Security+ SY0-601

Module 8: Risk

Table of Contents.

1. Risk concepts.
2. Risk types.
3. Risk assessment and analysis.

Learning objectives.

Upon completion of this module, you should be able to:

- Explain the concepts and key terms associated with risk.
- Explain the sources of risk. List examples of various risk types.
- Differentiate between qualitative and quantitative risk assessments. Explain and demonstrate key terms and formulas for assessing and prioritizing individual risks.

Risk concepts.

RISK CONCEPTS.

Key concepts.

In this section, we will cover the following key concepts:

- Risk management.
- Assets.
- Vulnerabilities.
- Threats.
- Actors.
- Risk management strategies.
- Required notifications.

RISK CONCEPTS.

Risk management.

Risk management is the process of identifying, assessing, and minimizing vulnerabilities and threats to the essential functions of a business.

There are five phases to this process:

1. Identify mission essential functions.
2. Identify vulnerabilities.
3. Identify threats.
4. Analyze business impacts.
5. Identify risk response.

Each business process and the threat must be assessed with a degree of risk to the organization.

Two main issues reviewed in this assessment are:

1. Likelihood (Probability of risk being realized).
2. Impact (Severity of risk).

RISK CONCEPTS.

Assets.

Assets are anything of value to an organization, such as data, IP, people, software, or hardware.

Administrators need to know what assets they have; you cannot do a risk assessment, assign risk levels, or train without knowing the assets and the value placed on each.

An inventory should be kept up-to-date at all times.

You can find most hardware assets by running a simple scan; some tools can assist. It is best to put a UPC label on each hardware asset and scan it into an inventory system.

Non-hardware assets are not as easily identified; however, assets such as intellectual property and other forms of data must also be inventoried and classified to place appropriate controls upon them.

Don't forget about human assets. Keep human safety in mind when designing security controls.

RISK CONCEPTS.

Vulnerabilities.

A vulnerability is a weakness that could be triggered and cause a security breach; this can be done purposefully or accidentally.

Frequently, it is a security loophole that allows an attacker to enter a system by bypassing user authentication.

Many vulnerabilities are due to a weakness in the design or implementation of a system. Insecure configurations, such as unencrypted protocols, may lead to network intrusions and access to applications and data. Some vulnerabilities are due to inherent technology weaknesses that make some systems or software more prone to attack.

Examples of vulnerabilities may include improperly configured or installed hardware or software, delays in applying or testing software and firmware patches, insecure password storage, or not sanitizing user input.

RISK CONCEPTS.

Threats.

- Threats are the potential for someone or something to exploit a vulnerability, which may be intentional or unintentional.

- There are many threats to an IT system, but not all threats are as important as others. The IT professional must take a data-driven and logical approach to make decisions on how to best combat threats; it is often wise to use best-practice guidance from reputable governance bodies to assist in making these decisions.

CONTINUED ON NEXT SLIDE >

RISK CONCEPTS.

Threats.

- The IT professional must also include other stakeholders from within the company who can help work through the risk management process.
- Threats come from many directions; IT professionals must keep themselves informed by reading through a weekly or daily brief of threats that have been identified.

RISK CONCEPTS.

Threat actor.

- Threat actors are persons or things that pose a threat.
- There are many types of threat actors — they can be internal or external, intentional or unintentional. Additional threat actors include script kiddies, hacktivists, organized crime, a nation-state, or an advanced persistent threat; each has different motivations and intent and must be studied to understand how they could be a risk to your organization.

RISK CONCEPTS.

Risk management strategies.

- Acceptance is when you assign no security control to the risk due to either a high cost for the control, the asset's value not being great enough, or applying security controls causes an undue delay in a workflow. Administrators need to monitor an acceptance response since no control was implemented — this could still be an entry point that an attacker could exploit.
- Transference is assigning the risk to a third party, such as insurance or a warranty. Cybersecurity insurance now covers both first- and third-person financial losses resulting from data breaches and other cybercrimes; it should be noted, however, that legal liabilities do NOT get completely transferred.

