

**Cyber Shujaa**

**Cloud Security Specialist**

## **Assignment 1: SC-900 Learning Path**

**NAME: WELDON KIPKIRUI KENEI**

**CS NO: ADC-CSS02-25027**

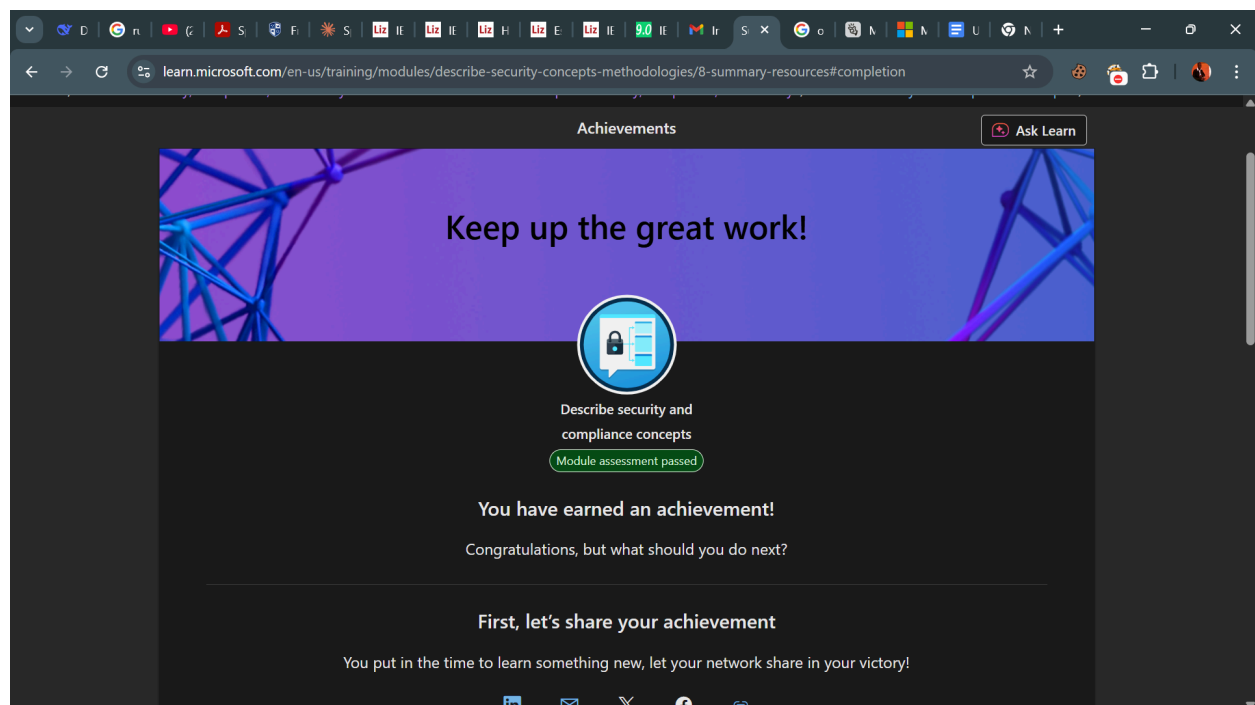
# Introduction

In this assignment, we will go through the fundamental modules required for cloud security specialist certification. These modules are highlighted in summary with screenshots of passed assessments and achievement badges.

## Describe security and compliance concepts.

In this module, we were introduced to some important security and compliance concepts. We learned about the shared responsibility model and how the workload responsibilities vary depending on where the workload is hosted. We also learned how an in-depth defense strategy uses a series of mechanisms to slow the advance of an attack. In addition, we learned about the guiding principles of Zero Trust and how the six foundational pillars work together to enforce organization security policies. Lastly, we were introduced to encryption and hashing as ways to secure your data and some basic concepts related to data compliance.

