# *IT Security (420-F30-HR)*

# *Lab 09a – IAAA, RBAC*

Date assigned: Friday, March 28

Date Due: Tuesday , April 1, 1pm (before class)

**Objectives:**

Learn:

1. IAAA concepts
2. RBAC concepts as applied to Azure

# IAAA - Individual

## Explain in your own words, the IAAA model describing what each letter stands for.

Identification: This is where a user claims an identity, typically by providing a username or ID number.

Authentication: This step verifies that the user is who they claim to be, often using passwords, biometrics, or multi-factor authentication.

Authorization: After being authenticated, the system determines what resources or actions the user is allowed to access.

Accountability: Ensures that all user actions are logged and traceable, so activity can be audited, and users held responsible for their actions.

## Provide a URL the describes the IAAA model:

<https://dustybugger.com/what-is-the-iaaa-framework/>

## Explain the terms “identity federation” and SSO. What are the benefits and differences between the two. Provide your sources:

Identity Federation allows users to access multiple systems or services using a single identity, even if the systems are owned by different organizations. It creates trust relationships between identity providers and service providers using standards like SAML or OpenID Connect.

Single Sign-On (SSO) allows users to authenticate once and gain access to multiple related systems or services without needing to log in again for each one.

Differences:

Identity federation is about trust between organizations, while SSO is often used within the same organization.

Federation uses external identity providers, while SSO might use internal credentials.

Benefits:

Both reduce password fatigue.

Federation allows collaboration across domains.

SSO improves user experience and security.

## Microsoft Azure supports Facebook as an identity provider. (See [here](https://docs.microsoft.com/en-us/azure/active-directory/external-identities/facebook-federation)). What is an identity provider? Name one other external entity provider for Azure. Provide your sources.

An identity provider (IdP) is a service that creates, maintains, and manages identity information and provides authentication services to other applications.

Another external identity provider Azure supports is Google.

# RBAC - Individual

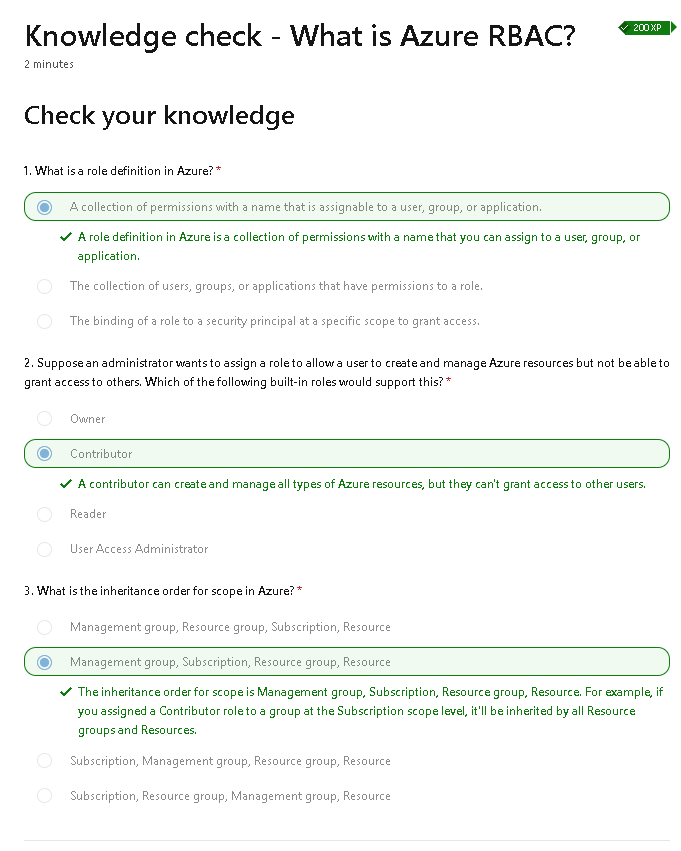
## Research Microsoft’s Azure RBAC. Read [this](https://docs.microsoft.com/en-us/learn/modules/secure-azure-resources-with-rbac/2-rbac-overview) and watch the included video.

## What does RBAC stand for? Provide a brief description.

RBAC stands for Role-Based Access Control. It is a method of restricting system access based on a user's assigned roles. Each role has specific permissions, and users get those permissions by being assigned to roles.

This simplifies management and improves security by ensuring users only have access to what they need.

## Do the knowledge check (next page from link provided). Provide screenshot below:



## What are the three elements of a Role assignment in Azure?

Security Principal – the user, group, or service that is assigned the role.

Role Definition – a collection of permissions, such as read, write, delete.

Scope – the set of resources the access applies to (e.g., a subscription, resource group, or specific resource).

**Marking Scheme**

|  |  |
| --- | --- |
|  | **Out of** |
|  |  |
| **Part A: IAAA** |  |
| Description | 8 |
| Source | 2 |
| Federated identity vs SSO | 6 |
| Identity Provider | 6 |
|  |  |
| **Part B: RBAC** |  |
| Definition | 4 |
| Knowledge check | 2 |
| Three elements | 6 |
|  |  |
|  |  |
| **Part C: Case Study Design** |  |
| Object Model | 4 |
| Role Model | 4 |
| Roles -> Pemissions | 8 |
| Map to Users -> Roles | 14 |
| Map to Roles -> Objects | 8 |
|  |  |
|  |  |
| Crossword | 10 |