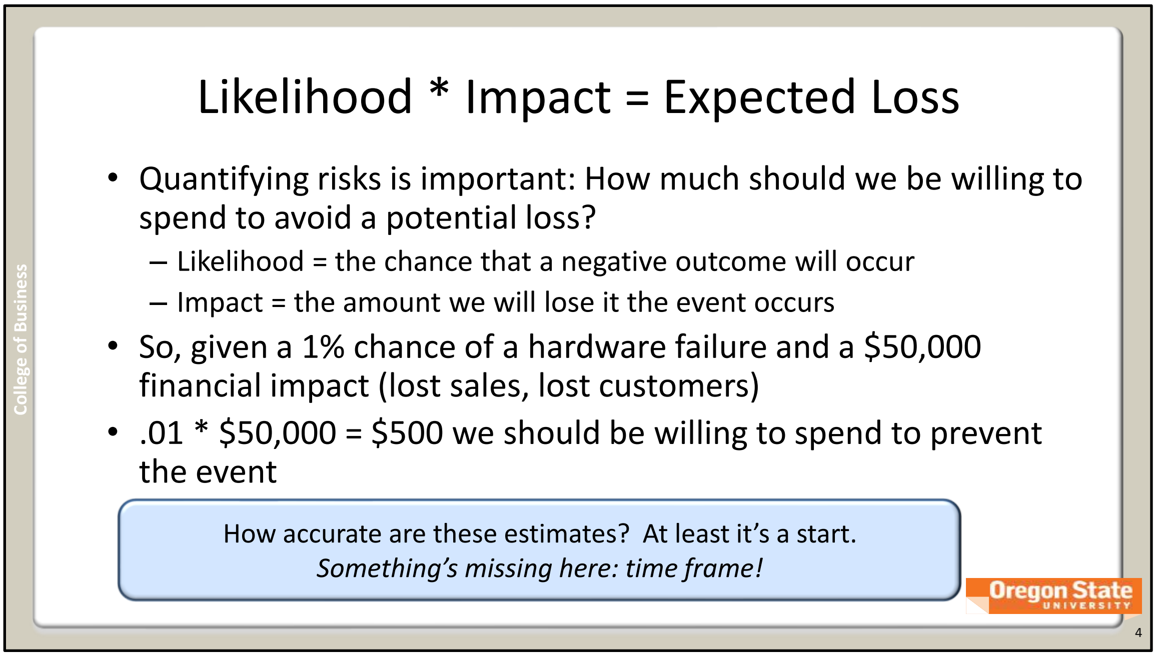
Remember that internal control is supposed to result in a variety of desirable outcomes including effective and efficient operations, protection of assets, compliance with laws and regulations, and generation of reliable financial statements.

IT audits and, more generally, internal control audits are supposed to consider the chances that an organization will fail to meet those objectives.

It is tempting to think of risks in this space as negative technical events: e.g., the hard drive in the server might fail.
That kind of thing is important but what is really important for auditing is to consider the negative consequence for the organization that is associated with sets of possible negative technical events.
For example, a network can fail in many ways, some would really hurt the organizations; others not so much.

A key task associated with risk assessment is estimating and quantifying the consequences of an event.
If a server used for a limited set of internal functions goes down, it might not cause any significant problem for a few days and it might be easily fixed in a couple of days; if so, costly controls to protect against such a failure might not be appropriate.
But in some industries, a down web site means losing buckets of cash in a few minutes.

So, in assessing risks, whether they be related to security, reliability, or availability, an organization needs to consider what it would cost them if the event occurred.



College of Business

Likelihood * Impact = Expected Loss

- Quantifying risks is important: How much should we be willing to spend to avoid a potential loss?
  - Likelihood = the chance that a negative outcome will occur
  - Impact = the amount we will lose it the event occurs
- So, given a 1% chance of a hardware failure and a $50,000 financial impact (lost sales, lost customers)
- .01 * $50,000 = $500 we should be willing to spend to prevent the event

How accurate are these estimates? At least it’s a start.
Something’s missing here: time frame!

4

Organizations seek to quantify risks in dollars so they can decide about or choose between control options.

While quantification can be somewhat arbitrary – just an informed guess in many cases – it is still often done.