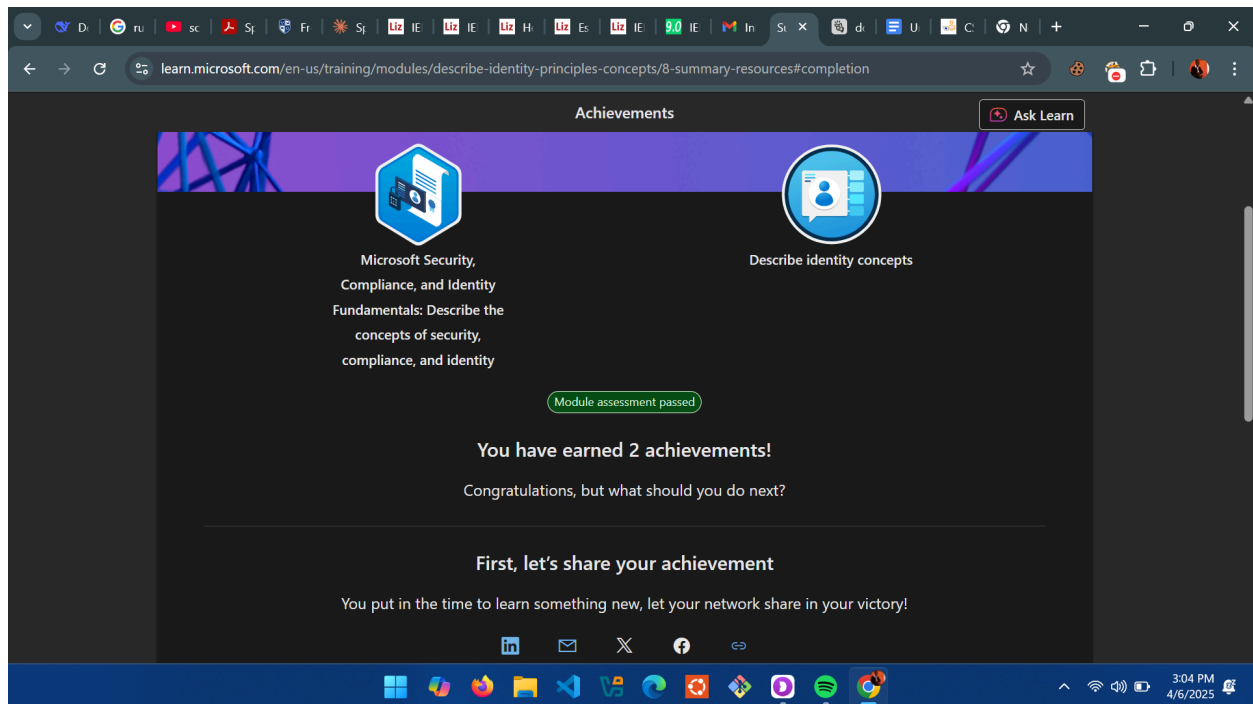
<https://learn.microsoft.com/api/achievements/share/en-us/weldonkeni-6817/QS4YH9HE?shareId=1C66F93EC0530812>



# Describe identity concept

In this module, we learned about authentication and authorization, identity as the new security perimeter, and the role of Active Directory. We also looked at the concept of federation to access resources that belong to another organization.

