Azure Identity, Governance, Privacy and Compliance Resources

Shailendra Chauhan

Microsoft MVP, Technical Consultant and Corporate Trainer

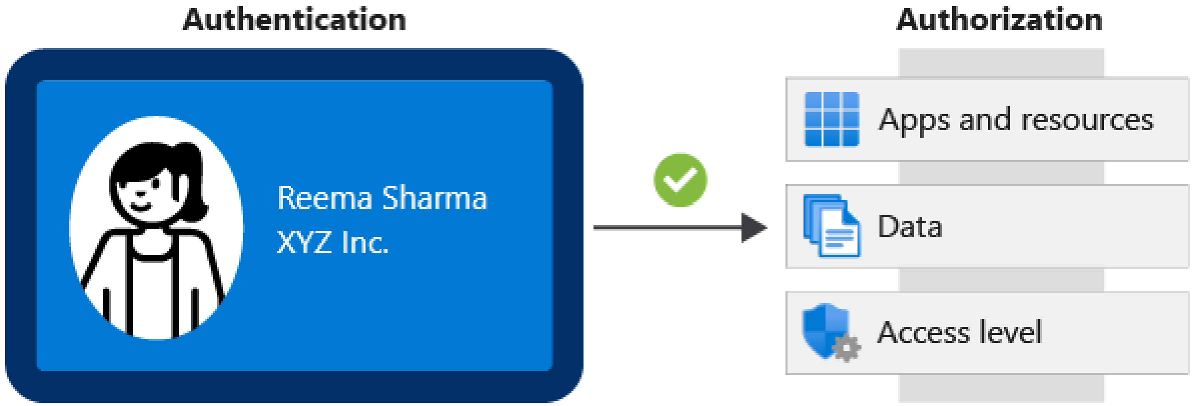
DotNetTricks

Agenda

- Authentication and Authorization
- Azure Active Directory
- Azure AD Services
- Multi Factor Authentication (MFA)
- Conditional Access and Role Based Access
- Azure Policy and Azure Blue Print
- Microsoft Compliance
- Microsoft Privacy Statement, OST and DPA
- Azure Sovereign Regions

Authentication and Authorization

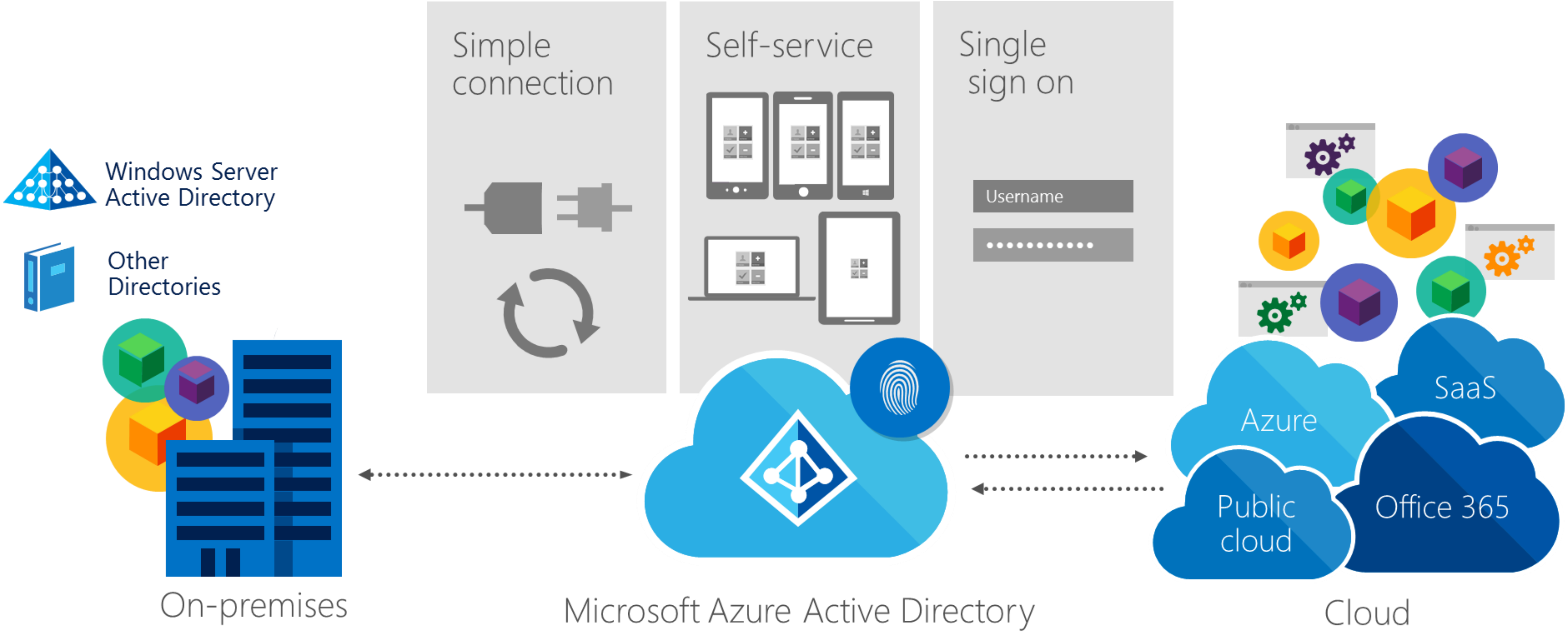
- **Authentication** is a process to know the identity of a person or service that wants to access a resource.
- **Authorization** is the process to know the access or permission of an authenticated person or service. It specifies what data they're allowed to access and what they can do with it.