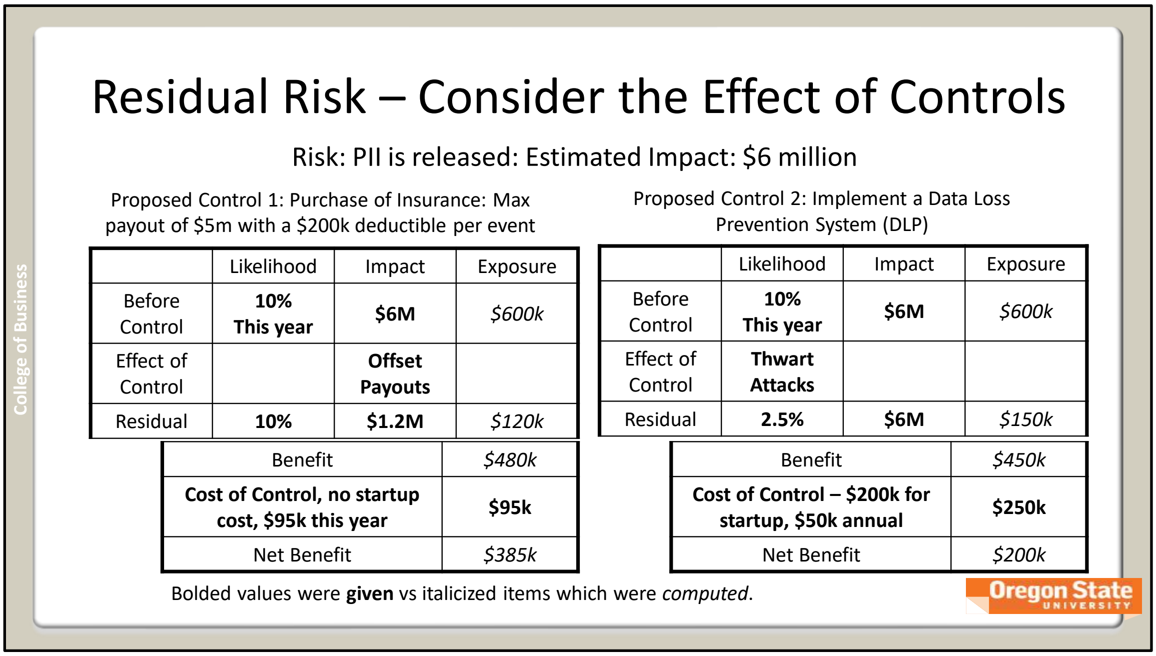
Two factors matter: Likelihood and Impact.

The likelihood is the chance that a risk event will occur.
Impact estimates the amount of money to be lost if the event occurs.
Multiply them to compute exposure.

You all understand this as some level; you travel in cars or airplanes even though you might be harmed in a crash.
You figure that the chances of a crash are small while the value of getting there is big.
Even though your REALLY REALLY don’t want to crash, you figure the risk is low despite the dire consequences if a crash happens.
So you take the chance.

Look over the computations on the slide.
This notion of “how much we should be willing to spend to protect” is just a benchmark.
But it is a well recognized place to start.

Risk quantification almost always requires consideration of a time frame. In this simplified example, no timeframe is mentioned. This is really important because if we mean a 1% chance of failure in the next week, that would be quite different from 1% in the next 5 years. We will say more on this topic later on.



Residual Risk – Consider the Effect of Controls

Risk: PII is released: Estimated Impact: $6 million

Proposed Control 1: Purchase of Insurance: Max payout of $5m with a $200k deductible per event

	Likelihood	Impact	Exposure
Before Control	**10% This year**	**$6M**	*$600k*
Effect of Control		**Offset Payouts**	
Residual	**10%**	**$1.2M**	*$120k*

Benefit	*$480k*
Cost of Control, no startup cost, $95k this year	**$95k**
Net Benefit	*$385k*

Proposed Control 2: Implement a Data Loss Prevention System (DLP)

	Likelihood	Impact	Exposure
Before Control	**10% This year**	**$6M**	*$600k*
Effect of Control	**Thwart Attacks**		
Residual	**2.5%**	**$6M**	*$150k*

Benefit	*$450k*
Cost of Control – $200k for startup, $50k annual	**$250k**
Net Benefit	*$200k*

Bolded values were **given** vs italicized items which were *computed*.