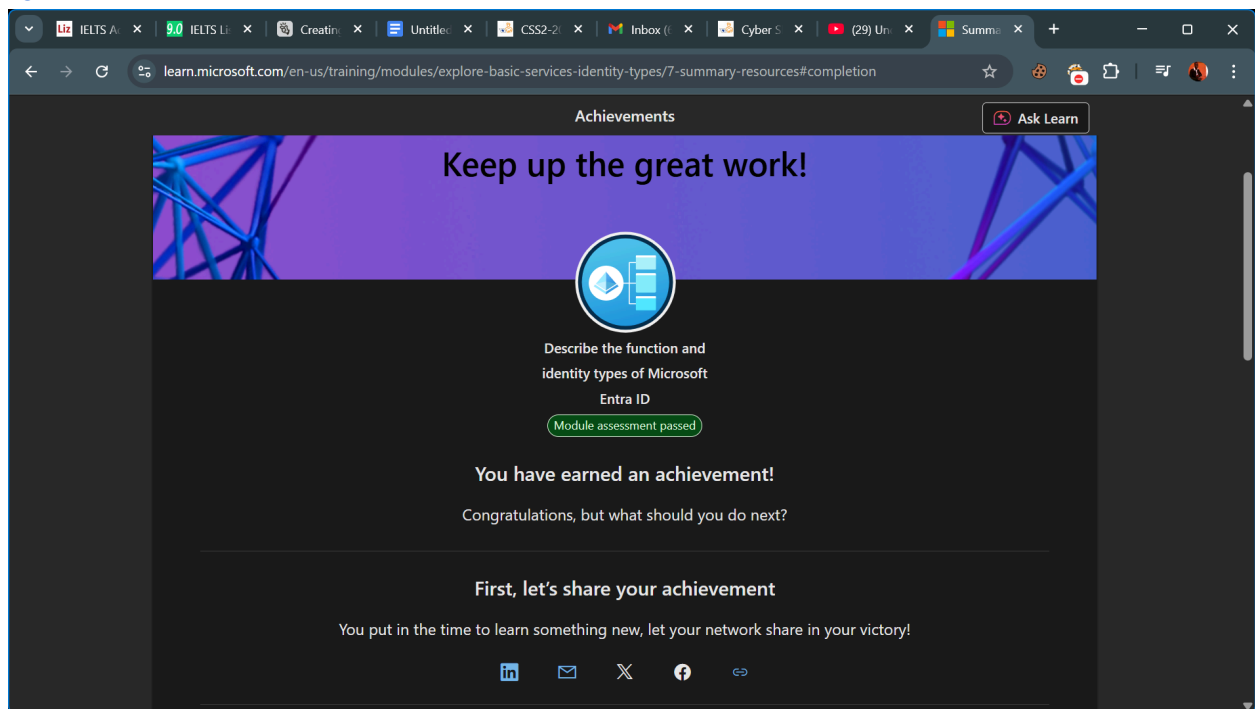
<https://learn.microsoft.com/api/achievements/share/en-us/weldonkenei-6817/QS4AD8KE?sharingId=1C66F93EC0530812>



# Describe the function and identity types of Microsoft Entra ID

In this module, we gained an insight into the core functionality of Microsoft Entra ID and the identity types supported. We also learned about a hybrid identity model, where all user identities are managed in your on-premises Active Directory Domain Services (AD DS) directory, and changes are synchronized to your Microsoft Entra ID.

<https://learn.microsoft.com/api/achievements/share/en-us/weldonkenei-6817/URWHFA63?sharengId=1C66F93EC0530812>

