INSTRUCTOR
ALTON

Risk Management 101 for IT Professionals: Essential Concepts

Instructor: Alton Hardin

Section 2: Understanding Risk

Quiz 1: Understanding Risk Section Quiz

Question 1

You’re discussing risk management in a team meeting, and a team member tells you that all risks are bad. Is this true or false?

- True
- **False**

Question 2

A realized risk is an issue.

- **Yes**
- No

Question 3

Your new website is quickly gained popularity, and you’ve noticed that your web server has gone from 20% to 60% of CPU, memory, and network utilization in two weeks. If you don’t upgrade your web server or load balance with a second web server, then your website may drastically slow down or even go offline. Would you consider this a risk or an issue?

- **Risk**
- Issue

Question 4

IT risk management should be a systematic and repeatable process.

- **True**
- False

Question 5

You’re reviewing Microsoft’s Patch Tuesday release notes for their latest patches. You inform your IT manager of a critical patch that hackers are already exploiting across the globe. In this scenario, hackers would be considered ________.

- Assets
- **Threats**
- Vulnerabilities

Question 6

You’re starting a new fast-food restaurant that utilizes a secret recipe passed down through your family. Would this recipe be considered a tangible or intangible asset?

- **Intangible**
- Tangible

Question 7

You hire a desktop support summer intern and ask him to defragment a server's hard drive, but he accidentally formats it instead. What type of threat would this be?

- Natural Hazard
- **Unintentional**
- Intentional

Question 8

One of your network engineers uses Telnet to connect to devices on the network. Telnet sends everything in plaintext across the network, which is a vulnerability. What type of IT vulnerability would this be classified as?

- Operating System
- **Protocol**
- Application

Question 9

You're a frontline manager for the network operations division of your IT department. Your senior management team holds an all-managers meeting and informs you that the department will be going through a major reorganization in the next couple of months. You and other managers voice your concerns regarding potential upcoming risks. What risk category would the reorganization be best classified as?

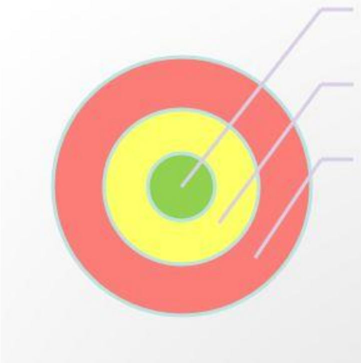
- Budget
- Information Security
- **Organizational**
- Regulatory
- Supply Chain

Section 4: Risk Identification

Quiz 2: Risk Identification Section Quiz

Question 1

Look at the diagram below, which was discussed in this section. The green portion would be the ___________.



- **Risk Appetite**
- Critical Risks
- Risk Tolerance

Question 2

Which of the following would NOT be considered an IT security assessment?

- **Business Impact Analysis**
- IT Audit
- Pen Test

Question 3

A ____________ is a simulated attack on a network and its IT systems.

- **Business Impact Analysis**
- IT Audit
- Pen Test

Question 4

Your IT management team is considering switching helpdesk ticketing software as an opportunity to save costs on annual software licensing fees, and they've asked you to perform and present a SWOT analysis to present at next week's IT operational review. During your SWOT analysis, you identify several potential negative risks associated with the cost savings opportunity. Would the cost savings opportunity be considered the parent or child risk in this scenario?

- Child
- **Parent**

Section 5: Risk Assessments

Quiz 3: Risk Assessments Section Quiz

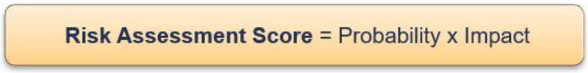
Question 1

Quantitative risk assessments are considered more subjective compared to qualitative risk assessments.

- True
- **False**

Question 2

The below equation is used in ____________ risk assessments.



Risk Assessment Score = Probability x Impact

- **Qualitative**
- Quantitative

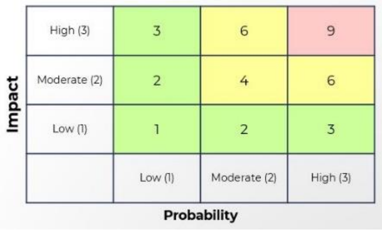
Question 3

You're performing a quantitative risk assessment for your IT department. Working with risk subject matter experts on your team, you've been informed that your Single Loss Expectancy (SLE) is $7,500.00, and the Annual Rate of Occurrence (ARO) is 25%. What would your Annualized Loss Expectancy (ALE) be?

- $750
- **$1,875**
- $4,125
- $5,250

Question 4

The RAID drives in your Network Attached Storage (NAS) device are three years old, and the manufacturer expected lifetime of each drive is five years, so you estimate there's an 80% probability that they will fail next year. If your NAS device goes offline, your business will not be able to access critical business-related files. Performing a qualitative risk assessment, you assign an impact score of three and a probability score of three. What would the overall risk score be considered for this risk?



Impact

High (3)	3	6	9
Moderate (2)	2	4	6
Low (1)	1	2	3
	Low (1)	Moderate (2)	High (3)

Probability

- Low
- Moderate
- **High**

Section 6: Risk Responses and Controls

Quiz 4: Risk Responses and Controls Section Quiz

Question 1

Not building your data center directly on the San Andreas fault in Los Angeles due to earthquake concerns would be considered risk ___________.

- Acceptance
- **Avoidance**
- Mitigation
- Transference

Question 2

Utilizing disk RAID and replicating your data to the cloud to combat hard drive failures would be considered risk ___________.

- Acceptance
- Avoidance
- **Mitigation**
- Transference

Question 3

You own and operate a small IT managed services company and expand to a second office suite in the same business park. To connect the two office's LANs, you decide to utilize your ISP's Internet connection utilizing VPN rather than paying a telecom contractor $20,000 to dig and place a dedicated WAN link under the business park's parking lot. To mitigate against Cybersecurity threats, you implement multi-factor authentication on the VPN. The multi-factor authentication would be considered a _________ security control.

- Management
- Operational
- **Technical**

Question 4

You require your employees to take annual security awareness training, focusing on social engineering and phishing attacks. One week after the annual training, your run a test phishing email campaign to see how many people click on the link in the email. Even with your annual security awareness training, 15% of your employees still click on the phishing email link. This would be considered ____________.

- Risk Transference
- Application Vulnerability
- **Residual Risk**
- Resource Risk

Section 8: Risk Monitoring and Control

Quiz 5: Monitoring and Control Section Quiz

Question 1

Risks and issues should be reviewed and updated on a regular basis until formally closed.

- **True**
- False

Question 2

Publicly traded companies in the United States must ensure they comply with the Sarbanes-Oxley Act (SOX Act), which typically includes IT audits that cover IT security, access controls, data backups, and change management. If your company hires an outside contractor firm, such as Deloitte, to perform a SOX IT audit, that would be considered ____________.

- Ongoing Monitoring
- **Separate Evaluation**

Question 3

Your IT department just recently created a formal risk management process and is currently using a simple risk register spreadsheet to record IT-related risks. You've asked for a cost-effective solution to visualize your department's current risks and asked your risk team to reach out to your Tableau subject matter expert. Which of the choices listed below would be the most appropriate solution:

- **Data Analytics & Visualization Dashboard**
- Balanced Scorecard Software
- Enterprise Risk Management Software

Question 4

While the Risk PMO is charged with designing and implementing an overall risk management process, it's is not supposed to build risk awareness because that is the job of the individual risk owners.

- True
- **False**