Azure Active Directory

- Azure AD provides identity services that enable users to sign in and access both Microsoft cloud applications and your cloud applications.
- A globally accessed, secured, cloud-based identity and access management service for your cloud applications.
- Available in 4 editions: Free, Office 365 apps, Premium P1, and Premium P2.

Azure AD as the control plane



DotNetTricks

Who Use Azure AD?

- **IT admins** - An IT admin can use Azure AD to control access of apps and app resources, based on the business requirements.
- **App developers** - An app developer can use Azure AD for adding single sign-on (SSO) functionality into to your app where a user can access your app using existing credentials.
- **Users** - A User can manage his identity using Azure AD. For example, self-service password reset enables users to change or reset their password with no involvement from an IT administrator or help desk.
- **Online service subscribers** - Microsoft 365, Microsoft Office 365, Azure, and Microsoft Dynamics CRM Online subscribers.

Azure AD Services

- **Authentication** - Verifying identity to access applications and resources. It also includes providing functionality such as self-service password reset, multifactor authentication etc.
- **Single sign-on** - SSO enables a user to access multiple applications by using only one username and one password.
- **Application management** - You can manage SaaS apps and single-sign for your cloud and on-premises apps by using Azure AD.
- **Device management** - Along with user accounts, Azure AD supports the registration of devices which allows for device-based conditional access policies to restrict access attempts to only those coming from known devices, regardless of the requesting user account.