CONTINUED ON NEXT SLIDE >

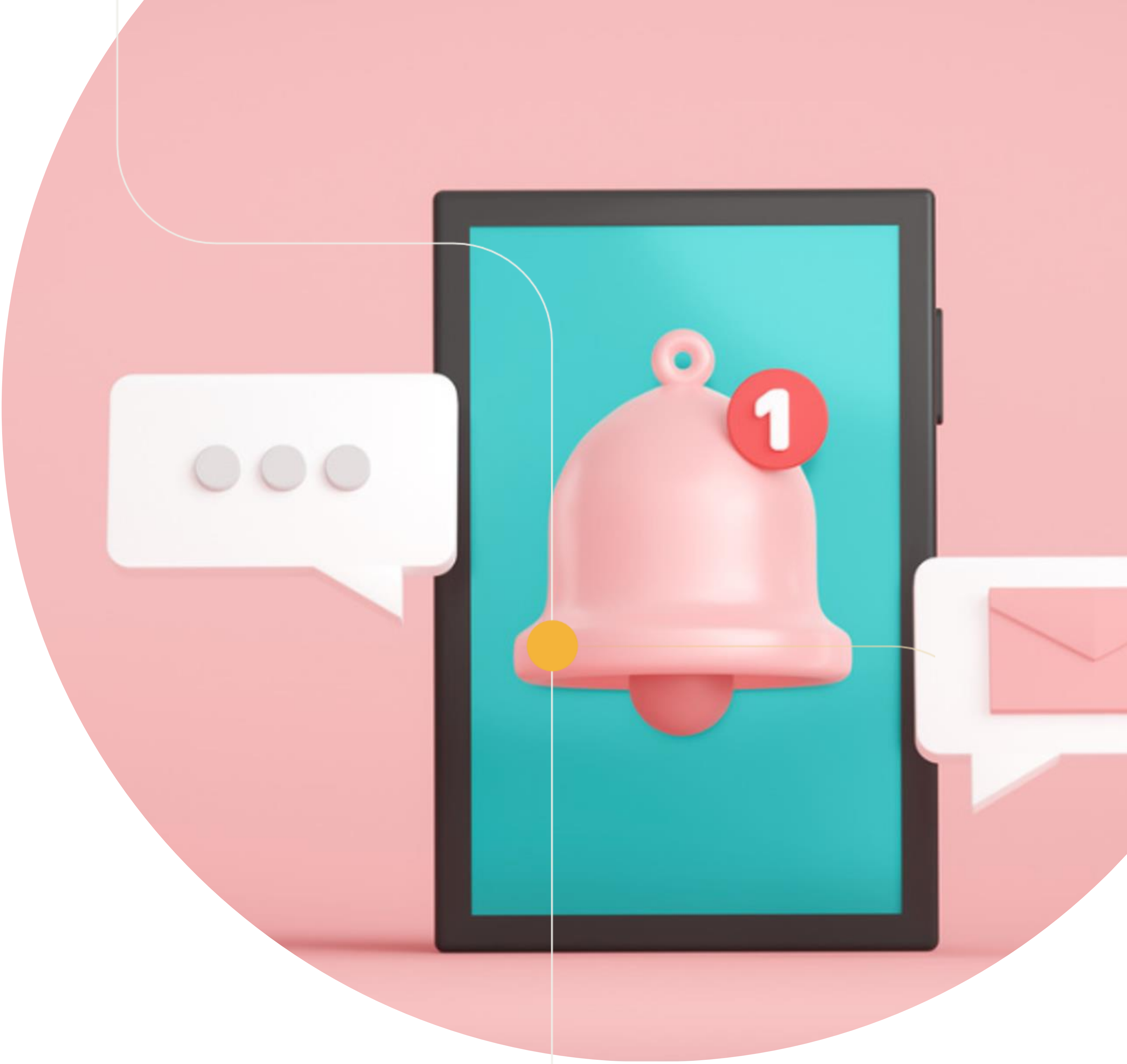
RISK CONCEPTS.

Risk management strategies.

- Avoidance is when you stop doing a risky activity. While it may seem like an easy solution, stopping an activity may have other consequences.
- Mitigation (remediation) is the overall process of reducing exposure to risk factors.
- Risk reduction refers to a set of controls that reduces the likelihood or cost of a risk being realized.

RISK CONCEPTS.

Required notifications.



Due diligence is a legal term that refers to meeting the legally-imposed obligations; failure to do so may constitute negligence, resulting in criminal or civil liabilities.