College of Business

These charts quantify risk for two controls that address the same risk. In both scenarios, risk before control is listed as $6 million in impact, times 10% likelihood, resulting in an expected loss of $600,000. In the case of a security event in which Personally Identifiable Information (PII) is released, an organization could face a number of tangible and intangible consequences, including:

- Paying for credit monitoring services for any individuals potentially affected by the release (easily quantified)
- The cost of handling the incident including reconfiguring the involved systems (can be estimated)
- The damage done to the organization’s reputation (difficult to accurately quantify)

Likelihood and the risk reduction effect of the controls are also subject to estimation.

- How could we decide on 10%? Tracking events at similar organizations is a start. But there are many possible factors: What systems and data do we have? What security controls are in place? We may be similar to peers, but these factors would vary. In the end, there is some guesswork here.

Internal control governance and IT management call for cost benefit analysis, even when some of the values are merely estimates. The tables are for two control scenarios:

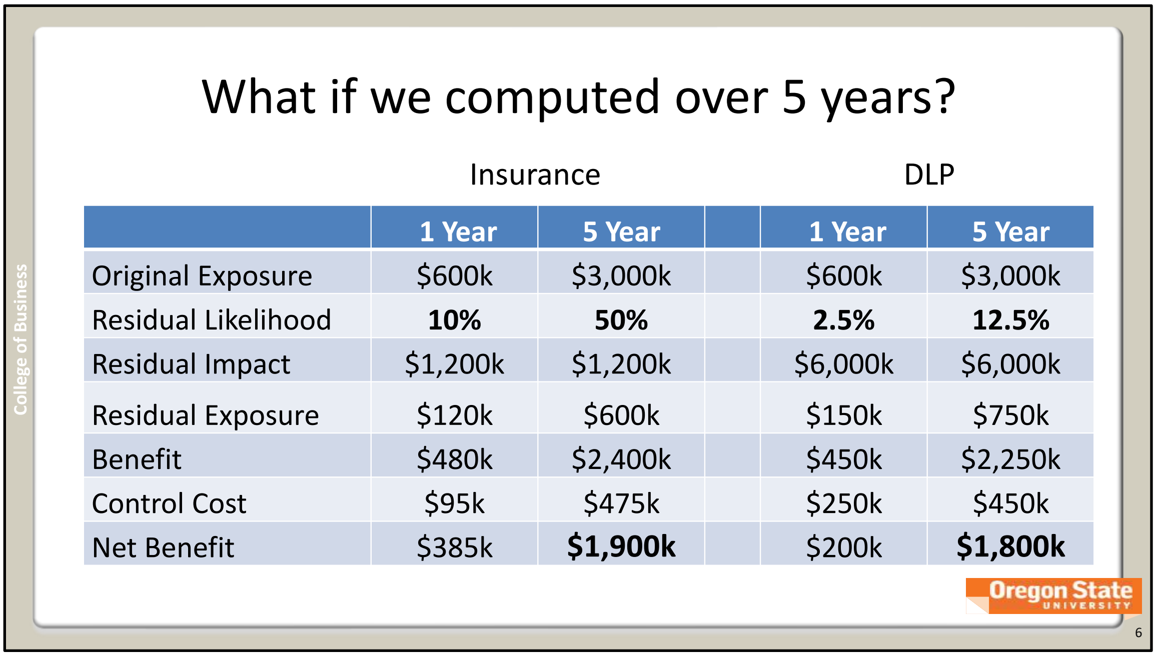
- Purchase of Insurance for $95k would provide up to $5 million to offset much of the financial impact of the associated risk
    - Residual risk is $120k: ($6m, less a $5m payout and a $200k deductible) times a 10% likelihood
    - In today’s market, the client would likely have a higher “deductible” than that, this is just an illustration!
    - The $600k risk less the $120k residual and the $95K premium cost leaves a net benefit of $385k
- A Data Loss Prevention (DLP) system costing $250k would reduce the likelihood of an event by thwarting exfiltration attempts
    - Residual risk is 120k: The full $6m risk times a 2.5% likelihood
    - The $600k risk less the $150k residual and the $250K cost, leaves a net benefit of $200k

An auditor reviewing internal control risk assessments as per COSO or assessing the design and operation of governance processes in an ITGC or compliance audit could look to see if cost/benefit analysis is built into security risk assessments and if that analysis is shown to governance bodies for consideration.