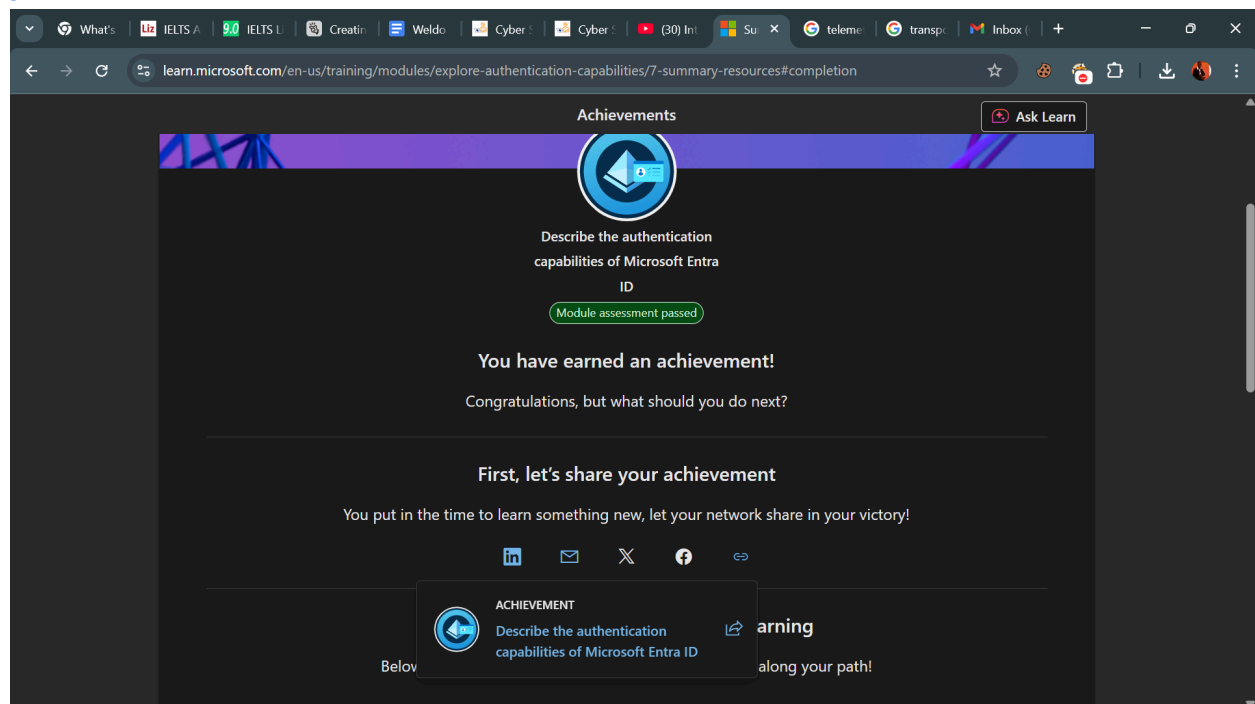


# Describe the authentication capabilities of Microsoft Entra ID

In this module, we've seen why passwords are a problematic form of authentication. We've learned about the different types of authentication that can be used with Microsoft Entra ID, including passwordless authentication with Windows Hello for Business and the Microsoft Authenticator app. We've also learned about multifactor authentication.

We've learned about the benefits of allowing users to reset their passwords with self-service password reset and how Microsoft Entra Password Protection mitigates against the inherent risks associated with passwords.

<https://learn.microsoft.com/api/achievements/share/en-us/weldonkeni-6817/E5BJK9WP?sharingId=1C66F93EC0530812>



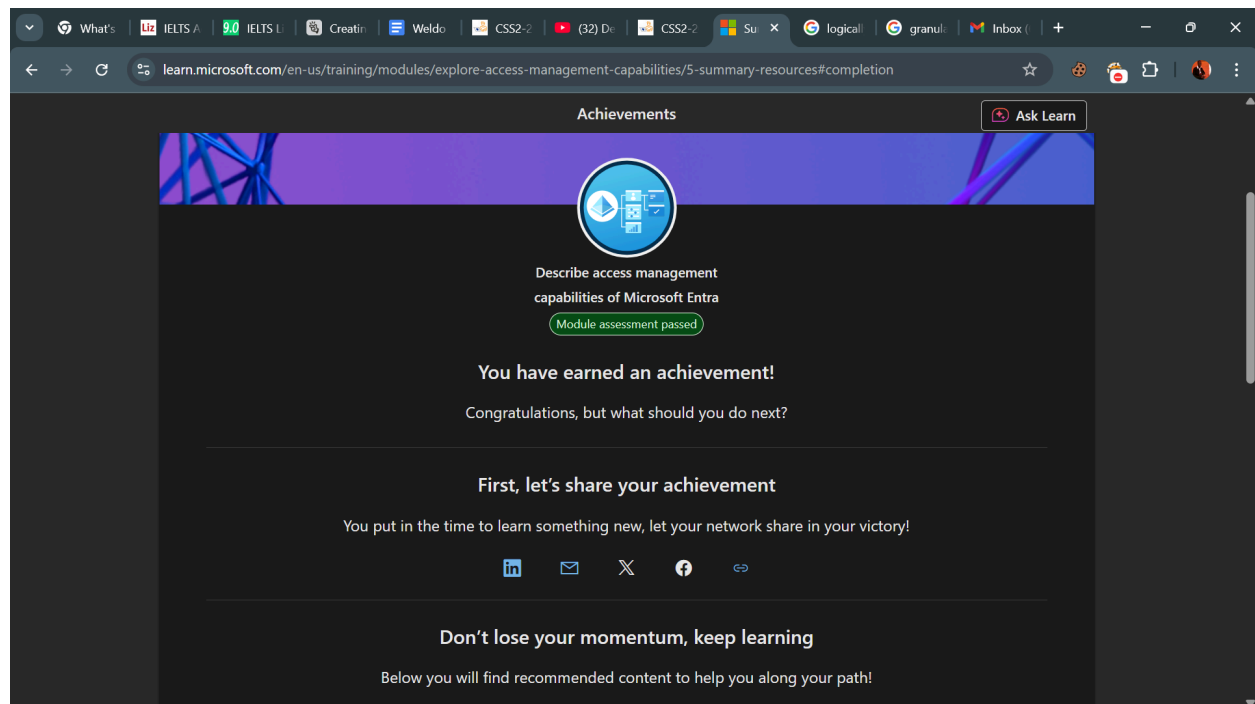
# Describe the access management capabilities of Microsoft Entra ID

In this module, we learned about Conditional Access and how it brings signals together to make decisions and enforce organizational policies.