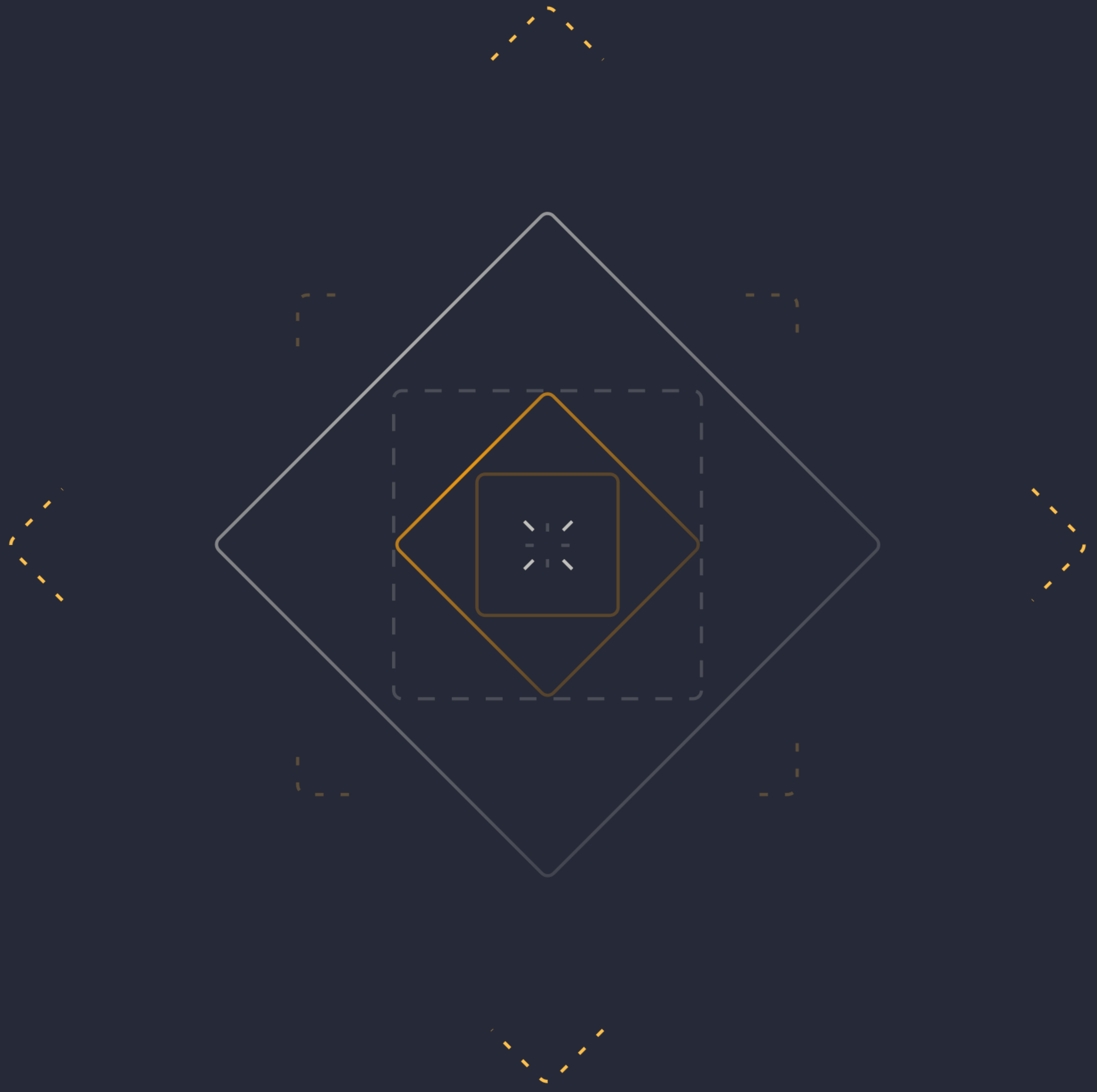
For Example: In the US, one well-known law that arose out of the fraudulent accounting practices of the Enron Corporation is the Sarbanes-Oxley Act, commonly referred to as SOX.

RISK CONCEPTS.

Knowledge check.

Let's apply what we have covered:

- What is a vulnerability?
- What is a threat?