Importantly, many control decisions are tradeoffs: not all desirable controls will be implemented. You could imagine why, for example, an organization might purchase the insurance shown on the slide but not immediately invest in an expensive data or digital loss prevention (DLP) system. It is hard to know just how much protection would be provided by DLP making it harder to compellingly justify the calculations. With the insurance, the calculated payoff is higher, and the uncertainty is lower.

But on the other hand, the loss of reputation may not be adequately considered in the impact valuation; an organization would much prefer to not have the attack succeed apart from dollar value impact, so reducing the likelihood to 2.5% would be valued.

In any case, this analysis introduces some realistic elements associated with organizational risk assessment.



College of Business

What if we computed over 5 years?

	Insurance			DLP	
	1 Year	5 Year		1 Year	5 Year
Original Exposure	$600k	$3,000k		$600k	$3,000k
Residual Likelihood	**10%**	**50%**		**2.5%**	**12.5%**
Residual Impact	$1,200k	$1,200k		$6,000k	$6,000k
Residual Exposure	$120k	$600k		$150k	$750k
Benefit	$480k	$2,400k		$450k	$2,250k
Control Cost	$95k	$475k		$250k	$450k
Net Benefit	$385k	**$1,900k**		$200k	**$1,800k**

Oregon State UNIVERSITY

6

First: Make sure you understand the computations from the previous charts:

- Likelihood * Impact = Exposure
- Original Exposure less Residual Exposure = Benefit of the control
- Benefit of the control less Cost of control = Net Benefit

This table expands the analysis by simplistically projecting exposure, control cost, and benefit over a five-year period. You should be able to build this chart from the information on the previous slide.

The impact of a single event does not change, but exposures are five times as large because an annual likelihoods accumulate. Notice how the reduced likelihood grows over time. For one year, the difference in likelihood between the two alternatives is only 7.5%, but over 5 years it is 37.5%. That's a big difference and that difference results in a substantially different risk picture.

Further, unlike insurance, the implementation of the DLP system creates an asset that has value over time. First year (startup) costs are high while ongoing costs for operating the control in future years are relatively low. So, while a one-year analysis makes the DLP system seem far more expensive than insurance, a longer-term view shows them to be comparably expensive.

The DLP system still loses out by a small margin saving an estimated $1.8 million as compared to $1.9 million for the insurance. But both show a substantial payoff over time. Maybe we should both install DLP AND purchase insurance.

As is typical, the extended estimates are not all that precise. Events may intervene to substantially change the picture.

Consider:

- If there was an event, the insurance costs would explode, and insurance might become unavailable.
- In recent years, insurance prices have skyrocketed even for well protected organizations, but technology costs for the same capability usually go down over time.
- Insurance terms are changing. If you install good controls, insurance costs may go down.
- Installing a DLP system would likely entail many other security improvements such as improved authorization processes, network monitoring, and network segmentation. Technical controls for one risk can reduce exposure for other risks as well.
- On the other hand, setting up DLP might distract key people from working on even more valuable controls or other valuable IT projects.

Financial quantifications can be informative. But they are only a starting point for prioritization decisions.