We learned about Global Secure Access, Microsoft's Security Service Edge solution that combines the identity controls you have with Conditional Access together with network controls to provide advanced protection for your internet-based resources and your private corporate resources.

We also learned about built-in and custom roles in Microsoft Entra ID that provide role-based access control.

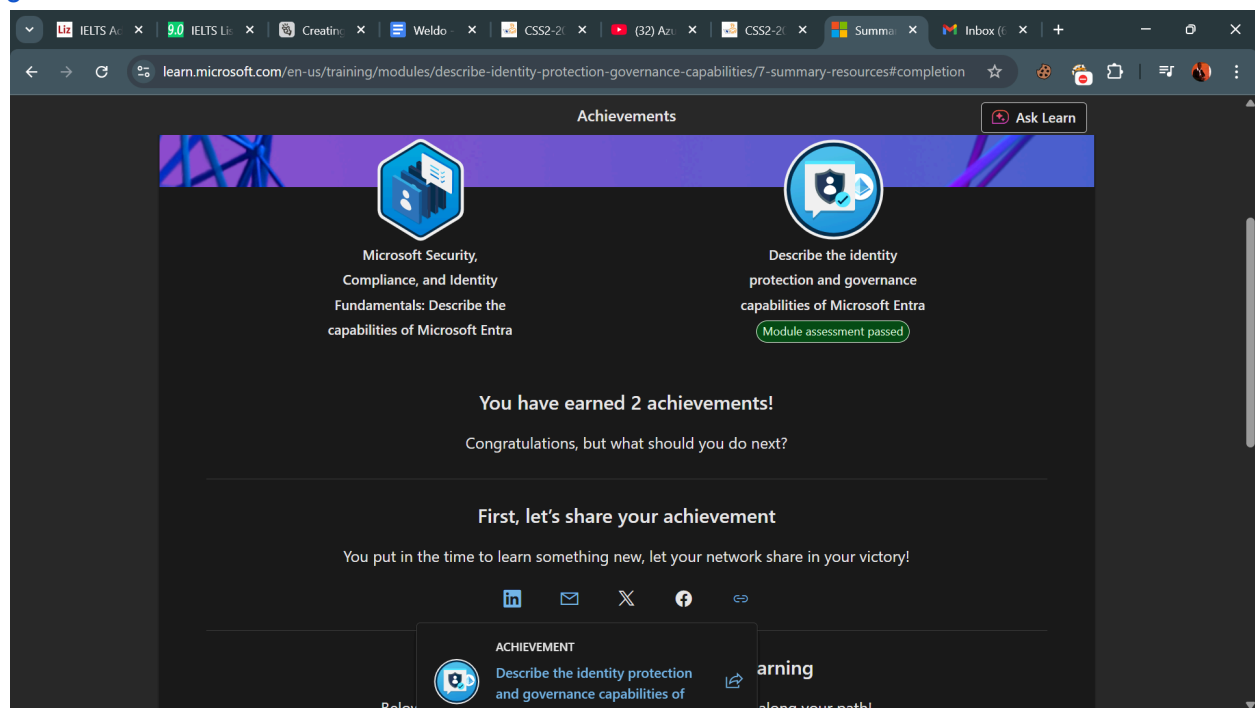
<https://learn.microsoft.com/api/achievements/share/en-us/weldonkeni-6817/E5BTFHDP?sharingId=1C66F93EC0530812>



# Describe the identity protection and governance capabilities of Microsoft Entra

In this module, we learned how Microsoft Entra ID provides tools to help us protect and govern identities. We also learned about identity life-cycle management and how Identity Protection can detect potential identity risks. Finally, we learned how solutions such as access reviews and privileged identity management help organizations adhere to the concept of least privilege access, a core principle of a Zero-Trust security strategy.

<https://learn.microsoft.com/api/achievements/share/en-us/weldonkenei-6817/ZBQBUL42?sharingId=1C66F93EC0530812>



## Conclusion

The modules that we have covered in this assignment have been a foundational work through which we have been introduced to concepts ranging from identity as a plane in security these days to the granular components of Microsoft Entra ID that would be vital in achieving organizational security, especially in the cloud.