Microsoft

Introduction to Microsoft Security, Compliance, and Identity

ASSESSMENT GUIDE

Overview

This document provides assessments for SC-900.

- **Section 1: Learning path questions**
  This provides guidance for assessing student mastery as they progress through the course. This section includes a set of items for each course learning path that you can use to monitor student progress and inform your instruction; the assessment items might include multiple-choice questions and/or open-ended questions.
- **Section 2: Capstone project**
  This provides guidance for using a capstone project to assess students' ability to apply what they've learned throughout the course to a real-world scenario. This project requires students to create and deliver a security strategy presentation that employs Microsoft's security solutions and is based on client requirements. The capstone project includes guidance for students and the instructor.

This guide is intended to be a reference and starting point for instructors as you plan how to assess your students. As you read through the guide, you may choose to tailor the assessment strategies, including the assessment items and rubric, for your classroom.

Table of contents

Section 1: Learning path questions

Introduction

This section includes multiple-choice and open-ended questions that are aligned to the course learning paths for SC-900 Introduction to Microsoft Security, Compliance, and Identity.

You can use the questions as they're presented or modify them as appropriate for your learners. The questions do not appear in any other course materials and are designed to supplement the formative assessment opportunities that are integrated directly into Microsoft Learn and the Microsoft Official Course, such as knowledge checks, "try-it" activities, exercises, walkthroughs, labs, and demos.

Questions are designed to allow for easy integration into an online quiz through Microsoft Forms or via your institution's learning management system (LMS). If you're not familiar with Microsoft Forms, short support videos are available. As a best practice, create new quizzes and delete old ones for each class to keep the response URLs from being circulated and replies continuing to come in after class.

Assigning the learning path questions to students as an independent activity enables you to collect data about individual progress. However, we recommend that you set aside class time to review answers and address any common student misconceptions, as later learning paths/modules depend on knowledge and understanding gained earlier in the course.

Overview of multiple-choice questions

The multiple-choice questions require one or more answer responses and will include plausible distractors. These are set at a level slightly lower than the multiple-choice questions in the Exam SC-900: Microsoft Security, Compliance, and Identity Fundamentals. Note: Although the course name is now called "Introduction to Microsoft Security, Compliance, and Identity," there are no changes to the name of the exam, the exam pages, nor the exam study guide. These will continue to be referenced as SC-900: Microsoft Security, Compliance, and Identity Fundamentals.

Overview of open-ended questions

The open-ended questions present further challenges beyond single answer responses and include scenario-based questions. These questions give students the opportunity to demonstrate critical thinking through their responses.

Learning path: Introduction to security, compliance, and identity concepts

Multiple-choice questions

1. Which of the following are principles of the Zero Trust model?

   Select all that apply.

   a. Verify explicitly (correct answer)

   b. Block access

   c. Least privileged access (correct answer)

   d. Assume breach (correct answer)

2. The shared responsibility model identifies which security tasks are handled by the cloud provider, and which are handled by you, the customer. The responsibilities vary depending on where the workload is hosted. Which approach places more responsibility on the cloud provider?

   Select the correct option.

   a. On-premises datacenter

   b. Infrastructure as a service (IaaS)

   c. Software as a service (SaaS) (correct answer)

   d. Platform as a service (PaaS)

3. Consider the shared responsibility model—in which approach does the customer own the security tasks related with information and data, devices, and accounts and identities?

   Select the correct option.

   a. On-premises datacenter

   b. Infrastructure as a service (IaaS) *and* platform as a service (PaaS)

   c. Software as a service (SaaS)

   d. All the above (correct answer)

4. The HTTPS protocol is an example of which type of encryption?

   Select the correct option.

   a. Encryption in transit

   b. Encryption at rest

c. No encryption

d. Hashing

5. What is the term used to describe the process for verifying the identity of an object, service, or person?

   Select the correct option.

   a. Authorization

   b. Authentication (correct answer)

   c. Auditing

   d. Administration

Open-ended questions

1. A client wants to implement a Zero Trust security strategy that's based on the three key principles: verify explicitly, least privilege access, and assume breach. As they consider their strategy, what elements/pillars should they account for to provide an end-to-end Zero Trust security strategy. What are examples of the types of security considerations they should contemplate for each element/pillar?

   Answer: Should include the six pillars: identities, devices, applications, data, infrastructure, and networks. Refer to the content to see explicit examples for each. This topic will be revisited in subsequent learning paths/modules as you further explore identity, security, and compliance.

2. The shared responsibility identifies which security tasks are handled by the cloud provider, and which ones are dealt with by you, the customer. The responsibilities vary depending on where the workload is hosted. For each approach to hosting (on-premises datacenter, IaaS, PaaS, and SaaS) describe the types of security responsibilities that would be owned by the customer versus those of the cloud provider.

   Answer: The responses should show that, as the customer moves from on-premises to IaaS to PaaS to SaaS, more of the responsibility shifts to the cloud provider. Importantly, the answer should also reflect that, regardless of which hosting is used, the customer always owns information and data, devices, and accounts and identities.

3. Defense in depth uses a layered approach to security, rather than relying on a single perimeter. What are examples of security layers and the security measures that can be taken for each layer described?

   Answer: Should include the layers from the training content: physical security, identity and access, perimeter, network, compute, application, and data. Refer to the training content for some examples of the types of security measures that can be applied to each.

4. The CIA triangle is a way to think about security trade-offs. Identify what each letter stands for and describe what they refer to.

   Answer: Should include the terms confidentiality, integrity, and availability. Refer to the training content for a description of what is referred to by each of these three components.

5. Identity has become the new security perimeter. Describe what is meant by this and the drivers that have led to a shift from a traditional perimeter-based security model to establishing identity as the new security perimeter?