HEADS
TAILS

College of Business

Bad or Not Good: Two Sides of the Risk Coin

Bad Things Might Happen

Good Things Might Not happen

Oregon State UNIVERSITY

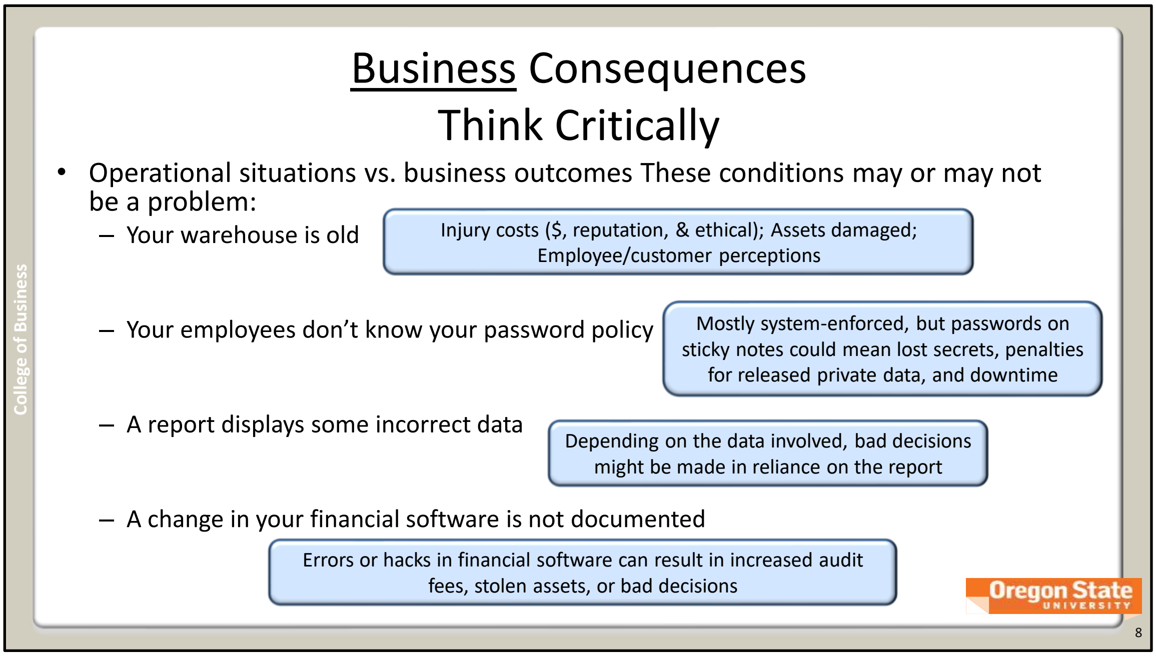
7

Risks we might assess include:

- Negative events like having intellectual property stolen or data bases being fraudulently altered.
- And the lack of good events, for example failing to meet growth objectives.

Both kinds of things can be addressed by controls, and maybe the difference is just a matter of semantics. Remember the definition of internal control? A good control system is supposed to result in effective and efficient operations – these are good things. When we do risk assessment in the control system sense, we think of failing to accomplish these objectives as a risk.

Many controls, including governance controls seek to foster effective operations apart from preventing negative events such as cybersecurity hacks or fraud.
For example, checking budget vs. actual on expenses may be useful in detecting fraud, but it is more likely to be useful in controlling costs to protect profitability.
And carefully crafting contracts with cloud-based service providers contributes to employee productivity in addition to protecting against business shutdowns or loss of intellectual assets.



Business Consequences Think Critically

- Operational situations vs. business outcomes These conditions may or may not be a problem:
  - Your warehouse is old
    - Injury costs ($, reputation, & ethical); Assets damaged; Employee/customer perceptions
  - Your employees don't know your password policy
    - Mostly system-enforced, but passwords on sticky notes could mean lost secrets, penalties for released private data, and downtime
  - A report displays some incorrect data
    - Depending on the data involved, bad decisions might be made in reliance on the report
  - A change in your financial software is not documented
    - Errors or hacks in financial software can result in increased audit fees, stolen assets, or bad decisions