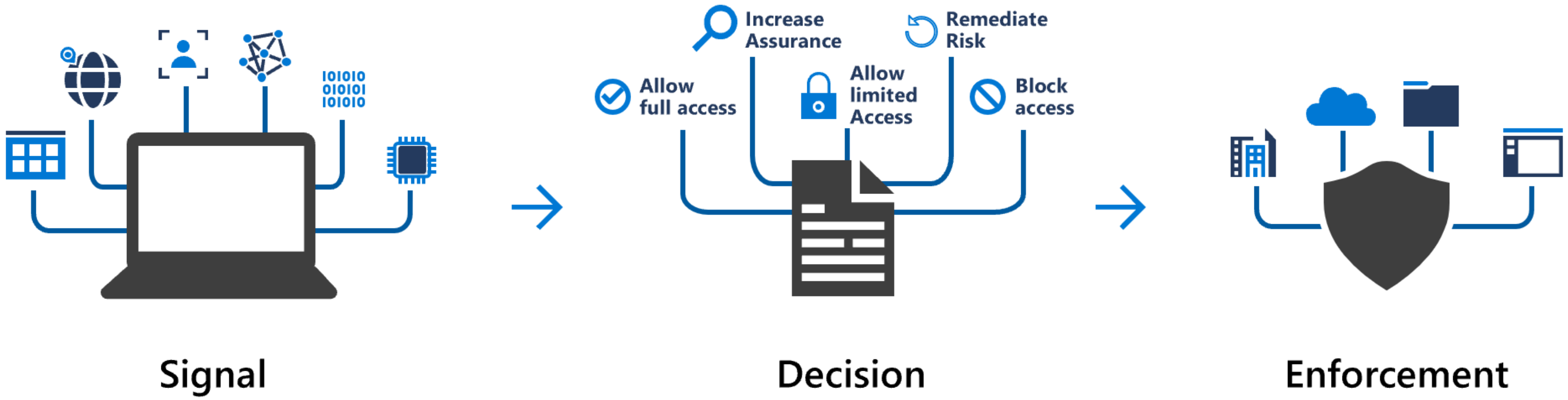
Multifactor Authentication

- Multifactor authentication is a process where a user is prompted during the sign-in process for an additional form of identification.
- For example a code on the mobile phone or a fingerprint scan.

- MFA increases identity security even your credential has been exposed or stolen.