   Answer: Should include a statement that defines an identity and the drivers that have led to this concept. This should include the acceleration in number of people working from home; SaaS applications that are hosted outside of the corporate network; the use of personal devices to access corporate resources; the use of unmanaged devices by partners and customers who may need to access your corporate resources; proliferation of IoT devices—and more.

Learning path: Introduction to Microsoft Entra

Multiple-choice questions

1. An organization allows its employees to use their personal devices to connect to the organization's resources. Given that these are employees personal devices, how are they most likely to be set up in the organization's Microsoft Entra ID implementation?

   Select the correct option.

   a. As Microsoft Entra registered devices (correct answer)

   b. As Microsoft Entra joined devices

   c. As Microsoft Entra hybrid joined devices

   d. They will not be visible to the organization's Microsoft Entra ID implementation.

2. Which of the following verification methods can be used with Microsoft Entra multifactor authentication?

   Select all that apply.

   a. Microsoft Authenticator app (correct answer)

   b. SMS (correct answer)

   c. Voice call (correct answer)

   d. Security questions

3. Self-service password reset (SSPR) works in which of the following scenarios?

   Select all that apply.

   a. Password change (correct, but there is a better answer)

   b. Password reset (correct, but there is a better answer)

   c. Account unlock (correct, but there is a better answer)

   d. All the above (correct answer)

4. Which of the following are signals that can be used by Conditional Access?

   Select all that apply.

   a. Named location information (correct, but there is a better answer)

   b. User risk (correct but there is a better answer)

   c. User or group membership (correct but there is a better answer)

d. All the above (correct answer)

5. How does Privileged Identity Management (PIM) mitigate the risks of excessive, unnecessary, or misused access permissions to Azure resources and Microsoft Entra?

   Select all that apply.

   a. Time-based role activation (correct answer)

   b. Approval-based role activation (correct answer)

   c. Password-based role activation

   d. Risk-based role activation

Open-ended questions

1. Describe the different identity types supported by Microsoft Entra and when you would use them.

   Answer: Should include the following identity types: user, service principal, managed identity, and device. When describing the user identity type, the response should include the different external identities supported by Microsoft Entra (B2B and B2C). The response should reference the point that a service principal is like an identity for an application. For a managed identity, there should be reference to system-assigned and user-assigned and some of the differences. For a device identity type, there should be reference to the multiple options for getting devices into Microsoft Entra.

2. You friends just started a small business and are using a free tier of Microsoft Entra ID. They want to increase security but don't know where to start and are on a very limited budget. They know that you just received your Microsoft Security, Compliance, and Identity Fundamentals certification, so they reach out for some guidance. What would you suggest and why?

   Answer: Should include a statement about security defaults in Microsoft Entra, and some of its features, including enforcing multifactor authentication registration for all users. Additionally, the answer should state that security defaults are available as part of the free tier of Microsoft Entra.

3. Your customer is looking to implement an extra layer of security before allowing authenticated users to access data or other assets. They need the ability to manage and control access to resources based on different conditions/signals. Which Microsoft Entra feature would you recommend—describe how that feature works and its benefits?

   Answer: Should describe Conditional Access in Microsoft Entra and include a statement about how signals are used to make decisions, and the analogy to if/then statements that might be included. The answer should also reference the different types of signals and the decisions that can be made based on those signals. Lastly, the answer should reference the fact that Conditional Access is

implemented through policies that are created in Microsoft Entra. Bonus points could be awarded if they tie the benefits back to Zero Trust methodology.

4. Your customer is facing challenges in managing employee and business partner access to corporate resources, at scale. There have been issues with people having access for much longer than they need it. The customer already has Microsoft Entra P2 premium licensing, so which features of Microsoft Entra would you recommend and why?

   Answer: Should include a statement that references entitlement management and its benefits, including the ability to manage access for internal and external users, and create access packages, and access reviews. Refer to the training content for details.

5. Your customer is looking for a solution to detect and remediate identity-related risks. They already have Microsoft Entra P2 premium licensing, so what solution would you offer and why? Also describe the capabilities the solutions offer.

   Answer: Should include a statement that references Microsoft Entra Identity Protection and describe the tasks: the ability to automate and remediate identity-based risks, investigate risks, and export risk detection data to third-party utilities for analysis. Also describe the types of risks—sign-in and user risk—that can be detected and the type of reports the solution provides. Refer to the training content for more details.

Learning path: Introduction to Microsoft security solutions

Multiple-choice questions

1. An attacker can bring down your website by sending a large volume of network traffic to your servers. Which Azure service can help protect from this kind of attack?

   Select the correct option.

   a. Azure Firewall

   b. Azure DDoS protection (correct answer)

   c. Network security groups (NSGs)

   d. Bastion

2. The features of Microsoft Defender for Cloud cover three broad pillars of cloud security: development security operations (DevSecOps), cloud security posture management (CSPM), and cloud workload protection (CWP). Which features fall under the pillar of CSPM?

   Select all that apply.

   a. Secure Score (correct answer)

   b. Endpoint detection and response (EDR)

   c. Recommendations (correct answer)

   d. Vulnerability scanning for VMs

3. Which Azure security solution provides cloud workload protection plans that can be enabled separately and will run simultaneously to provide a comprehensive defense for compute data and service layers in your environment?

   Select the correct option.

   a. Microsoft Defender for Cloud (correct answer)

   b. Microsoft Sentinel

   c. Azure Security Baselines

   d. Azure Policy

4. Which capability of Microsoft Sentinel can help automate and orchestrate your response to incidents and common security tasks?

   Select the correct option.

a. Workbooks

b. Security playbooks (correct answer)

c. Connectors

d. The MITRE framework

5. Which of the Microsoft Defender XDR services safeguards your organization against malicious threats posed by email messages, links (URLs), and collaboration tools; and provides functionality including safe attachments, safe links, anti-phishing protection, and more?