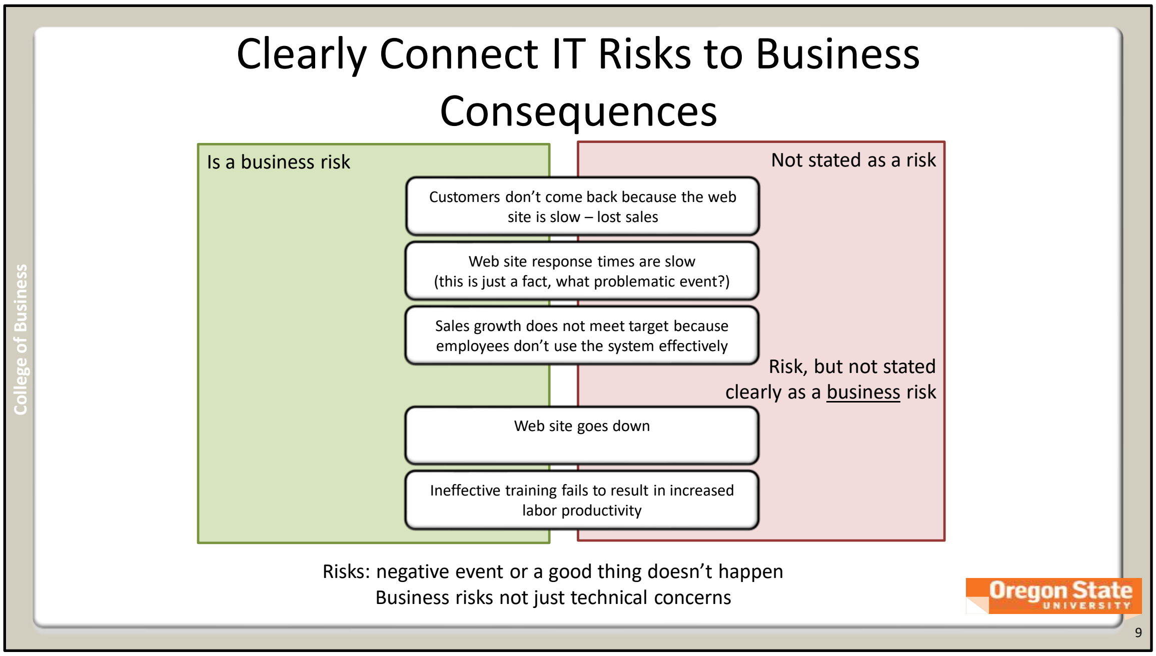
Look over the consequences in the blue boxes.
Some are pretty tangible: stolen assets, medical bills, paying for credit monitoring for customers whose PII (Personally Identifiable Information) you accidentally leaked.

Others are much harder to estimate:

- How much business would you lose if your reputation was damaged?
- How much would a bad decision cost you?

The point is that even if a risk is difficult to quantify, it is often useful to try to put a dollar amount on it so as to inform decision makers about the risk and support comparison between competing proposed control mechanisms.

Auditors investigating internal control always need to understand the business impact of control failure. Otherwise, they are likely to waste time auditing unimportant activities or emphasize the wrong things in their reports.



College of Business

Clearly Connect IT Risks to Business Consequences

Is a business risk

Not stated as a risk

Customers don’t come back because the web site is slow – lost sales

Web site response times are slow
(this is just a fact, what problematic event?)

Sales growth does not meet target because employees don’t use the system effectively

Risk, but not stated clearly as a business risk

Web site goes down

Ineffective training fails to result in increased labor productivity

Risks: negative event or a good thing doesn’t happen
Business risks not just technical concerns

9

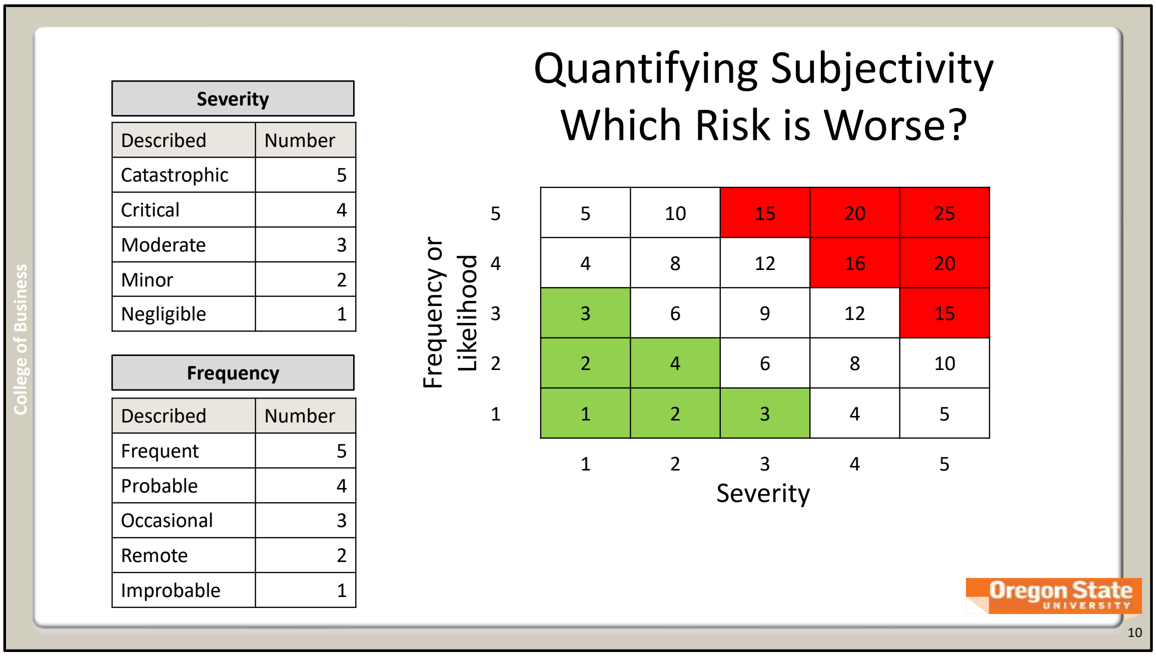
The animations in this slide can help you practice differentiating business risk from technical risk.

