Forage(/dashboard) Explore › My Dashboard (/ dashboard) ›

DATACOM

1 Task One

1-2 hours

2 Task Two

Conduct a comprehensive risk assessment

1-2 hours

Finish Line

Achievements

Why this is important ⓘ

Task 2: Cybersecurity risk assessment

1 2 3 4 5

Here is your task

In this task, you will be documenting the client's risk position using the padlock analogy as an example. The client wants you to help them define the context, assess their risk matrix and identify potential risk scenarios.

To complete this task, you will need to:

Back Next

1. Define the context – Identify the assets that need to be protected. This could include sensitive information, customer data, financial information or any other critical assets that are important to the client.

2.Define the risk matrix – Define the likelihood, consequence and risk rating for each potential risk scenario. The likelihood is the probability of the risk scenario occurring, while the consequence is the severity of the potential impact. The risk rating is a measure of the overall risk posed by the scenario, calculated by multiplying the likelihood and consequence.

3. Define three risk scenarios – Identify the specific risks that the client is trying to protect their assets from. For example, a cyberattack, natural disaster or employee negligence.

4. Assess risk rating for each risk scenario – Calculate the inherent risk rating for each scenario, assuming there are no measures in place to reduce the risk (without fence and padlock in place).

5. Assess risk rating for each risk scenario with existing measures – Calculate the current risk rating for each scenario taking existing measures in place to reduce the risk into consideration (with fence and padlock in place).

6. Assess risk levels for each risk scenario with additional measures – Identify any additional measures that could be put in place to further reduce the risk. Calculate the target risk rating for each scenario with these additional measures in place.

7. Create a risk assessment report for the client that summarises the risk assessment findings, the risk mitigation strategy and any recommended measures for implementation.

You will need to use the **"Risk Assessment Template"** provided in the Resources section below to complete this task.

It's important to keep in mind that there is no right or wrong answer. The solution may vary depending on the specific context and scenarios presented. Good luck!

Here are some resources to help you

An example of a risk scenario could be...

A cyberattack aimed at stealing sensitive information. The likelihood of such an attack could be rated as high, given the increasing frequency of cyberattacks. The impact of a

? Back Next

successful cyberattack could be severe, potentially leading to loss of data, financial harm and damage to the client's reputation. The inherent risk rating for this scenario would therefore be high. However, the client may already have existing measures in place to mitigate the risk of a cyberattack, such as firewalls and antivirus software. These measures would reduce the likelihood and impact of the attack, resulting in a lower current risk rating. Finally, the client could also consider additional measures, such as regular software updates and security awareness training for employees, to further reduce the risk and achieve a lower target risk rating.

XLS

Risk Assessment Template

Click to download file →

(https://cdn.theforage.com/vinternships/companyassets/gCW7Xki5Y3vNpBmnn/3gcAGm4XfHPEeiGo3/1683935453166/Risk Assessment Template.xlsx)

Links

- NIST Guide for Conducting Risk Assessments (https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf)
- SO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements (https://www.iso.org/standard/54534.html)
- SANS Institute: Risk Assessment Methodologies (https://www.sans.org/reading-room/whitepapers/auditing/risk-assessment-methodologies-32)
- Guide to Getting Started with a Cybersecurity Risk Assessment (https://www.cisa.gov/sites/default/files/video/22_1201_safecom_guide_to_cybersecurity_risk_assessment_508-r1.pdf)
- The Open Group Risk Management Standard (https://www.opengroup.org/forum/security-forum-0/securityriskmanagement)

?

Cybersecurity Definitions

Back **Next**

Risk assessment: a process of identifying potential risks, analysing their likelihood and potential impact, and implementing measures to mitigate those risks.
Risk position: The level of risk that an organisation faces.
Risk matrix: A tool used to assess and evaluate risks based on the likelihood and consequence of a risk event occurring.
Likelihood: The probability of a risk event occurring.
Consequence: The severity of the potential impact of a risk event.
Risk rating: A measure of the overall risk posed by a scenario, calculated by multiplying the likelihood and consequence.
Inherent risk rating: The risk rating of a scenario without any measures in place to reduce the risk.
Current risk rating: The risk rating of a scenario with existing measures in place to reduce the risk.
Target risk rating: The desired risk rating of a scenario with additional measures put in place to further reduce the risk.
Risk assessment report: A report that summarises the risk assessment findings, the risk mitigation strategy, and any recommended measures for implementation.
Avoid risk: completely eliminate or forego risk.
Treat risk: reduce the likelihood or impact of risk.
Transfer risk: assign or move the risk to a third party.
Accept risk: acknowledge the risk and choose not to resolve, transfer or mitigate.

Upload your risk assessment

Select a File or drag it here.

Back **Next**

Back Next