**MS-101 Course Acronyms – In the Order they first appear in the course**

**IaaS** **– Infrastructure as a Service** is a cloud computing offering in which a vendor provides users access to computing resources such as servers, storage and networking. Organizations use their own platforms and applications within a service provider's infrastructure.

**PaaS – Platform as a Service** is a category of cloud computing services that provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app.

**SaaS - Software as a Service** is a software licensing model in which access to the software is provided on a subscription basis, with the software being located on external servers rather than on servers located in-house. It is typically accessed through a web browser, with users logging into the system using a username and password Instead of each user having to install the software on their computer, the user is able to access the program via the internet. Businesses commonly use SaaS in customer retention management, human resources, and procurement. Technology companies, financial services companies, and utilities have led the business world in adopting SaaS technology.

**CRM - Customer Relationship Management** is an approach to manage a company's interaction with current and potential customers. It uses data analysis about customers' history with a company to improve business relationships with customers, specifically focusing on customer retention and ultimately driving sales growth.

**AIP – Azure Identity Protection** enables organizations to configure automated responses to detected suspicious actions related to user identities. It analyses your configuration and detects vulnerabilities that can have an impact on your user's identities. Azure Active Directory Identity Protection provides you with three policies: Multi-factor authentication registration policy, User risk policy, Sign-in risk policy

**DLP – Data Loss Prevention** uses rules and policies to determine which files and data are considered confidential, critical, or sensitive and then protects those files from being shared or transmitted. The goal of applying these rules, policies, and protective measures to Office 365 is to prevent data loss from the Office 365 environment.

**EOP – Exchange Online Protection** is a cloud-based email filtering service that helps protect your organization against spam and malware, and includes features to safeguard your organization from messaging-policy violations

**ATP – Advanced Threat Protection** is a cloud-based email filtering service that helps protect your organization against unknown malware and viruses by providing robust zero-day protection, and includes features to safeguard your organization from harmful links in real time. ATP has rich reporting and URL trace capabilities that give administrators insight into the kind of attacks happening in your organization

**SIEM – Security Incident and Event Management** software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware. Vendors sell SIEM as software, as appliances, or as managed services; these products are also used to log security data and generate reports for compliance purposes.

**Rest API - Representational State Transfer Application Programing Interface** is an API that uses HTTP requests to GET, PUT, POST and DELETE data. A RESTful API -- also referred to as a RESTful web service -- is based on representational state transfer (REST) technology, an architectural style and approach to communications often used in web services development.

**ML – Machine Learning** is an application of artificial intelligence (AI) that provides systems the ability to automatically learn and improve from experience without being explicitly programmed. Machine learning focuses on the development of computer programs that can access data and use it learn for themselves.

**ZAP – Zero-hour auto Purge** is an email protection feature that detects messages with phish, spam, or malware that have already been delivered to your users' inboxes, and then renders the malicious content harmless

**SMTP – Simple Mail Transfer Protocol** is a communication protocol for electronic mail transmission. User-level email clients typically use SMTP only for sending messages to a mail server for relaying, typically submit outgoing email to the mail server on port 587 or 465 as per RFC 8314.

**SPF – Sender Policy Framework** is an email-authentication technique which is used to prevent spammers from sending messages on behalf of your domain. With SPF an organisation can publish authorized mail servers.

**DKIM – Domain Keys Identified Mail** allows senders to associate a domain name with an email message, thus vouching for its authenticity. A sender creates the DKIM by “signing” the email with a digital signature. This “signature” is located in the message's header.

**DMARC – Domain-based Message and reporting Compliance** is a technology designed to combat email spoofing and is useful to stop phishing. Specifically, it protects the case where a phisher has spoofed the 5322.From email address, which is the email address displayed in mail clients like Outlook and outlook.com. Whereas the Sender Policy Framework, (SPF) catches the case where the phisher spoofs the 5321.MailFrom,which is where bounce messages are directed, DMARC catches the case that is more deceptive.

**SCC- Security & Compliance** Center is designed to help you manage compliance features across Office 365 for your organization. Links to existing SharePoint and Exchange compliance features bring together compliance capabilities across Office 365.

**URL - Uniform Resource** Locator is the address of a resource on the Internet. It indicates the location of a resource as well as the protocol used to access it. A URL contains the following information: The protocol used to a access the resource. The the location of the server (whether by IP address or domain name)

**CISO - Chief Information Security Officer** is the senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

**ATA - Advanced Threat** Analytics is an on-premises platform that helps protect your enterprise from multiple types of advanced targeted cyber attacks and insider threats.ATA works via leveraging a proprietary network parsing engine to capture and parse network traffic of multiple protocols (such as Kerberos, DNS, RPC, NTLM, and others) for authentication, authorization, and information gathering. This information is collected by ATA via; Port mirroring from Domain Controllers and DNS servers to the ATA Gateway and/or Deploying an ATA Lightweight Gateway (LGW) directly on Domain Controllers. ATA takes information from multiple data-sources, such as logs and events in your network, to learn the behavior of users and other entities in the organization, and builds a behavioral profile about them. ATA can receive events and logs from; SIEM Integration, Windows Event Forwarding (WEF) or Directly from the Windows Event Collector (for the Lightweight Gateway)

**CAS – Cloud APP Security** is a multimode Cloud Access Security Broker (CASB). It gives you rich visibility, enables you to control how your data travels, and provides sophisticated analytics to identify and combat cyber threats – across all of your cloud services. It helps you discover, protect and respond to threats. By definition, CASB provides security and monitoring of activity between users and cloud applications and enforces data security policies. A CASB may deliver security, the management or both, "security" is the prevention of high-risk events, whilst "management" is the monitoring and mitigation of high-risk events.