Select the correct option.

a. Microsoft Defender for Cloud Apps

b. Microsoft Defender for Office 365 (correct answer)

c. Microsoft Defender for Endpoints

d. Microsoft Defender for Identity

Open-ended questions

1. Describe how an enterprise would use Azure Firewall and Azure Network Security groups to protect resources in your virtual networks?

Answer: Should include statements about how NSGs and Azure Firewall each work to protect resources in your virtual network. NSGs allow/deny traffic to/from Azure sources in the virtual network, based on rules. Azure Firewall also protects your Azure virtual network—but the best approach is to use Azure Firewall on a centralized virtual network as it complements NSG functionality. Together they provide better defense in-depth network security. Network security groups provide distributed network layer traffic filtering to limit traffic to resources within virtual networks in each subscription. Azure Firewall is a fully stateful, centralized network firewall as a service, which provides network and application-level protection across different subscriptions and virtual networks. Refer to https://docs.microsoft.com/en-us/azure/firewall/firewall-faq#what-is-the-difference-between-network-security-groups--nsgs--and-azure-firewall.

2. You have a meeting with your customer to talk about Microsoft Defender XDR, an enterprise-wide defense suite, that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks. Describe, as you would to the customer, each of the component solutions, what areas of protection they address, and how they satisfy security needs.

Answer: Should include a statement that mentions the solution areas of Microsoft Defender XDR: Microsoft Defender for Identity, Defender for Endpoint, Defender for Cloud Apps, and Defender for Office 365. Also, as applicable, the response should include reference to Microsoft Defender for

Vulnerability Management and Microsoft Defender for Threat Intelligence. Refer to the training content for details on each. Bonus points could be awarded for those who can tie the benefits back to the Zero Trust methodology.

3. What are the capabilities of the cloud app security framework upon which the Microsoft Defender for Cloud Apps is built?

   Answer: Should include a statement that mentions the following:
   a) Discover and control the use of Shadow IT.
   b) protect your sensitive information anywhere in the cloud.
   c) Protect against cyberthreats and anomalies.
   d) Assess your cloud apps' compliance.

   Provide a brief explanation of each. Refer to the training content.

4. Your organization uses Azure services and Microsoft 365. The IT department needs to understand their current security posture and how to improve it. What solutions can provide this capability? Describe how these solutions can help improve their security posture.

   Answer: Should include a statement about Microsoft Defender for Cloud, how it provides a continuous assessment of the entire estate with recommendations and Secure Score. Because the customer has both Azure services and Microsoft 365, the answer also needs to include reference to Microsoft Secure Score, which is found in the Microsoft Defender portal, and the information that is provided in the improvement actions tab. This is analogous to the recommendations that are provided by Azure continuous assessment in Microsoft Defender for Cloud. The learner should also be able to articulate the difference between Azure Secure Score and Microsoft Secure Score—although they're similar, they measure different things. Secure Score in Microsoft Defender for Cloud is a measure of the security posture of your Azure subscriptions. Secure Score in the Microsoft Defender portal is a measure of the security posture of the organization across your apps, devices, and identities.

5. One of your customers is building a security operations center (SOC). They've heard about Microsoft Sentinel, but they don't know that much about it. They have Microsoft 365, Azure services, and many third-party cloud applications deployed and want to ensure the solution(s) they have in their SOC can integrate with the current enterprise solutions. How would you describe the benefits and value of Microsoft Sentinel to them?

   Answer: Should include some initial context on SIEM and SOAR then lead into discussion on Sentinel. The response should speak to the four areas of functionality in Sentinel—collect, detect, investigate, and respond—and drill down into each one. Answers should also speak to the topics covered in the content, at a high level: connecting your data, workbooks, analytics, incidents, automation and orchestration, playbooks, investigation, hunting, and community. Also, the response should reference the integrated threat protection with Microsoft 365 as an extended detection and response (XDR) system.

Learning path: Introduction to Microsoft Priva and Microsoft Purview

Multiple-choice questions

1. An organization has deployed Microsoft Priva as part of their commitment to user privacy. They plan to implement a Priva solution that can help them limit data overexposure, find and limit data transfers, and minimize stored data. Which Priva solution can help them address these needs?

   Select the correct option.

   a. Priva Privacy Risk Management (correct answer)

   b. Priva Subject Rights Requests

   c. Consent Management

   d. Tracker Scanning

2. What do sensitive information types use to classify data?

   Select all that apply.

   a. Artificial intelligence and machine learning (correct answer)

   b. Patterns defined by a regular expression (regex) or a function (correct answer)

   c. String length

   d. All the above

3. Audit (Premium) supports the long-term retention of audit logs for up to _____ years.

   Select all that apply.

   a. 5 years

   b. 3 years

   c. 10 years (correct answer)

   d. 25 years

4. The compliance administrators in your organization are looking to minimize risk associated with confidentiality violations, intellectual property theft, and regulatory compliance violations. Which Microsoft Purview solution can help address these requirements?

   Select the correct option.

   a. Microsoft Purview Records Management

   b. Microsoft Purview Communications Compliance

c. Microsoft Purview Insider Risk Management (correct answer)

d. Microsoft Purview eDiscovery

5. Your organization uses Microsoft Teams to collaborate on all projects. The compliance admin wants to prevent users from accidentally sharing sensitive information in a Microsoft Teams chat session. What capability can address this requirement?

   Select the correct option.

   a. Use records management capabilities.

   b. Use retention policies.

   c. Use data loss prevention policies. (correct answer)

   d. Apply a sensitivity label to the chat.

Open-ended questions

1. Compliance score measures progress in completing recommended improvement actions within controls. Describe the different actions that are part of compliance score and how they are categorized.

   Answer: Should include a statement that mentions the two types of actions: actions that the organization is expected to manage and actions that Microsoft manages for the organization. Additionally, the response should include the types of categories: mandatory and discretionary, preventive, detective, and corrective.