Risk types.

RISK TYPES.

Key concepts.

In this section, we will cover the following key concepts:

- Internal.
- External.
- Natural.
- Person-Made.
- Intentional.
- Accidental.
- Legacy Systems.
- Multiparty.
- IP theft.
- Software compliance/licensing.

RISK TYPES.

Internal.

- Internal: Risks to assets owned and managed by your organization are internal; these can be malicious, accidental, or non-malicious. Internal risks are caused by employees or contractors — people with authorized access to your systems.

- Using least privilege, job rotation, and employee monitoring is the best defense against internal risk.

RISK TYPES.

External.

- External: Risks that come from outside your organization are external; these are caused by threat actors with no privileged access. The most frightening attacks come from skilled and sophisticated external hackers. These attackers can find network vulnerabilities or socially manipulate insiders to get past outer network defense.
- External risk also includes natural disasters, fire, and accidents.

RISK TYPES.

Natural.

Natural: A natural risk is a disaster event that negatively impacts an organization, such as an earthquake, hurricane, tornado, or flooding.

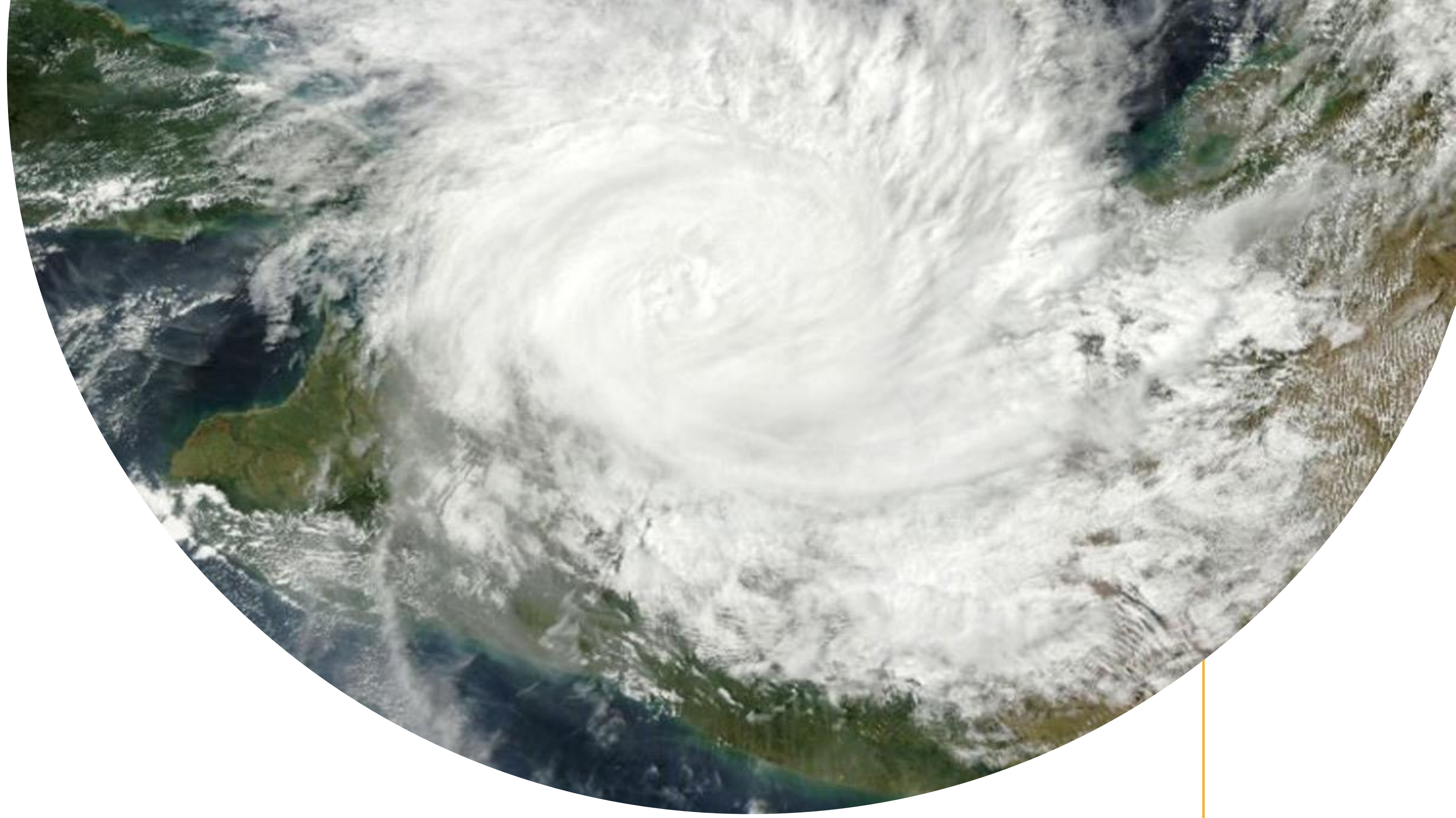
Disaster planning should be a big part of upper management planning efforts. Depending on the company's geographic location and the prevailing weather patterns, each company must prepare for different possibilities.