Were you able to properly anticipate the answers?

Lost sales is a business consequence.
Lots of web sites are slow, sometimes it matters, sometimes it doesn’t. Its hard to tell from this description.

Sales growth is an important business objective. Failing to meet that such an objective a business risk.
Similarly, labor productivity growth is a business objective and training should be helping with that.

As with many professional judgements, sometimes a bit of interpretation is needed. There are probably very few organizations who would not be harmed in obvious ways if their web site went down. Still, it is possible that a website is immaterial to the operations of a company. Auditors and other IT risk managers need to gather meaningful indications as they estimate the size of a risk.



College of Business

Quantifying Subjectivity
Which Risk is Worse?

Severity	
Described	Number
Catastrophic	5
Critical	4
Moderate	3
Minor	2
Negligible	1

Frequency	
Described	Number
Frequent	5
Probable	4
Occasional	3
Remote	2
Improbable	1

Frequency or Likelihood					
5	5	10	🟥 15	🟥 20	🟥 25
4	4	8	12	🟥 16	🟥 20
3	🟩 3	6	9	12	🟥 15
2	🟩 2	🟩 4	6	8	10
1	🟩 1	🟩 2	🟩 3	4	5
	1	2	3	4	5
			Severity		

Oregon State UNIVERSITY

10

In many cases risk assessment is difficult to quantify.
When an organization is choosing between control options or comparing risks across the organization, it may not be worth while to apply rough dollar estimates so relative values are often employed.

For example, a hospital may be trying to decide on priorities:
- Reduce the chance that patient information will be stolen by hackers.
- Reduce the chance of fraudulent billing activities being blamed on the hospital.
- Reduce the chance treatment data will be mis-coded resulting in non-payment by insurance.

These all could be quantified in dollars but those assessments would be subjective because so many factors would be involved.

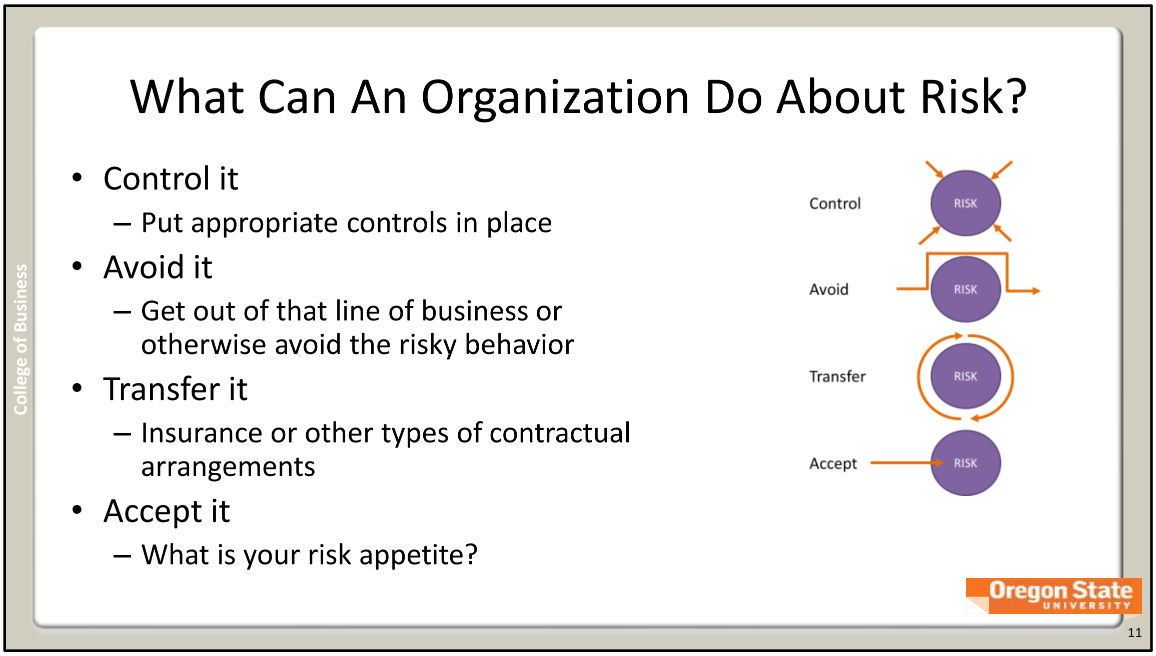
A matrix approach like the one shown here allows comparison of very different risks even with subjective estimates.
Perhaps it is probable that some treatment data will be mis-coded resulting in a loss of revenue, but that risk would have only moderate consequence.
Those assessments would result in a risk score or 12 on the chart (4 times 3) – a white box on the chart.