2. Describe the ways in which sensitivity labels provide information protection.

   Answer: Should include a description of how sensitivity labels can be used to encrypt email and documents, mark the content with watermarks, headers or footers, apply the label automatically or prompt users to apply the label, protect content in containers such as sites and groups—by controlling access to the container—extending sensitivity labels to third-party apps and services, and classifying content that persists with the content.

3. Your organization is looking to implement solutions to mitigate internal risk (insider risk solutions). What are some of the different solutions that can be offered and how they do address insider risk?

   Answer: Should include a statement that mentions one or both of the following, and how they address insider risk:

   - **Insider risk management—helps minimize internal risks by enabling an organization to detect, investigate, and act on risky and malicious activities. Refer to the workflow.**
   - **Communication compliance—helps minimize communication risks by enabling organizations to detect, capture, and take remediation actions for inappropriate messages.**

4. Describe the purpose of eDiscovery?

   Answer: Should include a statement detailing that sometimes a company may become involved in litigation and need to find electronic information to be used as evidence. Electronic discovery or eDiscovery tools can be used to search for content in Exchange Online mailboxes, Microsoft 365 Groups, Microsoft Teams, SharePoint Online and OneDrive for Business sites, Skype for Business conversations, and Yammer teams.

5. Describe how Microsoft Purview Data Catalog helps organizations govern their data and drive greater value creation from their data.

   Enter your answer in the following space.

   Answer: Should include references to the different capabilities of Data Catalog including Governance domains, Data products, Glossary terms, Data Access policies, Health Management, OKRs, and Critical data elements. Bonus points could be awarded if learners are able to put into context of the different data roles, such as data consumer, data owners, data stewards, and the central data office.

Section 2: Capstone project

Overview

This guide features a summative, end-of-course capstone project. In this capstone, each student creates and presents an end-to-end security plan based on client requirements. The student can design the security plan based on the Zero Trust model or the defense in depth model. Students will present this plan to the class for discussion and feedback. The project asks students to demonstrate their knowledge and understanding of course content and apply that to the design and presentation of a scenario-based security, identity, and compliance solution built with Azure and Microsoft 365 services. It's designed for use in diverse contexts and for students of various technical levels.

The Capstone Project Student Guide and the customer scenario in Appendix A can be shared with students as standalone content. It provides an example of a project that instructors can tailor to fit the needs of various learners.

The Capstone Project Educator Guide provides comprehensive information on instructor best practices in the preparation and development of the project.

The Capstone Project Rubric provides evaluation criteria for teachers using the project as a summative assessment. Encourage students to use this document to ensure their work meets the teacher's expectations and reflects what they have learned in the course.

Capstone Project Educator Guide

Overview and objectives

This is intended as the final activity for the SC-900 course. Students' primary objective is to develop an Azure security, identity, and compliance solution that meets the needs of an industry client. They will deliver a presentation that describes their solution and explains how it will address the needs and goals of the industry client. Students will also provide full documentation of the proposed solution, which should either implement the six pillars of the Zero Trust model or the principles of defense in depth. This is an opportunity for students to reflect on what they learned about Microsoft Azure, Microsoft 365, and their security services, as well as the principles that effective security personnel use to ensure security in a modern, heterogeneous IT environment.

Capstone parts

The capstone is split into three parts that offer some flexibility to adapt to student needs and their program of study:

- Part 1: Analysis

  Read the client scenario (see Appendix A) and analyze their current defensive posture against the principles of Zero Trust or defense-in-depth. Analyze the client's current systems against all applicable data protection legislation described in the scenario. List the client's requirements for security, identity, and compliance to satisfy the principles and regulations. As part of the analysis, map the customer's business and regulatory requirements against pillars or layers of the selected model. The analysis should ensure an end-to-end view of the customer's cloud environment and span the areas of security, compliance, and identity.

- Part 2: Solution planning

  Select a set of Azure and Microsoft 365 cloud services that satisfy the requirements you identified in Part 1, from the services that you learned about in the training course. For each service, identify how it satisfies the requirement and make recommendations for high-level configuration details and policies. For example, if you suggest a Conditional Access policy, propose a signal that might trigger it. If you suggest a data storage solution, suggest how you will configure its data encryption.

- Part 3: Presentation

  Present the security, identity, and compliance solution with a discussion on the selected Azure and Microsoft 365 services, their configuration, and how they address the needs identified in the analysis.

Part 1: Analysis

Depending on how you deliver the course, students can use class sessions or independent study time to complete their capstone work. You can also provide remote support sessions for students to ask questions and get feedback related to the capstone.

Review the capstone rubric (see Appendix B) with students so they understand the required tasks for Part 1 as listed below:

- An analysis of threats to the client's proposed cloud infrastructure. The analysis can be organized either under the six security principles of the Zero Trust model or by the layers of a defense in depth approach.
- A list of functional requirements that you must implement to be compliant with the relevant data protection legislation. For example: "The database service must encrypt data at rest."

Part 2 – Solution planning

Review the capstone rubric (see Appendix B) with students so they understand the required tasks for Part 2 as listed below:

- A list of proposed Azure and Microsoft 365 services that address all the requirements identified in Part 1. For each service:
  - Identify the security threat or functional requirement that it addresses.
  - Make high-level recommendations for the configuration of each proposed service.
- Document procedures and policies for:
  - User account life cycle management and access management.
  - Responding to attacks.
  - Responding to regulatory compliance.
- Describe the benefits of your proposals to the client's business decision makers. Sample solutions are provided in Appendix C.

Part 3: Presentation

Students can deliver their presentations in class or remotely. Plan for approximately 10 minutes for the presentation followed by five minutes for questions. Consider the following options and identify the best format for your students:

- **Whole-class presentations:** Students share their presentations with the whole class, taking turns and following time limits—this is only suitable for small class sizes.

- **Small group presentations:** Divide the class into small groups. Allow each student a set amount of time to present to the other students in the group.