Natural risk often means company personnel will be unable to make it back to work, so cross-training is an important aspect of this planning.

CONTINUED ON NEXT SLIDE >

RISK TYPES.

Natural.



Companies should also look at backup sites in different geographic areas that will not be impacted by the same natural risk event. IT professionals must be ready to ensure power and connectivity are not affected anytime a weather event happens; if you can't, make sure you have a backup site and that everything is moved before the event.

RISK TYPES.

Person-made.

Person-made: A person-made risk is a disaster event where a human is a primary cause; this can be war, terrorism, or something as simple as cutting through a telecom cable.

RISK TYPES.

Intentional.

Intentional: Intentional risk is when a threat actor purposefully and wilfully performs a malicious act on your system.

Intentional acts can be overt and direct action (when an employee with access to customer credit card information sells it to a third party) or be from individuals who use covert technical means.

Risk management demands that we think like an attacker:

- Can someone easily get into the server room?
- Could someone shred the patch cables going into the switch?
- Could someone use a USB to load malware?

RISK TYPES.

Accidental.

Accidental: Accidental risks are not malicious nor intended; these threats often result from a lack of training or following instructions.

Training is the number one deterrent to accidental risk.

For example, clicking on a phishing link, leaving sensitive materials on desks uncovered, not locking up sensitive materials and more.

RISK TYPES.

Additional risk types.

- **Legacy Systems** no longer receive security updates as they have exceeded End of Life (EOL) and End of Service Life (EOSL) periods.

- **Multiparty** risk is when your organization is dependent on other organizations for some portion of the product or service you develop or provide.

CONTINUED ON NEXT SLIDE >

RISK TYPES.

Additional risk types.