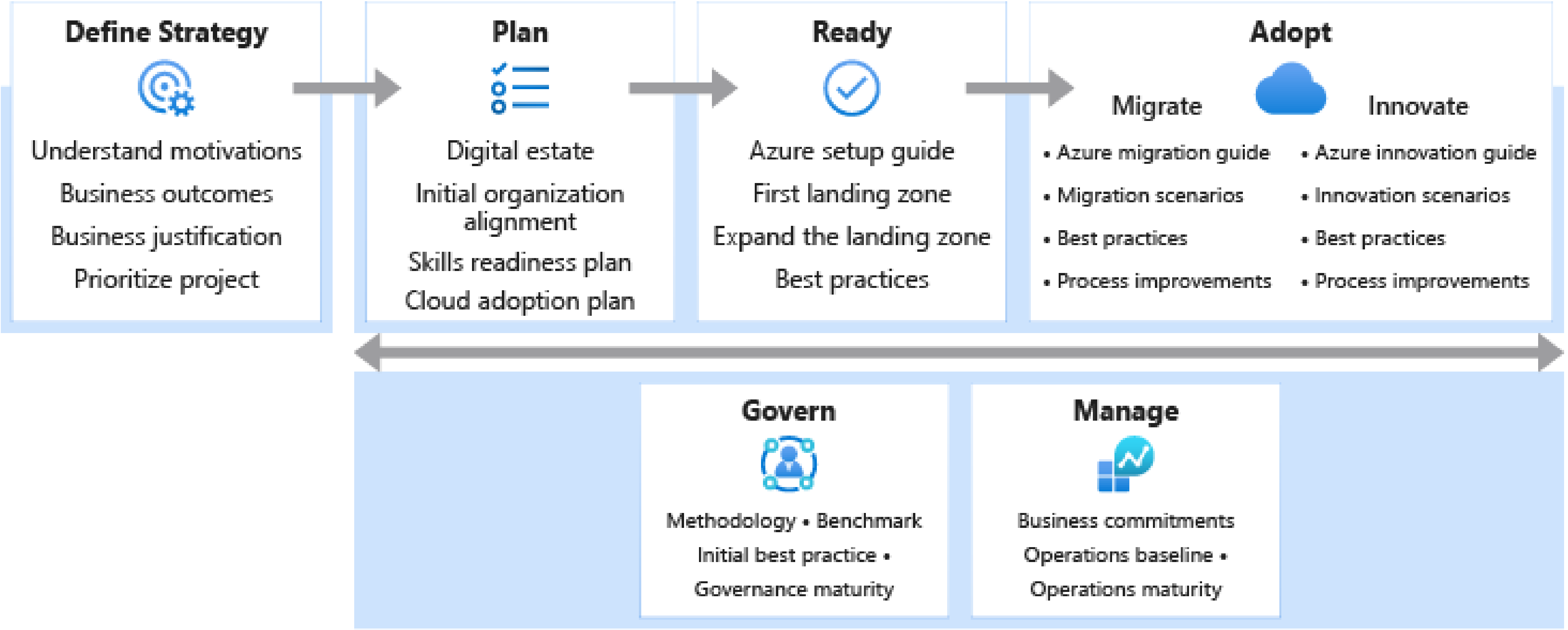
Conditional Access

- A tool that Azure Active Directory uses to allow (or deny) access to resources based on identity signals.
- Identity signals include who the user is, where the user is, and what device the user is requesting access from.
- Available in Azure AD Premium P1 or P2 and Microsoft 365 Business Premium license.



Cloud Adoption Framework for Azure

- Consists of tools, documentation, and proven practices.



Define Strategy

Understand motivations

Business outcomes

Business justification

Prioritize project

Plan

Digital estate

Initial organization alignment

Skills readiness plan

Cloud adoption plan

Ready

Azure setup guide

First landing zone

Expand the landing zone

Best practices

Adopt

Migrate

- Azure migration guide
- Migration scenarios
- Best practices
- Process improvements

Innovate

- Azure innovation guide
- Innovation scenarios
- Best practices
- Process improvements