Encourage students to discuss and justify the services and procedures they selected to meet the client's needs. They should also discuss how their solution meets the requirements of their chosen model: Zero Trust or defense-in-depth. You may want to ask students to respond to some, or all, of these reflection questions:

- Why did you select the services used in the proposed solution?
- How do the access management, threat response, and compliance and information protection policies and/or procedures in your solution increase security or compliance?
- Does the proposed solution address all six pillars of the Zero Trust model or all seven layers of the defense in depth model?
- Does the proposed solution ensure complete compliance with applicable legislation?
- What benefits might the client expect?
- What was the most challenging part of the project?
- If you had more time, what improvements would you make?

Preparing and supporting students

We recommend introducing the capstone early in the course so students can start thinking about how to apply what they learn to the project. The learning path questions, particularly those with an open-ended format, lend themselves well to preparing your students to think independently about the processes to design a suitable security, identity, and compliance solution for the project, based on Azure and Microsoft 365.

If students have questions, or are facing problems while completing the tasks, direct them to the following problem-solving strategies before asking you for help:

- Review the content in the Student Capstone Guide.
- Review the content in Microsoft Learn.
- Research the official Microsoft Azure and Microsoft 365 documentation.
- Ask peers for help.
- Review their client notes/pre-defined scenario document.

You may consider adding extra sessions as needed for the capstone preparation and presentation delivery. This will give students dedicated collaborative time to work in groups and allow you to informally monitor their progress as they move through the project.

Capstone Project Student Guide

Overview

In this capstone, you'll create a presentation that:

- Summarizes your client's current situation, needs, and goals.
- Describes the services and tools you'd recommend for your client.
- Documents the expected costs.
- Outlines a security, identity, and compliance solution.
- States the benefits for your client.

This is an opportunity for you to reflect on what you learned about Microsoft Azure and Microsoft 365 security services in this course.

Preparing for the capstone

To best prepare for the capstone, consider the following:

- **Start preparing early**. Read this capstone guide and the client scenario (Appendix A) early in the course.
- **Familiarize yourself with the client presented in the scenario and make your own notes**. Take and keep thorough notes about your client. It's better to get too much information than not enough.
- **Think about the scenario in each learning path/module**. As you learn new concepts, consider how they might apply to the client.
- **Work on the presentation early and complete the learning path questions**. Consider building your presentation throughout the course. The learning path questions are designed to help support your understanding of the capstone tasks, so think about your project as you complete them.

Capstone tasks

Task 1: Analysis

In the first phase of this project, you will analyze your client's proposed move to a cloud-based system for app infrastructure hosting and the development environment. You'll choose to do your analysis either against the Zero Trust model or against the defense-in-depth model. By the end of this task, you should be able to describe the issues that must be addressed before the proposed cloud systems satisfy your chosen model. You should also understand the functional requirements your systems must implement to comply with relevant legislation. You'll be using this information to create a presentation in Task 3, so be sure you have the following documented:

- An analysis of threats to the client's proposed cloud infrastructure. The analysis can be organized under the six security principles of the Zero Trust model or by the layers of a defense in depth approach.
- A list of functional requirements you must implement to comply with the relevant data protection legislation described in the scenario (Appendix A).

Task 2: Solution planning

Use the lists of threats and functional requirements identified in Task 1, and your knowledge of Azure and Microsoft 365, to propose a solution for your clients. Be sure to include the following in your proposal:

- A list of proposed Azure and Microsoft 365 services that address the requirements identified in Task 1. For each service:
  - Identify the security threat or functional requirement it addresses.
  - Make high-level recommendations for its configuration.
- Document procedures and policies for:
  - User account life cycle management and access management.
  - Responding to attacks.
  - Responding to regulatory requirements.
- Describe the benefits of your proposal to the client's business decision makers.

Task 3: Presentation

In this phase, you will deliver a 10-minute presentation that describes the needs analysis, recommendations, and explanations that you documented in Tasks 1 and 2. After the presentation, others will have an opportunity to ask questions about your process and recommendations. Make sure you include evidence to support the decisions you made based on the information in the scenario, and that your presentation is organized and detailed enough for the audience to have a good understanding of the benefits of your recommendations.

Support and resources

If you have questions or face problems while completing the tasks, use these problem-solving strategies before asking your instructor for help:

- Review the content in this Student Capstone Guide.
- Research the official Microsoft Azure and Microsoft 365 documentation.
- Ask peers for help.
- Review your client notes and the scenario document.

Post-project reflection questions

1. What did you learn from creating and delivering this capstone presentation that might be helpful to you in the future?
2. What challenges did you experience? How did you overcome them?
3. What components of your presentation went well? What are some things you could improve?
4. Add other comments you would like to make about this project or your work.

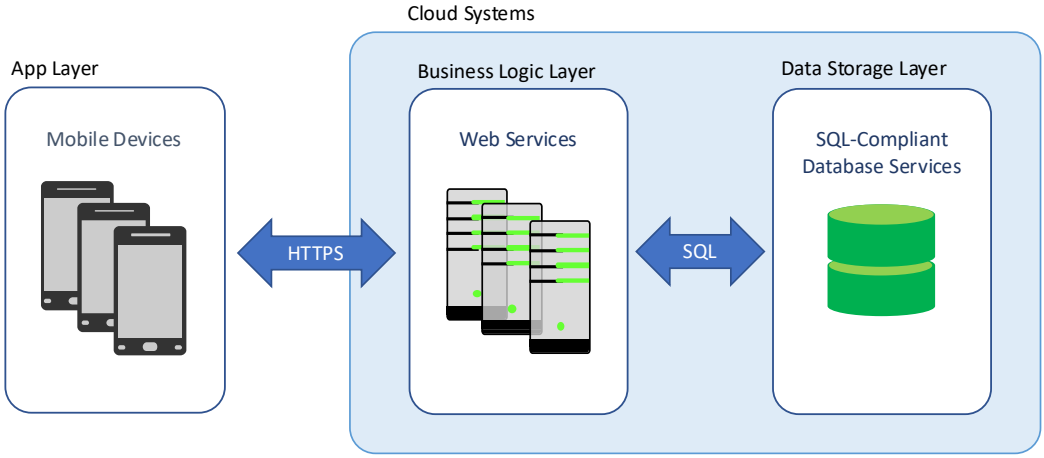
Appendix A: Client scenario

The following paragraphs outline a business scenario in which a start-up company needs to improve on its current security posture and regulatory compliance. You're free to modify the scenario or develop one of your own:

The client company has developed a new physical training app for mobile phones, tablets, and wearable devices. The app helps users develop a personalized regime that includes general strength and cardiovascular training and activities such as running, cycling, and swimming, targeted to the user's personal goals. Once the regime is designed, the app shows users their progress toward their goals as they complete their daily training tasks. Users can log into the app by using their Google or Facebook accounts, or by creating a new account specific to the training app.

The application consists of three layers:

- **App Layer**—the app that users install on their mobile device. This app is used to configure the training regime, record training session results, display progress, and communicate with other users. Users interact with their data entirely through this app. Users must be securely authenticated and communications with the business logic layer must be encrypted.
- **Business Logic Layer**—the business logic for the application consists of a set of web services that the app calls to read and write training data.
- **Data Storage Layer**—all the data for the app and its functions are stored in SQL-compliant databases, including personal goals, training data, and training app authentication credentials.



During the development, alpha, and beta phases, the business logic and data storage layers were hosted on-premises on servers with enough capacity to satisfy the demands of a small number of beta users. As the client approaches the launch date for version one—which includes publishing the app in major app stores and a marketing campaign—they want to deploy the completed business logic and data storage layers to a cloud-hosted system to ensure they can respond rapidly to the high user demand they expect.

After the app launch, the next priority is to move the development environment to the cloud to support a team of developers who bring their own devices for coding and testing the three layers of the application. The team

includes the client's employees and others from partner organizations that provide coding and testing services. These devices include Windows, Linux, and Apple laptops for writing code and iOS and Android devices for user testing the app layer. When the development environment moves to the cloud, the client will close down their on-premises servers.

Due to recent cybersecurity threats and attacks reported in the news and those that impacted their competitors, the client company wants to implement more secure identity and access management policies to mitigate against potential breaches. They feel at risk because employees and partners access resources from remote locations, using their own devices, and partners are often involved for a short time.

They hired a small team of security professionals to be more proactive and efficient in their threat monitoring and response. The security team wants to segment the cloud solution strictly and grant the minimum level of access to app users, employees, and partners. They need to be notified immediately if the systems come under attack.

In the client's operational jurisdiction, government legislation imposes the following requirements:

- All users' personal data must be protected against disclosure to third parties. When stored and transmitted, data must be encrypted.
- All users must be informed about how you use their personal data and give consent.
- All users can request all the personal data that you hold about them.
- If there is any breach of data protection regulations, you must inform the regulator within 48 hours.
- If the regulator opens an investigation into your data usage, you must be able to respond with all relevant files and communications within 48 hours of their request.
- You must keep relevant communications for at least five years.

Now that you understand the client's environment and some of the challenges that they're facing, design a security and compliance plan for the company's new cloud systems, based either on the principles of Zero Trust or on the principles of defense in depth. You must protect both the deployed cloud app and also the development environment. If you choose Zero Trust, the design must consider the six elements that are foundational pillars of the Zero Trust model. If you choose defense in depth, the design must look at how to secure the seven security layers in that model. What Azure and Microsoft 365 services are included in your solution and why?

Appendix B: Capstone rubric

Table 1: Capstone rubric - Task 1

Item	Approaches standard	Meets standard	Exceeds standard (includes items in meets standard)	Summarize where and how you included this item
Analysis of threats to the client's proposed cloud infrastructure	Description of the threats is not clear or is not categorized according to the Zero Trust or defence-in-depth models.	Description of the threats is clear. Threats are listed in the appropriate Zero Trust or defence-in-depth categories.	Description of threats demonstrates a clear understanding of common security problems and a deep comprehension of the selected model.	
List of functional requirements you must implement to be compliant with the relevant data protection legislation	Not all legislative requirements are covered by the listed functional requirements.	All legislative requirements are met by the listed functional requirements.	All legislative requirements are met and the student demonstrates an understanding of the importance of data protection legislation.	

Table 2: Capstone rubric - Task 2

Item	Approaches standard	Meets standard	Exceeds standard (includes items in meets standard)	Summarize where and how you included this item
List of proposed Azure and Microsoft 365 services that address all the requirements identified in Task 1.	List does not address all the requirements in Task 1 or includes services that are not relevant.	List addresses all the requirements in Task 1 and includes relevant recommendations for configuration.	List addresses all the requirements in Task 1 and demonstrates a good understanding of how each service addresses security needs.	
Documentation of procedures and policies	Procedures and policies listed do not address access management fully or don't enable rapid responses to attacks or complete responses to regulatory requirements.	Procedures and policies listed fully address access management and permit rapid and complete responses to attacks and regulatory requirements.	Procedure and policies implement a thorough and secure approach to access management, attack response, and regulatory compliance.	
Describe the benefits of your proposals to the client's business decision makers	Description is incomplete or does not fully address the client's needs.	Description is complete and fully addresses the client's needs. A single end-to-end solution is described.	Description is complete, fully addresses the client's needs, and makes a clear case to implement the solution to non-technical decision makers.	