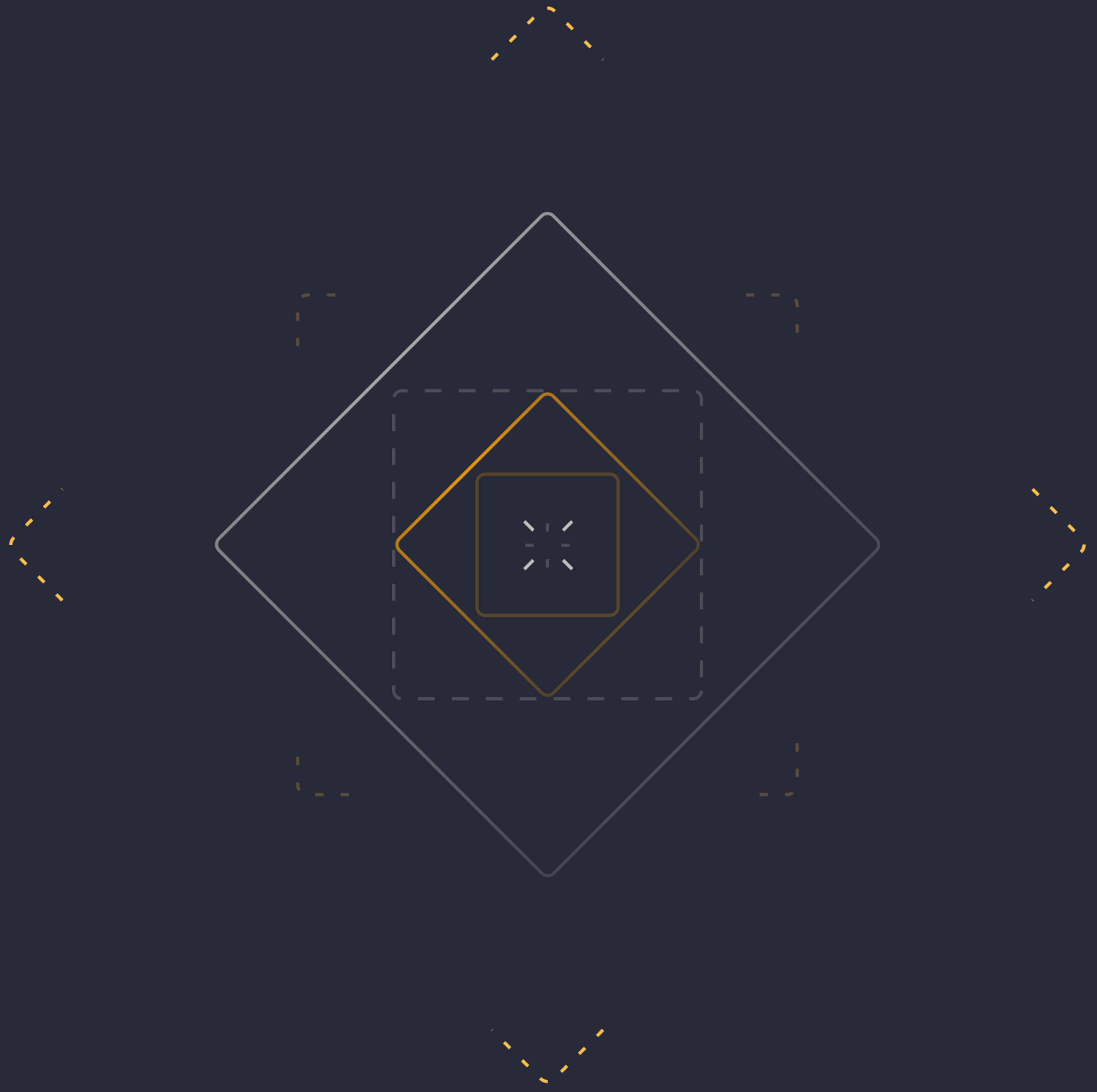
- IP Theft is any data of commercial value to an organization. Exfiltration and release of IP to the general public may cause the loss of commercial value.
- Software Compliance/Licensing must continuously be audited to ensure the End User Licensing Agreement (EULA) terms are not violated.

RISK TYPES.

Knowledge check.

Let’s apply what we have covered:

- What is an example of an internal risk?
- What is an example of an external risk?



Risk assessment and analysis.

RISK ASSESSMENT AND ANALYSIS.

Key concepts.

In this section, we will cover the following key concepts:

- Impact.
- Probability.
- Quantitative assessment.
- Risk matrix.
- Qualitative assessment.

RISK ASSESSMENT AND ANALYSIS.

Key concepts.

In this section, we will also cover the following key concepts:

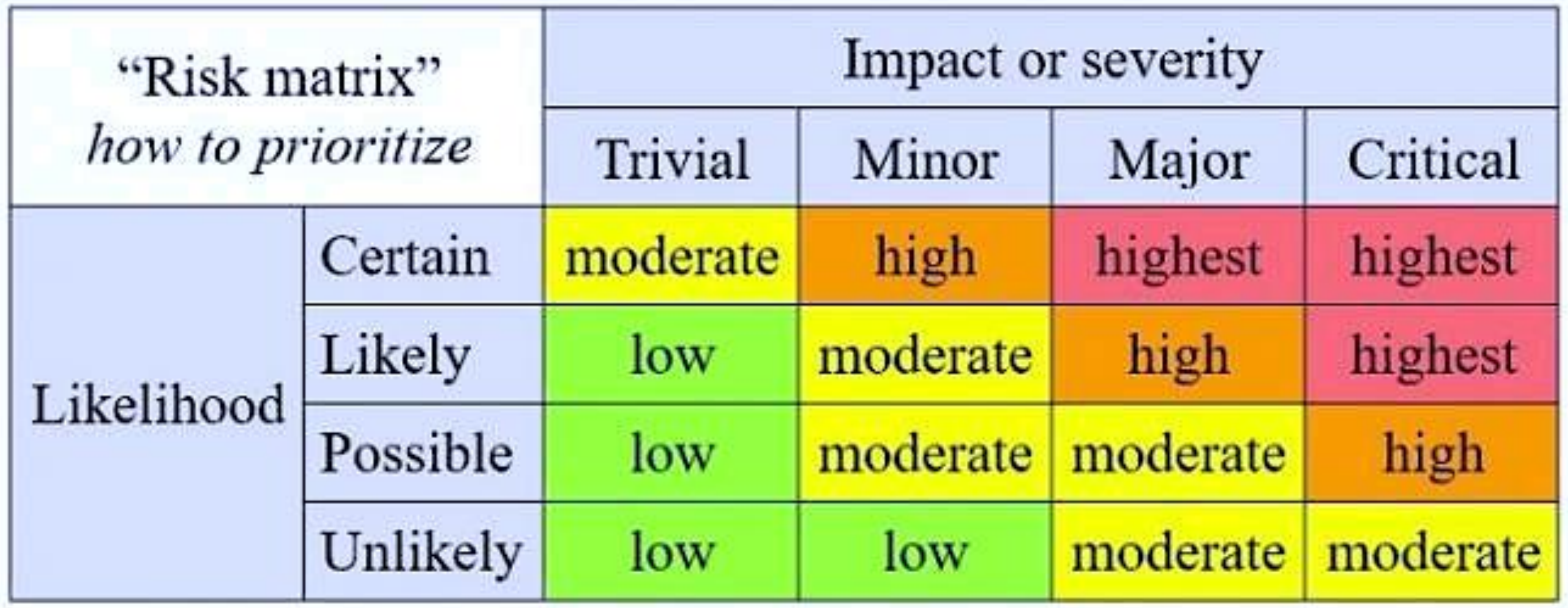
- Qualitative assessment.
- SLE/ARO/ALE.
- Risk control assessments.
- Risk analysis terms.
- Risk register.

RISK ASSESSMENT AND ANALYSIS.

Impact.

The impact is the severity of a risk if it is realized as a security incident.

The impact may be determined by the asset's value or the cost of disruption if the asset is compromised. Impact, therefore, is an important piece when determining the Risk Matrix and assigning a priority to it.



“Risk matrix” *how to prioritize*		Impact or severity			
		Trivial	Minor	Major	Critical
Likelihood	Certain	moderate	high	highest	highest
	Likely	low	moderate	high	highest
	Possible	low	moderate	moderate	high
	Unlikely	low	low	moderate	moderate

RISK ASSESSMENT AND ANALYSIS.

Probability.

Probability is the likelihood of a threat being realized.

Probability is one of the factors used in determining how to respond to risk; however, just because the probability of something happening is high does not mean it has the highest priority to be mitigated — costs, business impact, and other factors must also be considered.

In most cases, IT professionals will have to prioritize mitigation measures based on, amongst other things, probability — if it has a lower probability, these measures will be lower on the priority list.

RISK ASSESSMENT AND ANALYSIS.

Qualitative assessment.

A qualitative assessment is a risk assessment methodology that seeks out people's opinions on the significance of risk factors, generalized into simple categories such as high, medium, and low.

A qualitative assessment emphasizes "experience" and "what I think" rather than measurable information.

You will generally see a qualitative assessment when a "stoplight" chart is shown.

RISK ASSESSMENT AND ANALYSIS.

Risk matrix / heat map.

A risk matrix/heat map is a tool to help security professionals prioritize which vulnerabilities pose the greatest risk to the organization.

RISK ASSESSMENT AND ANALYSIS.

Quantitative assessment.

A quantitative assessment is a risk assessment methodology that applies numerical values to each risk factor, which can be prioritized. A quantitative assessment is the preferred method of weighting risk.

Risk management meetings that an expert facilitates will use quantitative approaches, even with what many might feel are qualitative measures. Anytime you can apply numerical values, you increase your chances of success because you have a greater buy-in from the team. Placing a numerical value on risk removes heated discussions about what people "think" should be done.

CONTINUED ON NEXT SLIDE >

RISK ASSESSMENT AND ANALYSIS.

Quantitative assessment.