Govern

Methodology • Benchmark

Initial best practice •

Governance maturity

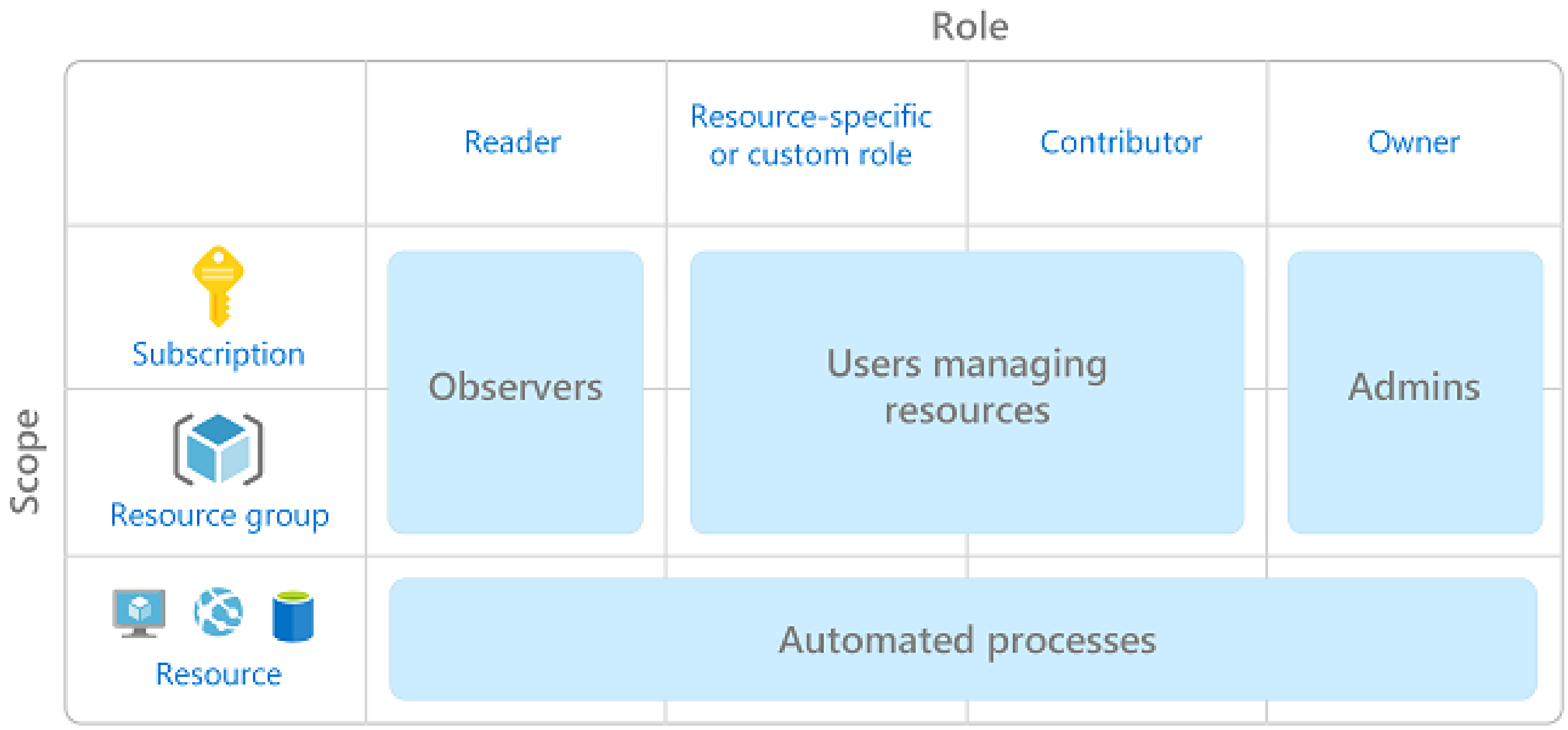
Manage

Business commitments

Operations baseline •

Operations maturity

Role-based Access Control (RBAC)



Role

Reader

Resource-specific or custom role

Contributor

Owner

Scope

Subscription

Resource group

Resource

Observers

Users managing resources

Admins

Automated processes

RBAC Apply To

- **IT Administrators** - This team requires full control of all resources.
- **Backup and Disaster Recovery** - This team is responsible for managing the health of regular backups and invoking any data or system recoveries.
- **Cost and Billing** - This team track and report on technology-related spend. They also manage the organization's internal budgets.
- **Security Operations** - This team monitors and responds to any technology-related security incidents. The team requires ongoing access to log files and security alerts.

Resource Locks

- A resource lock prevents resources from being accidentally deleted or changed.
- A lock can be applied to a subscription, a resource group, or an individual resource.
- You can set the lock level to **CanNotDelete** or **ReadOnly**.
- Resource locks apply regardless of RBAC permissions. Even if you're an owner of the resource, you must still remove the lock before you can perform the blocked activity.

Azure Policy

- A service that enables you to create, assign, and manage policies that control or audit your resources.
- Enforce different rules and effects over resource configurations so that those configurations stay compliant with corporate standards.
- Here are policy example:
    - Allowed virtual machine SKUs
    - Allowed locations
    - MFA should be enabled on accounts with write permissions on your subscription
    - CORS should not allow every resource to access your web applications
    - System updates should be installed on your machines

Azure Policy Apply Steps

- Create a policy definition.
- Assign the definition to resources.
- Review the evaluation results.

Azure Policy Initiatives

- A way of grouping related policies into one set.
- The initiative definition contains all of the policy definitions to help track your compliance state for a larger goal.
- Apply to a specific scope of a management group, a subscription, or a resource group.
- Make easier to add and remove policies without the need to change the policy assignment for your resources.

