cvation
CLOUD INNOVATION

Cloud Assessment

Agenda

01 Introduction

02 Conclusions

03 Assessment Areas

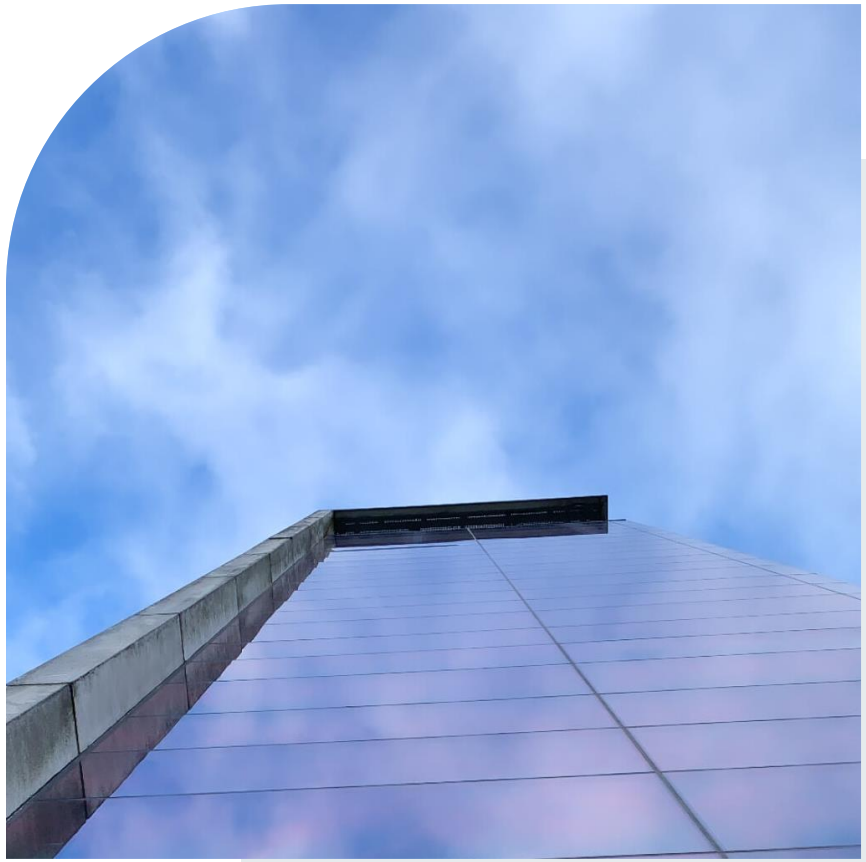
04 Next Step Priorities

01

Introduction

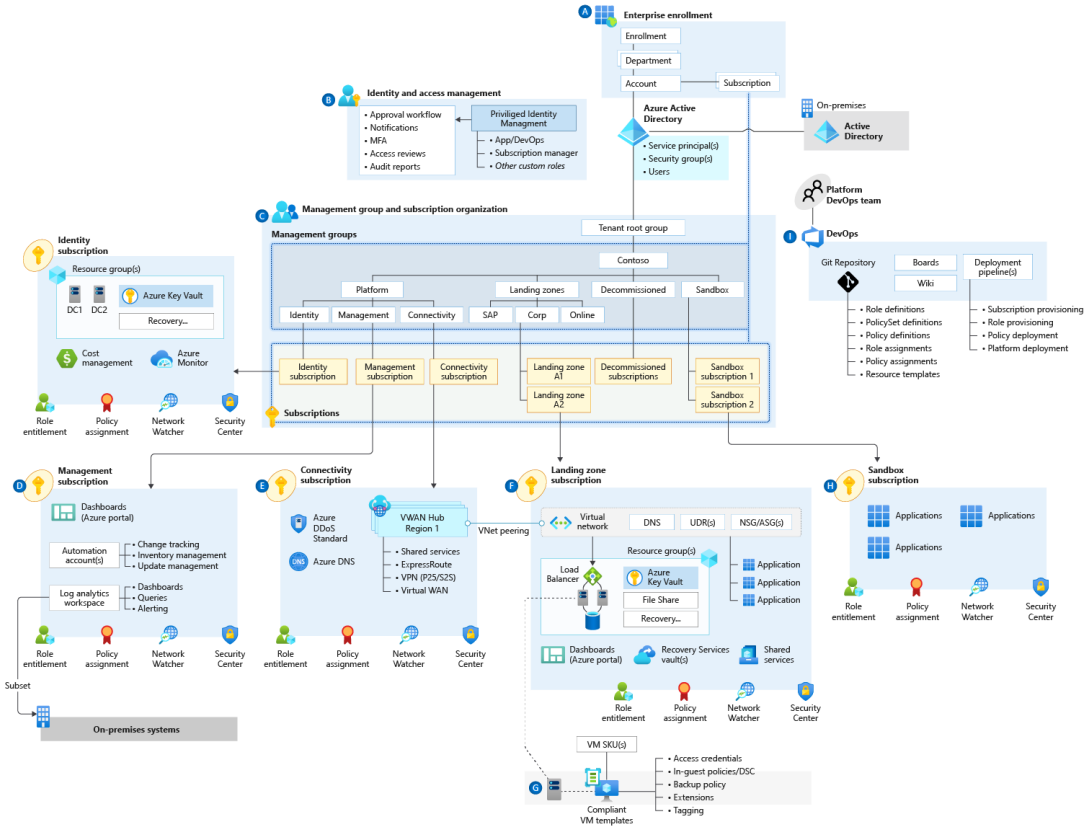
Purpose

- The cloud provides scalable and managed services to promote agility and innovation with a short time-to-market
- This is achieved by utilizing several managed services in combination, from the huge catalogue of new and innovative cloud services
- A Cloud Assessment determines if pre-requisites are in place to ensure this happens in a structured and secure way, when work become play in cloud DevOps teams
- When done correctly, guardrails and guidelines are deployed to create boundaries on *what* can be done – but without limiting *how* it can be done, thus providing a full-blown cloud experience to development teams, allowing them to provision compute and storage services as desired with a mind at rest



Approach

- Assessment is based on Microsoft's Cloud Adoption Framework - CAF
- Identifies risks, and recommends actions for remediation
- The critical design areas to be assessed in a secure Azure deployment are:
  - ✓ Enterprise Enrollment and Azure AD tenants
  - ✓ Identity and Access Management
  - ✓ Management Group and Subscription Organization
  - ✓ Network Topology and Connectivity
  - ✓ Management and Monitoring
  - ✓ Business Continuity and Disaster Recovery
  - ✓ Security, Governance and Compliance
  - ✓ Platform Automation and DevOps



cyation | CLOUD INNOVATION

02

Conclusions

Executive Summary

This part of the assessment will gauge the overall state of the installation(s) highlight, prioritize and summarize the key findings and recommended actions across the assessment areas found on the following pages.

Assessment Areas

Enterprise Enrollment and Azure AD Tenants

Risks	Recommendations
Risk 1 …	Recommendation 1 …
Risk 2 …	Recommendation 2 …

In this part of the assessment we will help you examine your Enterprise Agreement and Azure AD tenants.

Enterprise Agreement (EA) enrollment are managed via the Azure EA portal, and often represents an organization's hierarchy, which includes departments, accounts, and subscriptions, that represents cost-enrollment groups within an organization.

Azure AD tenants are managed with the standard Azure portal. It is the core component of Azure and must be configured correctly to provide a secure identity infrastructure with end-to-end protection through layers of security as barriers of authentication.

Identity and Access Management

Risks	Recommendations
Risk 1 …	Recommendation 1 …
Risk 2 …	Recommendation 2 …

Identity and access management (IAM) is boundary security in the public cloud. It must be treated as the foundation of any secure and fully compliant public cloud architecture. The set-up has to offer a comprehensive set of services, tools, and reference architectures to enable your organization to make highly secure, operationally efficient environments.

Identity provides the basis of a large percentage of security assurance. It enables access based on identity authentication and authorization controls in cloud services to protect data and resources and to decide which requests should be permitted.

This section examines design considerations and recommendations related to IAM for an enterprise environment.