Table 3: Captone rubric - Task 3

Item	Approaches standard	Meets standard	Exceeds standard (includes items in meets standard)	Summarize where and how you included this item
Presentation aids	Not all materials are organized or easy to understand. Not all visual and/or audio elements help audience understanding, and some might distract.	Materials are organized and clear. Visual or audio elements help audience understanding.	Materials are interesting, easy to understand, and include at least one way to gather audience responses beyond just asking if there are any questions.	
Delivery of presentation	Presenter isn't prepared or doesn't engage with the audience.	Presenter is prepared and engaged with the presentation and the audience. Communication of ideas is mostly clear and effective.	Presenter communicates beyond just reading the words on the presentation materials. Communication of ideas is consistently clear and effective.	

Appendix C: Capstone example solutions

The students can choose to complete the capstone project either according to the Zero Trust model or the defense in depth model. This document presents parts 1 and 2 of an example solution for each of those models. The example solutions are not assumed to include all the available solutions covered in the training content. Part 3 of the capstone project is a presentation.

Zero Trust example solution

In the Zero Trust methodology, you assume everything is an open network with potential threats and attackers anywhere. You must trust no one and verify everything.

The Zero Trust guiding principles are:

- Verify explicitly.
- Least privilege access.
- Assume breach.

Part 1: Analysis

The following sections list threats and functional requirements to mitigate them, classified under the six pillars of Zero Trust.

Foundational Pillar—Identities

Threats:

- Users of the app send credentials for authentication across the internet. These must be protected from interception.
- Identities of employees or partners may be compromised and used to gain access to source code.

Functional requirements:

- Federated authentication must be implemented to allow users to authenticate with their Facebook or Google accounts.
- Policies that secure identities and manage access to resources for development.
- Policies that ensure least privilege access for employees and partners.

Foundational Pillar—Devices

Threats:

- Employees and partners may use their own devices to access development and testing environments. They might copy code to unsecured devices.

Functional requirements:

- Detailed control over who can access the development and testing environments, and when.

Foundational Pillar—Applications

Threats:

- Employees and partners might use devices with unsecure apps installed on them. These apps may be able to compromise source code.

Functional requirements:

- The ability to diagnose Shadow IT apps installed on developers' and partners' devices.

Foundational Pillar—Data

Threats:

- Data stored in the production data layer databases is at risk of theft and tampering by personnel who have access.
- Business data is at risk of theft and tampering by internal personnel and partner users. This includes the application source code.

Functional requirements:

- All app users' training data is personal and must be protected against disclosure to third parties.
- Data stored in the data layer must be encrypted.
- Access to source code must be limited to those who need it and removed from users who have finished their work on the project.
- Data layer servers must be monitored for vulnerabilities.
- Attacks against the application data layer should be detected automatically.
- Ability to enforce data retention policies to conform to data protection legislation.
- Ability to locate and manage all communications that relate to a data protection breach to conform to data protection legislation.

Foundational Pillar—Infrastructure

Threats:

- Malicious attacks from internet users.
- Malicious attacks from internal users.

Functional requirements:

- Monitoring for malicious attacks on both the deployed application and the development and testing environment.
- Monitoring for attacks against servers hosting the business logic layer.
- Monitoring for vulnerabilities in the business logic layer.

Foundational Pillar—Networks

Threats:

- Connections between the mobile app and the business layer include personal information and are at risk of interception and tampering.
- Anyone who gains access to the business layer or data layer compute resources may be able to intercept data.

Functional requirements:

- Data exchanged between the mobile app and the business layer must be encrypted on the wire.
- Separate the business logic layer compute resources from the internet and filter communications.
- Segment the business logic layer from the data layer and filter communications.

Part 2: Solution planning

The following sections list Microsoft Azure and Microsoft 365 services that can be used to implement the functional requirements identified in Part 1.

Foundational Pillar—Identities

- Secure communication between the app and the business logic layer by implementing network encryption.
- Microsoft Entra supports federated authentication from Facebook, Google, and other providers.
- Password policies in Microsoft Entra should require multifactor authentication (MFA) for employees and partners.

Foundational Pillar—Devices

- Use Microsoft Entra Conditional Access policies to control who can access source code, when they can access it, and where they can access it from.
- Use Microsoft Sentinel to detect attacks on development team devices.

Foundational Pillar—Applications

- Use Microsoft Defender for Cloud Apps to diagnose shadow IT on developers' and partners' devices.

Foundational Pillar—Data

- If data is stored in Azure SQL Database or SQL Server on a virtual machine, use TDE to encrypt personal data at rest.
- If data is stored in Cosmos DB, the encryption at rest is implemented by default.
- Use Microsoft Defender for SQL in Microsoft Defender for Cloud to identify and mitigate security vulnerabilities.
- Use Microsoft Defender for SQL advanced threat protection to check for database attacks.

Foundational Pillar—Infrastructure

- Azure DDoS Protection to detect attacks.
- Microsoft Sentinel to detect and respond to attacks.
- Microsoft Defender for Cloud to detect and respond to attacks.
- Microsoft Defender for Cloud to monitor for vulnerabilities in the business logic layer.

Foundational Pillar—Networks

- Require encryption of user data between app and business layer.
- Use Azure Key vault to manage the required certificates.
- Use Azure network security groups to segment the business logic layer from the data layer.

Solution summary

The Zero Trust model enables architects to analyze any security solution against six pillars and its three principles. However, the finished solution must be a single integrated system, albeit with multiple components, not six separate systems.

The proposed solution is as follows:

- Microsoft Entra
    - Stores users accounts for app users, employees, and partners.
    - Federates with Facebook and Google for authenticating app users.
    - Enforces password policies and MFA requirements.
    - Enforces Conditional Access policies to protect source code.
- Microsoft Defender for Cloud:
    - Identifies vulnerabilities and monitors for attacks against the database servers and business logic layer servers.
    - Diagnoses shadow IT on developers' and partners' devices.
- Microsoft DDoS protects servers against denial-of-service attacks.
- Azure Key Vault manages and protects encryption keys.
- Azure network security groups segment the network.
- Microsoft Sentinel will be the primary user interface for the end-to-end security system:
    - Attack detection for the development team's computers and devices.
    - Centralized monitoring of vulnerabilities, including those identified by Microsoft Defender for Cloud.
    - Security incident management.
    - Management of security procedures as playbooks.
    - Deep incident investigation and hunting.