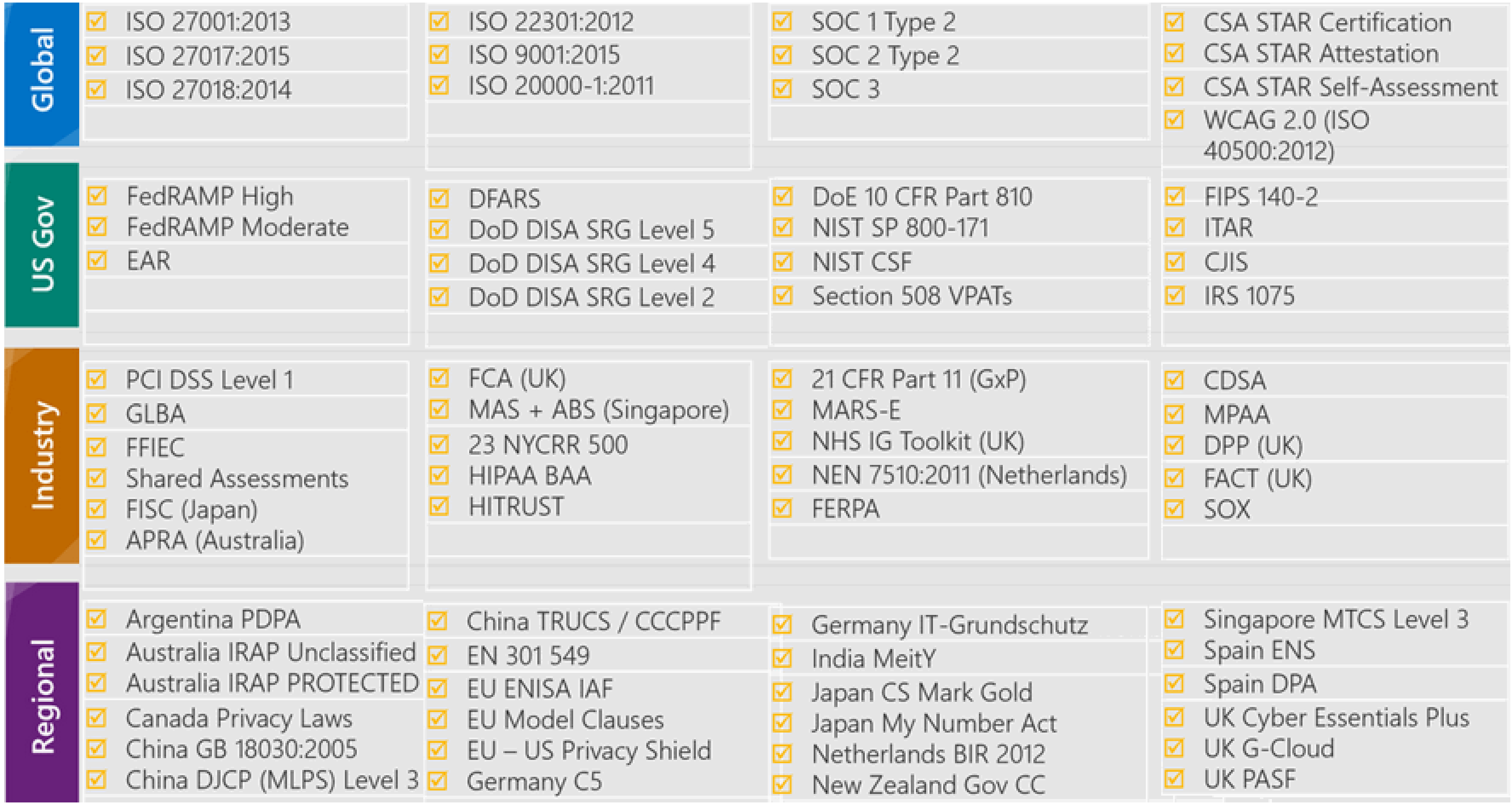
Azure Blueprints

- Enables you to define a repeatable set of governance tools and standard Azure resources that your organization requires.
- Azure Blueprints orchestrates the deployment of various resource such as:
  - Role assignments
  - Policy assignments
  - Azure Resource Manager templates
  - Resource groups

Azure Compliance

- Microsoft's commitment to privacy and how Azure adheres to common regulatory and compliance standards.
- In general, compliance means to adhere to a law, standard, or set of guidelines. Regulatory compliance refers to the discipline and process of ensuring that a company follows the laws that governing bodies enforce.