**EMS – Enterprise Mobility + Security** is a cloud-based offering from Microsoft which combines valuable standalone solutions licensed on a per user base. EMS integrates Identity and Access Management, Mobile Application (MAM) and Mobile Device Management (MDM) solutions with security solutions for information protection and threat management. In a modern workspace where mobility and Bring-your-own-device (BYOD) scenarios gain increasing significance, Enterprise Mobility + Security can help IT administrators meet the challenges that exist between the best possible user experience and productivity and a high level of security, data protection and risk management.

**MRM - Messaging Records Management** is the records management technology in Exchange Server and Exchange Online that helps organizations manage email lifecycle and reduce the legal risks associated with email.

**DPT – Default Policy Tag -** apply to untagged mailbox items in the entire mailbox. Untagged items are mailbox items that don't already have a retention tag applied. It’s 1 of 3 types of tags that can make up a Retention Policy.

**RPT – Retention Policy Tag** is a type of retention tag that you can apply to default folders in a mailbox, such as Inbox and Deleted Items

**IRM - Information Rights Management** is a feature that is available on the Enterprise Office 365 Plans. It allows you control the security of your data, and prevent users from printing, marking up your documents or even accessing them after a specified period of time.

**S/MIME - Secure/Multipurpose Internet Mail Extensions** is a technology that allows you to encrypt your emails. S/MIME is based on asymmetric cryptography to protect your emails from unwanted access. It also allows you to digitally sign your emails to verify you as the legitimate sender of the message, making it an effective weapon against many phishing attacks out there.

**TLS - Transport Layer Security** is a cryptographic protocol that provides end-to-end communications security over networks and is widely used for internet communications and online transactions. It is an IETF standard intended to prevent eavesdropping, tampering and message forgery. Common applications that employ TLS include Web browsers, instant messaging, e-mail and voice over IP.

**RMS – Rights Management Server** lets enterprises protect sensitive email messages and other documents with manageable rights technologies that limit whether others can read, print, forward, edit, or perform other tasks on these documents.

**PKI – Public Key Infrastructure** is the set of hardware, software, policies, processes, and procedures required to create, manage, distribute, use, store, and revoke digital certificates and public-keys.

**OME - Office 365 Message Encryption** is an online service that's built on Microsoft Azure Rights Management (Azure RMS) which is part of Azure Information Protection. This includes encryption, identity, and authorization policies to help secure your email. You can encrypt messages by using rights management templates, the Do Not Forward option, and the encrypt-only option. Users can then encrypt email messages and a variety of Office 365 attachments by using these options.

**HTML – Hyper Text Markup Language** is the major markup language used to display Web pages on the Internet. In other words, Web pages are composed of HTML, which is used to display text, images or other resources through a Web browser. All HTML is plain text, meaning it is not compiled and may be read by humans.

**RBAC – Role Based Access Control** helps you manage who has access to Azure resources, what they can do with those resources, and what areas they have access to. Using RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs. Instead of giving everybody unrestricted permissions in your Azure subscription or resources, you can allow only certain actions at a particular scope.

**EU – European Union** is an international political and economic organization of 28 European countries.

**GDPR - General Data Protection Regulation** is a regulation in EU law on data protection and privacy for all individual citizens of the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas.

**PII - Personally Identifiable Information** is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

**FCI – File classification Infrastructure** helps organizations classify data stored on Windows file servers. Using FCI, system administrators can set up rules that automatically classify files based on various factors, such as location or content. Once files have been classified, FCI can perform specified actions on them, such as moving them to a specified directory or encrypting them.

**BYOK - Bring Your Own Key** is where the end-user independently generates, backs up and submits its own encryption key. If the service provider doesn’t have access to the key in the first place, it can’t be compelled to hand it over, meaning that the user’s data will remain encrypted no matter who tries to access it.

**HYOK - Hold Your Own Key** is an information security feature designed to support enterprise customers that need to adhere to strict regulation and compliance policies. Microsoft is tasked with guarding organizations’ most sensitive data while still allowing organizations to have full control over the encryption keys and authorization process for the “highly-classified” company data.

**WIP - Windows Information Protection** is a feature built into Windows 10 that allows IT shops to control and manage business data separately from personal data on users' devices. Formerly known as enterprise data protection, Windows Information Protection (WIP) debuted in the Windows 10 Anniversary Update. In addition to separating business and personal data, IT administrators can use WIP to determine which users and which applications have access to what data and what users can do with corporate data.