If the security program is thought to be weak, a breach in the near future might be thought to be probable and the severity to be critical as the hospital could lose funding for violating HIPAA by releasing Personal Health Information (PHI) and suffer a significant loss of reputation. These estimates would result in a risk score of 16 (4 times 4) – a red box.

There is thought to be only a remote frequency of billing fraud because there are extensive procedures for ensuring only delivered care is billed and any impact would be considered minor because it would not make headlines or result in regulatory action.
This would result in a score of 4 (2 times 2) – a green box.

This kind of analysis is appropriate for many kinds of internal control risk assessment because it provides governance bodies with a way to compare risks and set priorities.

In extensive risk analyses you try to come up with comparable 1-5 numbers across very different risks – say the chance of losing a patient because of IT failure vs the chance of a cybersecurity event. It isn't precise, but it can be informative.
You want to protect against risks in the red boxes first.



College of Business

What Can An Organization Do About Risk?

- Control it
  - Put appropriate controls in place
- Avoid it
  - Get out of that line of business or otherwise avoid the risky behavior
- Transfer it
  - Insurance or other types of contractual arrangements
- Accept it
  - What is your risk appetite?

Control
RISK
Avoid
RISK
Transfer
RISK
Accept
RISK

Oregon State University

11

While a full coverage of risk mitigation is not in scope for this class, IT auditors need to understand what organizations can do about identified risks.

Different organizations appropriately handle risk differently.

- Some risks are controlled, e.g., Cybersecurity processes and safeguards are implemented.
- Some risks are avoided, e.g., Don't sell child versions of your product.
- Some risks are transferred,
  - e.g., Errors and omissions insurance or cybersecurity event insurance can be purchased.
  - e.g., Include liability clauses in a contract with a third party that hosts your eCommerce site.
- Some risks are accepted: "We know that could happen, but we are prepared to take that chance".

Understanding risk appetite or tolerance is important:
For example, a start up company may choose not to implement some governance controls because they might distract key managers from innovation and slow down the rate of change. As a result, they may find themselves suddenly out of business because of some operational failure or unanticipated risk. That's ok, startups are supposed to be high risk and reward operations – their investors allow, or even demand risk taking.

But it's bad when an organization is unknowingly taking on risk or when an auditor doesn't properly understand risk or mitigation. As an auditor, you should think about the organization's risk profile:

- Organizations with high risk appetite for some circumstances might well need to be audited with that in mind.
- Considering the control environment may be especially important even if it seems like the right controls are in place because lack of top management support may mean controls are less effective then expected.
- You might expect certain controls based on guidance from resources such as FISCAM. But actually, a particular agency may have transferred or avoided certain risks making the specified controls unnecessary.

Don't over apply avoidance and transfer. For example, even if a third party builds and runs your web site or handles credit card payments, you could suffer if they inappropriately release your customers' data or foul up your operations. Avoidance means "this won't happen to us", transfer means someone else will pay for the damages. So, using a third party service only transfers risk if a contract requires them to pay in case of a risk event. Weaseling out of such a contract is not uncommon.

In short, internal control is all about risk, and proper auditing is always risk-based – auditors need to understand risk concepts.