You will see quantitative assessments in reports with many numbers assigned to various risks. Also, any risk with a monetary value assigned to it will fall into this category.

Single Loss Expectancy (SLE).

A Single Loss Expectancy (SLE) is an amount of money that would be lost due to a single risk factor occurrence. You will see an SLE when your company goes through its risk management process. An SLE enables you to determine potential hazards that may negatively affect specific projects or result from certain decisions.

An SLE is a part of quantitative risk analysis; this is the amount of money you expect to lose each time a specific asset is lost or compromised.

For instance, you may expect to lose $30,000 each time your business server breaks down, or you might lose $1,500 every time a laptop is lost or stolen.

CONTINUED ON NEXT SLIDE >

RISK ASSESSMENT AND ANALYSIS.

Single Loss Expectancy (SLE).

To calculate single loss expectancy, multiply the asset value (AV) and exposure factor (EF). Asset Value (AV) may include more than replacement value; it may also include capital losses due to an asset being down or reputational value lost. EF is the percentage of the value of a given asset that gets lost due to a specific incident.

SLE = AV * EF

RISK ASSESSMENT AND ANALYSIS.

Annualized Rate of Occurrence (ARO).

The Annualized Rate of Occurrence (ARO) is the number of times the same risk factor occurs in a year.

ARO can be considered the likelihood or probability of something happening.

If the ARO is high, you may have a high risk, and some mitigating systems should be prioritized as high. The converse is also true: a low ARO may indicate low risk and a lower priority for implementing a control.

If the ARO is less than 1, it is expressed as a percentage — for instance, if the likelihood of an incident is once every four years, the ARO for that incident would be 0.25 (25%).

RISK ASSESSMENT AND ANALYSIS.

Annual Loss Expectancy (ALE).

The Annual Loss Expectancy (ALE) is the annual amount (generally measured in dollars) lost over a year from a risk factor; you find this by multiplying the ARO by the SLE.

ALE = ARO x SLE

You will see the annual loss expectancy (ALE) when your company goes through its risk management process. The ALE enables you to determine potential hazards that may negatively affect specific projects or result from certain decisions.

CONTINUED ON NEXT SLIDE >

aci LEARNING

RISK ASSESSMENT AND ANALYSIS.

Annual Loss Expectancy (ALE).

The annual loss expectancy (ALE) is part of a quantitative risk analysis. ALE is a calculation that helps you determine the expected monetary loss for an asset due to a particular risk over a single year.

For example, you calculate an ALE of $10,000 and figure it would cost $15,000 a year to eliminate the risk; based on these numbers, you might decide that the cost isn’t worth the risk. ALE determines the cost of the risk; do not confuse ALE with the total cost of ownership (TCO), which assesses the cost of a particular solution.

RISK ASSESSMENT AND ANALYSIS.

Risk control assessments.

Risk Control Self-Assessment (RCSA) is an internal process where stakeholders identify risks and the security controls needed to reduce the risk. RCSA reports are a necessary part of the external audit process.

Risk Control Assessment (RCA) is similar to an RSCA, except an external agency leads the process.

RISK ASSESSMENT AND ANALYSIS.

Risk analysis terms.

- Risk acceptance means that no countermeasures were put in place.
- Inherent risk is the level of risk that exists when no controls are put in place.
- Residual risk is the likelihood and impact of a risk after mitigation, transference, or acceptance measures have been applied.
- Risk tolerance (appetite) is a strategic assessment of what level of residual risk is tolerable.

CONTINUED ON NEXT SLIDE >

RISK ASSESSMENT AND ANALYSIS.

Risk analysis terms.

When the risk scenario is understood in simple terms by the asset owner, they are said to have risk awareness.

Control risk is a measure of how much a security control degrades over time.

RISK ASSESSMENT AND ANALYSIS.

Risk registers.

A risk register is a document showing risk assessment results, which could be through using a heat map or scattergram chart.

Risk registers are also useful to track where you have been versus where you are now to show improvement.

Risk registers appear in executive briefings and IRP planning sessions.

RISK ASSESSMENT AND ANALYSIS.

Knowledge check.

Let's apply what we have covered:

- Describe the differences between a qualitative and quantitative assessment.
- How would you calculate the Annual Loss Expectancy?

End of Module.

For additional practice, please complete all associated self-study activities and labs.