**EDP - Enterprise Data Protection** is the previous name of Windows Information Protection **(see above)**

**MDM – Mobile Device Management** is a type of security software used by an IT department to monitor, manage and secure employees' mobile devices that are deployed across multiple mobile service providers and across multiple mobile operating systems being used in the organization.

**MAM – Mobile Application Management** is software that secures and enables IT control over enterprise applications on end users' corporate and personal smartphones and tablets.

**CSP - configuration service provider** is an interface in the client operating system, between configuration settings specified in a provisioning document, and configuration settings on the device. CSPs are similar to Group Policy client-side extensions, in that they provide an interface to read, set, modify, or delete configuration settings for a given feature. Typically, these settings map to registry keys, files or permissions. Some of these settings are configurable, and some are read-only.

**SCCM – System Center Configuration Manager** is a Windows product that enables administrators to manage the deployment and security of devices and applications across an enterprise.

**CSV – Comma Separated Value** is a simple file format used to store tabular data, such as a spreadsheet or database

**LOB – Line of Business apps** is a general term which refers to a product or a set of related products that serve a particular customer transaction or business need.

**UWP - Universal Windows Platform** is an API created by Microsoft and first introduced in Windows 10. The purpose of this platform is to help develop universal apps that run on Windows 10, Windows 10 Mobile, Xbox One and HoloLens without the need to be re-written for each.

**NTLM – NT Lan Manager** is the old authentication protocol used on networks that include systems running the Windows operating system and on stand-alone systems. The Microsoft Kerberos security package adds greater security than NTLM to systems on a network.

**SDK - Software Development Kit** is typically a set of software development tools that allows the creation of applications for a certain software package, software framework, hardware platform, computer system, video game console, operating system, or similar development platform.

**WaaS - Windows as a Service** is the approach Microsoft introduced with Windows 10 to deploy, update and service the operating system. Instead of releasing a new version of Windows every three to five years, as the company did with past iterations of the operating system, Microsoft will continually update Windows 10.

**KMS - Key Management Service** provides a way to automatically activate volume license editions of Microsoft Windows and Microsoft Office. It is designed to allow Volume Licensing customers to automate the activation process in a way that is transparent to end users. Volume Activation applies to systems that are covered under a Volume Licensing program and is used strictly as a tool for activation and not tied to license invoicing or billing.

**QMTH - Qualified Multi-tenant Hoster** program authorizes qualified third-party hosting service providers to host customers’ Windows virtual machines via Microsoft Cloud Agreement subscription or Microsoft Volume Licensing on multitenant hardware. The program also authorizes these third-party hosting service providers to host Office 365 ProPlus (including E3 and E5), Project Online Professional, and Visio Pro for Office 365 in shared computer activation (SCA) mode.

**VDA - Virtual Desktop Access)** is an authorization strategy that requires each device seeking access to a Windows virtual desktop in a virtual desktop infrastructure (VDI) to be licensed. The goal of Windows Virtual Desktop Access is to simplify licensing requirements in a virtual environment by licensing the devices that seek access to virtual desktops, instead of licensing the virtual desktops themselves.

**RDP – Remote Desktop Protocol** is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection. ... Microsoft currently refers to their official RDP client software as Remote Desktop Connection, formerly "Terminal Services Client".

**EA - Enterprise Agreement** offers the best value to organizations with 500\* or more users or devices that want a manageable volume licensing program that gives them the flexibility to buy cloud services and software licenses under one agreement.

**OOBE - Out-of-box experience** is the experience a consumer (or user) has when preparing to first use a new product. In relation to computing, this includes the setup process of installing and/or performing initial configuration of a piece of hardware or software on a computer.

**WUfB - Windows Update for Business** allows IT professionals to utilize the cloud-based Windows Update service to deploy and manage Windows updates. You can use Group Policy or MDM solutions such as Microsoft Intune to configure the Windows Update for Business settings that control how and when Windows 10 devices are updated. Windows Update for Business has been available since Windows 10, version 1511 and has been enhanced in Windows 10, version 1703 (also referred to as the Creators Update) to provide IT pros with greater control, while offering an improved experience for the end user.

**MFA – Multi-Factor Authentication** is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.

**APN - Apple Push Notification** is a robust, secure, and highly efficient service for app developers to propagate information to iOS (and, indirectly, watchOS), tvOS, and macOS devices. On initial launch of an app on a user’s device, the system automatically establishes an accredited, encrypted, and persistent IP connection between your app and APNs. This connection allows your app to perform setup to enable it to receive notifications.

**DEP - Device Enrollment Program** is a free program devised by Apple and the most preferred method for enrolling corporate iOS devices. Apple DEP makes the enrollment process of corporate-owned iOS devices automated and seamless for IT Admin.

**DEM - Device enrollment manager** is an Intune permission that can be applied to an AAD user account and lets the user enroll up to 1,000 devices. A DEM account is useful for scenarios where devices are enrolled and prepared before handing them out to the users of the devices. By design, there's a limit of 25 Device Enrollment Manager (DEM) accounts in Microsoft Intune.