Task 1

Security maturity assessment

Conducting a security maturity assessment for a new client

Here is the background information on your task

You are a new security analyst in the security advisory team. You have just been assigned to a client, who wants to understand their current maturity level with regards to security. Your team has been discussing different approaches with the client and agreed to conduct a security maturity assessment based on the NIST Cybersecurity Framework.

Here is your task

Assess and score the client's current security maturity levels, using the NIST Cybersecurity Framework's maturity tiers.

Resources to help you with the task

NIST Cybersecurity Framework divides cybersecurity into 5 different functions, those functions are:

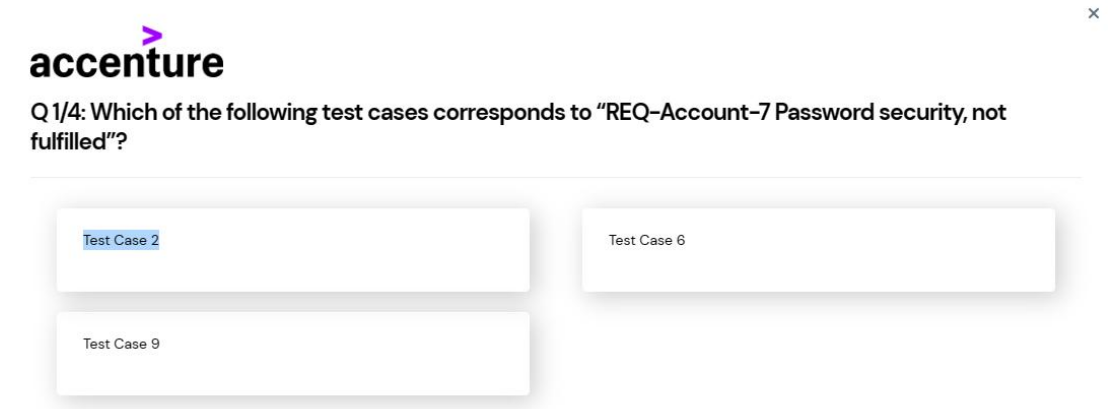
- **Identify**: Identification, inventory, assessment, and governance of enterprise assets and related risks.
- **Protect**: What is important to protect, why protection is necessary, and what protections are prudent.
- **Detect**: Deployment and management of capabilities designed to monitor for potential security incidents.
- **Respond**: Analysis, implementation, and maintenance of methods to address and minimize impacts of security incidents.
- **Recover**: Maintaining or returning the business to normal operations following security incidents.

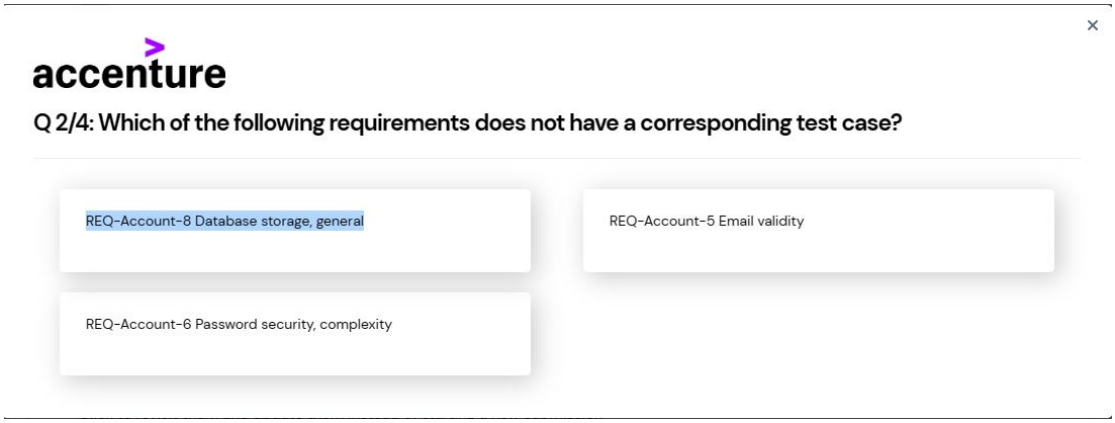
NIST Cybersecurity Framework has five maturity tiers, which can be used for current state scoring: Tier 0: Non-existent, Tier 1: Partial, Tier 2: Risk-Informed, Tier 3: Repeatable and Tier 4: Adaptive.

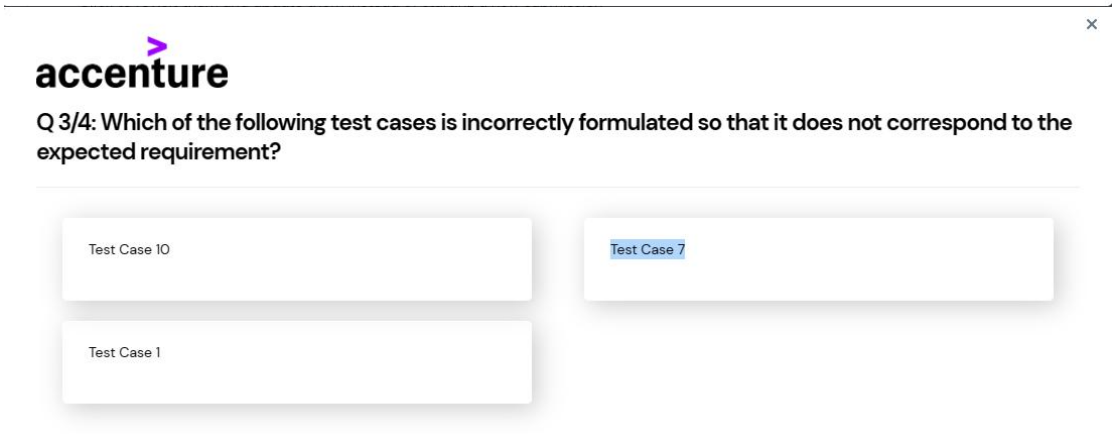
Brief explanation of different tiers:

- **Tier 0**: does not exist
- **Tier 1**: ad-hoc or heavily relying on individual's knowledge
- **Tier 2**: decentralized or there are only informal processes
- **Tier 3**: company-wide, documented processes
- **Tier 4**: innovative technologies in use, proactive review and development

For further information: https://www.nist.gov/cyberframework







accenture

Q 4/4: Which of the following test cases does not adhere to any requirement?

Test Case 3

Test Case 8

Test Case 13

While reviewing the client's documentation you discover that they have extensive documentation for risk management. They have processes in place to identify, prioritize, manage, mitigate, monitor and escalate risks. During the interview, you get it confirmed that the processes are in use and have been working for a couple years. It will also be updated at some point.

- **Tier 0**: does not exist
- **Tier 1**: ad-hoc or heavily relying on individual's knowledge
- **Tier 2**: decentralized or there are only informal processes
- **Tier 3**: company-wide, documented processes
- **Tier 4**: innovative technologies in use, proactive review and development

Client maturity tier is 1

Client maturity tier is 2

Client maturity tier is 3

Client maturity tier is 4

Basics are in place: identities are protected by corporate password policies and the client maintains role-based access controls. However, the organization does not follow a consistently documented approach to provision access rights to personnel. Furthermore, client stakeholders state that they do have an authentication process for privileged accounts and that they at least are auditing accounts who have access to extremely sensitive data, the processes are just not documented There is no process in place to enforce segregation of duties.

- **Tier 0**: does not exist
- **Tier 1**: ad-hoc or heavily relying on individual's knowledge
- **Tier 2**: decentralized or there are only informal processes
- **Tier 3**: company-wide, documented processes
- **Tier 4**: innovative technologies in use, proactive review and development

Client maturity tier is 0

Client maturity tier is 1

During the interview you ask whether the client has any established and documented procedures for a secure system development lifecycle. The client answers that the topic has been part of several discussions and that they are planning on starting a project next year, where they will establish company-wide procedures. But as of now, they don't have anything in place.

- **Tier 0**: does not exist
- **Tier 1**: ad-hoc or heavily relying on individual's knowledge
- **Tier 2**: decentralized or there are only informal processes
- **Tier 3**: company-wide, documented processes
- **Tier 4**: innovative technologies in use, proactive review and development

Client maturity tier is 0

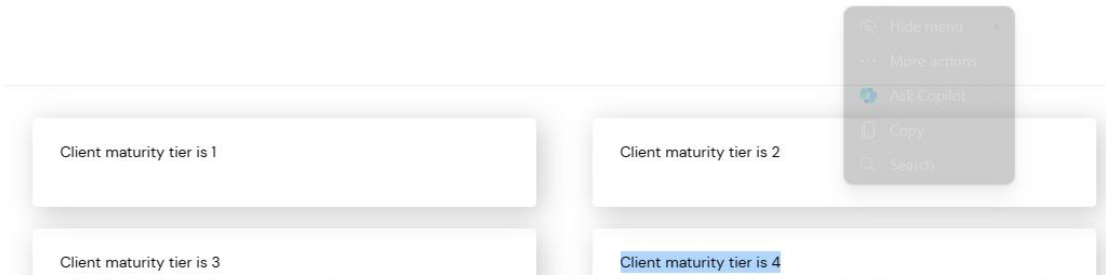
Client maturity tier is 1

Client maturity tier is 2

Client maturity tier is 3

Operations Center (SOC) managed through a security service provider, which monitors the network to detect potential cybersecurity events. Monitoring tools can discover unauthorized systems in the organization or anomalous events indicating a breach. Further automated tools are in use. All the processes are well-defined and documented. There are also metrics in place to check the Security Operations Center effectiveness. Processes are regularly reviewed and improved.

- **Tier 0**: does not exist
- **Tier 1**: ad-hoc or heavily relying on individual's knowledge
- **Tier 2**: decentralized or there are only informal processes
- **Tier 3**: company-wide, documented processes
- **Tier 4**: innovative technologies in use, proactive review and development



seems to be in a good level and relatively extensive. You ask about this during the interview and find out that the documentation is outdated since all the key people know how to act. Client stakeholders also state that the process has been improved to such a degree that it is not following the documented process, but all the relevant people know how to follow the up to date process.

- **Tier 0**: does not exist
- **Tier 1**: ad-hoc or heavily relying on individual's knowledge
- **Tier 2**: decentralized or there are only informal processes
- **Tier 3**: company-wide, documented processes
- **Tier 4**: innovative technologies in use, proactive review and development