Defense in depth example solution

In the defense in depth methodology, you define security measures at each of seven different layers. If any of those layers are compromised, attackers must penetrate multiple other layers to be successful.

Part 1: Analysis

The following sections list threats and functional requirements to mitigate them, classified under the seven layers of the defense in depth model.

Layer—Physical

Threats:

- Datacenter personnel have physical access to servers that host the business logic layer and the data layer.
- Employees and partner users may not secure their computers and devices properly when accessing development and testing environments.

Functional requirements:

- Physical access to host servers should not enable personnel to steal data or source code.

Layer—Identity and access

Threats:

- App users send credentials for authentication across the internet. These must be protected from interception.
- Identities of employees or partners may be compromised and used to gain access to source code.

Functional requirements:

- Federated authentication must be implemented to allow users to authenticate with their Facebook or Google accounts.
- Policies that secure identities and manage access to resources for development.
- Policies that ensure least privilege access for employees and partners.

Layer—Perimeter

Threats:

- Distributed denial of service (DDoS) attacks from internet users.
- Other malicious attacks from internet users.

Functional requirements:

- Monitoring for DDoS attacks on both the deployed application and the development and testing environment.
- Monitoring for attacks against servers hosting the business logic layer.

Layer—Network

Threat:

- Connections between the mobile app and the business layer include personal information and are at risk of interception and tampering.
- Anyone who gains access to the business layer or data layer compute resources may be able to intercept data.

Functional requirements:

- Data exchanged between the mobile app and the business layer must be encrypted on the wire.
- Separate the business logic layer compute resources from the internet and filter communications.
- Segment the business logic layer from the data layer and filter communications.

Layer—Compute

Threats:

- Employees and partners may use their own devices to access development and testing environments. They may copy code to unsecured devices.

Functional requirements:

- Detailed control over who can access the development and testing environments and when.

Layer—Application

Threats:

- Employees and partners may use devices with unsecured apps installed on them. These apps may be able to compromise source code.

Functional requirements:

- The ability to diagnose Shadow IT apps installed on developers' and partners' devices.

Layer—Data

Threats:

- Data stored in the production data layer databases is at risk of theft and tampering by personnel with database access.
- Business data is at risk of theft and tampering by internal personnel and partner users. This includes the application source code.

Functional requirements:

- All app users' training data is personal and must be protected against disclosure to third parties.
- Data stored in the data layer must be encrypted.
- Access to source code must be limited to those who need it and removed from users who have finished their work on the project.
- Data layer servers must be monitored for vulnerabilities.
- Attacks against the application data layer should be detected automatically.
- Ability to enforce data retention policies to conform to data protection legislation.
- Ability to locate and manage all communications that relate to a data protection breach to conform to data protection legislation.

Part 2: Solution planning

Layer—Physical

- Access to Azure datacenters controlled and secured by Microsoft.
- Train employees to control physical access to devices carefully—lock devices away, lock screens when not present.
- Define policies to lock devices when not used.

Layer—Identity and access

- Microsoft Entra supports federated authentication from Facebook, Google, and other providers.

- Password policies in Microsoft Entra should require multifactor authentication (MFA) for employees and partners.

Layer—Perimeter

- Azure DDoS Protection to detect attacks.
- Firewall in front of business logic layer.
- Firewall between business logic and data layer.

Layer—Network

- Secure communication between the app and the business logic layer by implementing network encryption.
- Use Azure Key vault to manage the required certificates.
- Use Azure network security groups to segment the business logic layer from the data layer.

Layer—Compute

- Use Microsoft Entra Conditional Access policies to control who can access source code, when they can access, and where they can access from.
- Use Microsoft Sentinel to detect attacks on development team devices.
- Microsoft Defender for Cloud to detect and respond to attacks.
- Microsoft Defender for Cloud to monitor for vulnerabilities in the business logic layer.

Layer—Application

- Use Microsoft Defender for Cloud Apps to diagnose shadow IT on developers' and partners' devices.

Layer—Data

- If data is stored in Azure SQL Database or SQL Server on a virtual machine, use TDE to encrypt personal data at rest.
- If data is stored in Cosmos DB, the encryption at rest is implemented by default.
- Use Microsoft Defender for SQL in Microsoft Defender for Cloud to identify and mitigate security vulnerabilities.
- Use Microsoft Defender for SQL advanced threat protection to check for database attacks.

Solution summary

The defense in depth model enables architects to analyze any security solution against seven layers. Attackers must penetrate multiple layers to mount a successful attack. However, the finished solution must be a single integrated system, albeit with multiple components, not seven separate systems.

The proposed solution is as follows:

- Microsoft Entra
    - Stores users' accounts for app users, employees, and partners.
    - Federates with Facebook and Google for authenticating app users.
    - Enforces password policies and MFA requirements.
    - Enforces Conditional Access policies to protect source code.

- Microsoft Defender for Cloud:
    - Identifies vulnerabilities and monitors for attacks against the database servers, and business logic layer servers.
    - Diagnoses shadow IT on developers' and partners' devices.
- Microsoft DDoS protects servers against denial-of-service attacks.
- Azure Key Vault manages and protects encryption keys.
- Azure network security groups segment the network.
- Microsoft Sentinel will be the primary user interface for the end-to-end security system:
    - Attack detection for the development team's computers and devices.
    - Centralized monitoring of vulnerabilities, including those identified by Microsoft Defender for Cloud.
    - Security incident management.
    - Management of security procedures as playbooks.
    - Deep incident investigation and hunting.