Management Group and Subscription Organization

Risks	Recommendations
Risk 1 …	Recommendation 1 …
Risk 2 …	Recommendation 2 …

Management of group structures must be considered thoroughly when an organization plans Azure adoption at scale.

We will validate the organization of your management groups and implementation. This includes verification of platform management group under the root management group supporting platform policies and RBAC assignments. Ensuring that different policies can be applied and that the billing for common resources is centralized in one set of foundational subscriptions.

Subscriptions are a unit of management, billing, and scale. They play a critical role when you're designing for large-scale Azure adoption. We will validate subscription requirements and design target subscriptions based on critical factors. Factors include environment type, ownership and governance model, organizational structure, and application portfolios.

Network Topology and Connectivity

Risks	Recommendations
Risk 1 …	Recommendation 1 …
Risk 2 …	Recommendation 2 …

Networking and connectivity are core components in a hybrid clouds, and any cloud environment where perimeter security should be used as an additional protection layer, and consists of several sub areas, including:

- *Plan for IP addressing (IPAM)*
- *DNS and name resolution for on-premises and Azure resources*
- *Connectivity to Azure and Azure PaaS services*
- *Plan for inbound and outbound internet connectivity*
- *Plan for subscription network segmentation*
- *Define network encryption requirements*
- *Plan for traffic inspection*

Management and Monitoring

Risks	Recommendations
Risk 1 …	Recommendation 1 …
Risk 2 …	Recommendation 2 …

This section explores how to operationally maintain an Azure enterprise estate with centralized management and monitoring at a platform level. More specifically, it presents key recommendations for central teams to maintain operational visibility within a large-scale Azure platform.

Application-centric platform monitoring, encompassing both hot and cold telemetry paths for metrics and logs, respectively:

- *Audit logs*
- *Diagnostics, performance counters and custom metrics*
- *Operating system logs*
- *Application specific logs*
- *Alerts and resource health events*
- *Integration with on-premises monitoring systems*

Business Continuity and Disaster Recovery

Risks	Recommendations
Risk 1 …	Recommendation 1 …
Risk 2 …	Recommendation 2 …

Your organization or enterprise needs to design suitable, platform-level capabilities that application workloads can consume to meet their specific requirements. Specifically, these application workloads have requirements pertaining to recover time objective (RTO) and recovery point objective (RPO). We help you make sure that you capture disaster recovery (DR) requirements in order to design capabilities appropriately for these workloads.

Validating plan for a business continuity and DR network architecture that provides concurrent connectivity to all sites. DR networks that use the same classless inter-domain routing blocks, such as production networks, require a network failover process that can complicate and delay application failover in the event of an outage.

Security, Governance and Compliance

Risks	Recommendations
Risk 1 …	Recommendation 1 …
Risk 2 …	Recommendation 2 …

This part of the report verifies encryption and key management, planning for governance, defining security monitoring and an audit policy on top of planning for platform security.

Encryption is a vital step toward ensuring data privacy, compliance, and data residency. It's also one of the most important security concerns of many enterprises. This section covers design considerations and recommendations as they pertain to encryption and key management.

Governance provides mechanisms and processes to maintain control over your applications and resources. This is essential to ensure security and compliance within enterprise technical estates. This can enforce vital management and security conventions across your platform services and supplement role-based access control (RBAC) that controls what actions authorized users can perform.

Platform Automation and DevOps

Risks	Recommendations
Risk 1 …	Recommendation 1 …
Risk 2 …	Recommendation 2 …

Many traditional IT operating models aren't compatible with the cloud, and therefore organizations must undergo an operational and organizational transformation to deliver against enterprise migration targets. DevOps capabilities are key to meet these targets across AppDevOps, PlatformOps, NetOps and SecOps.

We will validate your cross-functional DevOps capabilities against the ability to build, manage, and maintain an enterprise-scale architecture.

04

Next Step Priorities

Recommended Actions

- *In this part of the report you will get the clear overview of your current solution and state.*
- *We will provide you with a clear action plan and recommendations to follow.*

Suggested Action Plan

1. Action 1 …
2. Action 2 …
3. Action 3 …
4. Action 4 …

cvation
CLOUD INNOVATION

We accelerate your development