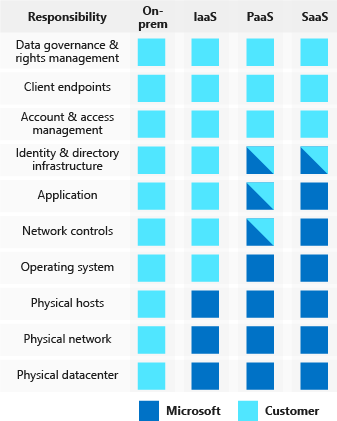
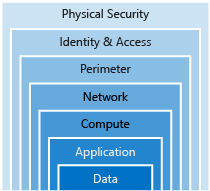
**Module 3.1: Security-Responsibility-Trust**

* Security responsibility between Microsoft , Iaas, Paas, Saas , On-Prem

* Layered Approach to Security
* Azure Security Center
  1. It is a Monitoring service that provides Threat Protection across all Azure Services
* Identity & Access
  1. Authentication (AuthN)
  2. Authorization (AuthZ)
  3. Azure Active Directory

It is a cloud based Identity Service which provides

* + 1. Authentication
    2. Single-Sing-on(SSO)
    3. Application Management
    4. B2B Identity Service
    5. Device Management
  1. Multi-factor Authentication(MFA)
  2. Role-Based Access Control(RBAC)
  3. Azure AD Privileged Identity Management (PIM)
* Encryption
  1. **Symmetric encryption** uses the same key to encrypt and decrypt the data
  2. **Asymmetric encryption** uses a public key and private key pair. Either key can encrypt but a single key can't decrypt its own encrypted data. To decrypt, you need the paired key
  3. Encryption at rest: - Database, Disk Files etc.
  4. Encryption in transit: - HTTP , VPN , TLS
  5. Azure Storage Service Encryption
  6. Azure Disk Encryption
  7. Transparent Data Encryption (TDE)
     1. Real time ENC and DEC
  8. Azure Key Vault
     1. Azure Key Vault is a centralized cloud service for storing your application secrets
     2. *Secrets management*. Access to tokens, passwords, certificates, *Application Programming Interface* (API) keys, and other secrets.
     3. *Key management*.
     4. *Certificate management*. *Secure Sockets Layer/ Transport Layer Security* (SSL/ TLS)
     5. *Store secrets backed by hardware security modules* (HSMs). The secrets and keys can be protected either by software, or by FIPS 140-2 Level 2 validated HSMs.
* Azure Certificates

Azure uses **x.509 v3** signed certificate, or they can be self-signed

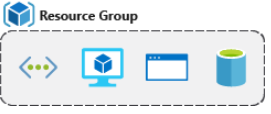
* 1. **Service certificates** are used for cloud services
  2. **Management certificates** are used for authenticating with the management API
* Network Security
  1. Azure Security Center
  2. Azure Firewall
     1. is a managed, cloud-based, network security service that protects your Azure Virtual Network resources
  3. Azure Application Gateway
     1. is a load balancer that includes a Web Application Firewall (WAF) that provides protection from common, known vulnerabilities in websites.
  4. Network virtual appliances(NVAs)
     1. are ideal options for non-HTTP services or advanced configurations, and are similar to hardware firewall appliances.
  5. Azure DDos Protection
     1. **Volumetric attacks**. The attackers goal is to flood the network layer with a substantial amount of seemingly legitimate traffic.
     2. **Protocol attacks**. These attacks render a target inaccessible, by exploiting a weakness in the layer 3 and layer 4 protocol stack.
     3. **Resource (application) layer attacks**. These attacks target web application packets to disrupt the transmission of data between hosts.
* Network Security Groups (NSGs) are a critical piece to restrict unnecessary communication.
* Document Protection
  1. **Microsoft Azure Information Protection** (AIP) is a cloud-based solution that helps organizations classify and optionally protect documents and emails by applying labels.
* Azure Advanced Threat Protection(ATP)
  1. is a cloud-based security solution that identifies, detects, and helps you investigate advanced threats, compromised identities, and malicious insider actions directed at your organization
  2. **Azure ATP portal**
  3. **Azure ATP sensor**
  4. **Azure ATP cloud service**
* Security for ALM
  1. **Microsoft Security Development Lifecycle (SDL)**
     1. introduces security and privacy considerations throughout all phases of the development process.

**Module 3.2: Monitor-Azure Ploicy**

* **Azure Policy** is an Azure service you use to create, assign and, manage policies
  1. The policy definition itself is represented as a JSON file
* **Azure Blueprints** enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements.
* **Compliance Manager** is a workflow-based risk assessment dashboard within the Trust Portal that enables you to track, assign, and verify your organization's regulatory compliance activities related to Microsoft professional services and Microsoft cloud services
* **Trust Center** is a website resource containing information and details about how Microsoft implements and supports security, privacy, compliance, and transparency in all Microsoft cloud products and services
* **Azure Monitor** maximizes the availability and performance of your applications by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments. It helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on.
* **Azure Service Health** is a suite of experiences that provide personalized guidance and support when issues with Azure services affect you. It can notify you, help you understand the impact of issues, and keep you updated as the issue is resolve

**Module 3.3: Azure-Resource Manager**

* What is a Resource Group
  1. Resource groups are a fundamental element of the Azure platform.
  2. A resource group is a logical container for resources deployed on Azure.
  3. These resources are anything you create in an Azure subscription like virtual machines, Application Gateways, and CosmosDB instances
  4. All resources must be in a resource group and a resource can only be a member of a single resource group.
  5. Resource groups can't be nested
  6. Logical Grouping of resources of similar usage, type, or location, you can provide some order and organization to resources you create in Azure
  7. If you delete a resource group, all resources contained within are also deleted
  8. Resource groups are also a scope for applying role-based access control (RBAC) permissions
  9. Resource groups serve as the life cycle for the resources within it
  10. Use **Resource Locks** to ensure critical resources aren't modified or deleted



* How to create Resource Groups
  1. Azure portal
  2. Azure PowerShell
  3. Azure CLI
  4. Templates
  5. Azure SDKs (like .NET, Java)
* What are Tags?
  1. Tags are name/value pairs of text data that you can apply to resources and resource groups
  2. A resource can have up to 50 tags.
  3. The name is limited to 512 characters except storage accounts, which have a limit of 128
  4. The tag value is limited to 256 characters for all types of resources
  5. Tags aren't inherited from parent resources.
  6. Not all resource types support tags, and tags can't be applied to classic resources
  7. Tags can be added and manipulated through
     1. Azure portal,
     2. Azure CLI,
     3. Azure PowerShell,
     4. Resource Manager templates,
     5. Through the REST API
* What is Azure Policy
  1. Azure Policy is a service you can use to create, assign, and manage policies
  2. These policies apply and enforce rules that your resources need to follow.
  3. Policies can be created and assigned through
     1. Azure portal
     2. Azure PowerShell
     3. Azure CLI.
  4. Once a Policy is created it needs to be assigned. It may take up to 30 mins to effect
  5. RBAC provides fine-grained access management for Azure resources, enabling you to grant users the specific rights they need to perform their jobs.
* What are Resource Locks
  1. Resource locks are settings that can be applied to any resource to block modification or deletion.
  2. Resource locks can set to either **Delete** or **Read-only**
  3. Resource locks apply regardless of RBAC permissions.
  4. Locks must be removed before you'll actually be able to perform the blocked activity.
  5. Locks get inherited by all resource group with in the resource group
  6. To perform the blocked activity you have to remove the Lock first