Azure Compliance Category



Global	☑ ISO 27001:2013 ☑ ISO 27017:2015 ☑ ISO 27018:2014	☑ ISO 22301:2012 ☑ ISO 9001:2015 ☑ ISO 20000-1:2011	☑ SOC 1 Type 2 ☑ SOC 2 Type 2 ☑ SOC 3	☑ CSA STAR Certification ☑ CSA STAR Attestation ☑ CSA STAR Self-Assessment ☑ WCAG 2.0 (ISO 40500:2012)
US Gov	☑ FedRAMP High ☑ FedRAMP Moderate ☑ EAR	☑ DFARS ☑ DoD DISA SRG Level 5 ☑ DoD DISA SRG Level 4 ☑ DoD DISA SRG Level 2	☑ DoE 10 CFR Part 810 ☑ NIST SP 800-171 ☑ NIST CSF ☑ Section 508 VPATs	☑ FIPS 140-2 ☑ ITAR ☑ CJIS ☑ IRS 1075
Industry	☑ PCI DSS Level 1 ☑ GLBA ☑ FFIEC ☑ Shared Assessments ☑ FISC (Japan) ☑ APRA (Australia)	☑ FCA (UK) ☑ MAS + ABS (Singapore) ☑ 23 NYCRR 500 ☑ HIPAA BAA ☑ HITRUST	☑ 21 CFR Part 11 (GxP) ☑ MARS-E ☑ NHS IG Toolkit (UK) ☑ NEN 7510:2011 (Netherlands) ☑ FERPA	☑ CDSA ☑ MPAA ☑ DPP (UK) ☑ FACT (UK) ☑ SOX
Regional	☑ Argentina PDPA ☑ Australia IRAP Unclassified ☑ Australia IRAP PROTECTED ☑ Canada Privacy Laws ☑ China GB 18030:2005 ☑ China DJCP (MLPS) Level 3	☑ China TRUCS / CCCPPF ☑ EN 301 549 ☑ EU ENISA IAF ☑ EU Model Clauses ☑ EU – US Privacy Shield ☑ Germany C5	☑ Germany IT-Grundschutz ☑ India MeitY ☑ Japan CS Mark Gold ☑ Japan My Number Act ☑ Netherlands BIR 2012 ☑ New Zealand Gov CC	☑ Singapore MTCS Level 3 ☑ Spain ENS ☑ Spain DPA ☑ UK Cyber Essentials Plus ☑ UK G-Cloud ☑ UK PASF

Microsoft Privacy Statement & Online Services Terms

- The **Microsoft Privacy Statement** explains what personal data Microsoft collects, how Microsoft uses it, and for what purposes.
- The privacy statement covers all of Microsoft's services, websites, apps, software, servers, and devices.
- The **Online Services Terms (OST)** is a legal agreement between Microsoft and the customer. The OST details the obligations by both parties with respect to the processing and security of customer data and personal data.
- The OST applies to Microsoft's online services including Azure, Dynamics 365, Office 365, and Bing Maps.

Data Protection Addendum

- Defines the data processing & security terms for online services.
- DPA terms include:
  - Compliance with laws.
  - Disclosure of processed data.
  - Data Security, which includes security practices and policies, data encryption, data access, customer responsibilities, and compliance.
  - Data transfer, retention, and deletion.

Trust Center

- The Trust Center showcases Microsoft's principles for maintaining data integrity in the cloud and how Microsoft implements and supports security, privacy, compliance, and transparency in all Microsoft cloud products and services.
- The Trust Center is an important part of the Microsoft Trusted Cloud Initiative and provides support and resources for the legal and compliance community.

Azure Compliance Documentation

- Provides you with detailed documentation about legal and regulatory standards and compliance on Azure.
- Compliance Categories:
  - Global
  - US government
  - Financial services
  - Health
  - Media and manufacturing
  - Regional

Azure Government

- Azure Government is a separate instance of the Microsoft Azure service.
- Addresses the security and compliance needs of US federal agencies, state and local governments, and their solution providers.
- Azure Government offers physical isolation from non-US government deployments and provides screened US personnel.

Azure China 21Vianet

- A physically separated instance of cloud services located in China.
- Azure China 21Vianet is independently operated and transacted by Shanghai Blue Cloud Technology Co., Ltd. ("21Vianet"), a wholly owned subsidiary of Beijing 21Vianet Broadband Data Center Co., Ltd.
- To comply with China Telecommunication Regulation the Azure service in China is operated by 21Vianet, based on the technologies licensed from Microsoft.