Cloud Platform review
Management Report

Architektur für

Muster-Kunde

Max Mustermann

max.mustermann@acp.at

vertraulich

Architektur von

ACP IT Solutions GmbH

ACP Consultant

ACPConsultant@acp.at

Präambel

Innerhalb dieser Übersicht werden die von ACP IT Solutions („ACP“) geplanten Leistungen, Nicht Inhalte, Mitwirkungspflichten und Hinweise überblicksartig aufgelistet und beschrieben.

Hinweis betreffend Urheberrecht

Das Copyright dieser Arbeit liegt bei ACP IT Solutions GmbH ("ACP").

Änderungen und Ergänzungen an diesem Dokument, einschließlich seiner Anhänge, dessen Vervielfältigung sowie die Weitergabe an Dritte bedürfen der schriftlichen Zustimmung durch ACP IT Solutions GmbH. Die auf allen Seiten dieses Konzeptes enthaltenen Informationen (Daten) sind Geschäftsgeheimnisse bzw. Informationen wirtschaftlicher oder finanzieller Art. Sie sind vertraulich zu behandeln und nur für den internen Gebrauch bestimmt.

Eine auszugsweise oder vollständige Weitergabe dieser vertraulichen Informationen an Dritte ist nur mit schriftlicher Einverständniserklärung seitens ACP IT Solutions GmbH gestattet.

Version	Datum	Erstellt/geändert von	Bemerkung
1.0	29.08.2026	Johannes Lagler-Gruener	Initial Version

Inhaltsverzeichnis

1 Management Summary 4

1.1 Bewertung nach Well-Architected-Säule 4

1.2 Top-Handlungsempfehlungen 5

1.3 Bewertung nach Kategorie 7

1 Management Summary

Dieser Bericht dokumentiert die Ergebnisse des Azure Cloud Platform Reviews für Muster-Kunde. Es wurden 147 Checks geprüft, davon 85 erfüllt (gewichteter Compliance-Score nach Schweregrad: 57.7% – Kritisch). Automatisiert erhobene Checks basieren auf Azure Resource Graph, Microsoft Graph und Azure PowerShell; alle übrigen Checks wurden im strukturierten Interview mit dem Kunden erhoben. Technische Details zu jedem einzelnen Check finden Sie im separaten Detailbericht.

Score	Geprüft	Erfüllt	High	Medium	Low	Abdeckung	Ausgeschlossen
57.7%	147	85	17	42	3	57.6%	108

Score = erfüllt / (erfüllt + offen), gewichtet nach Schweregrad (High×3, Medium×2, Low×1). Rating: ≥90% Sehr gut · ≥75% Gut · ≥60% Verbesserungswürdig · <60% Kritisch.

1.1 Bewertung nach Well-Architected-Säule

Säule	Erfüllt	Offen	Score	Abdeckung
Cost	2/4	2	50%	100%
Operations	16/25	9	64%	100%
Performance	2/3	1	66.7%	100%
Reliability	19/25	6	76%	100%
Security	46/90	44	51.1%	100%

1.2 Top-Handlungsempfehlungen

Priorität	Check	Kategorie	Empfehlung
High	E01.05	Governance	Manage policy assignments at the highest appropriate level with exclusions at bottom levels, if required.
High	B03.09	Identity and Access Management	When deploying Active Directory Domain Controllers, use a location with Availability Zones and deploy at least two VMs across these zones. If not available, deploy in an Availability Set.
High	D03.09	Network Topology and Connectivity	Enable auto-registration for Azure DNS to automatically manage the lifecycle of the DNS records for the virtual machines deployed within a virtual network.
High	D05.06	Network Topology and Connectivity	Use Azure DDoS Network or IP Protection plans to help protect Public IP Addresses endpoints within the virtual networks including application landing zones.
High	D05.08	Network Topology and Connectivity	Add diagnostic settings to save DDoS related logs for all the protected public IP addresses (DDoS IP or Network Protection).
High	D05.08b	Network Topology and Connectivity	Ensure there is a policy assignment to deny Public IP addresses directly tied to Virtual Machines. Use exclusions if public IPs are needed on specific VMs.
High	D09.02	Network Topology and Connectivity	Don't rely on the NSG inbound default rules using the VirtualNetwork service tag to limit connectivity.

High	G02.01	Security	Use Azure Key Vault to store your secrets and credentials.
High	G03.03	Security	Enable Defender Cloud Security Posture Management (CSPM) plan for all resources in addition to the on-by-default Foundational plan for advanced security posture features .
High	G03.04	Security	Enable a Microsoft Defender for Servers plan for all cloud servers.
High	G03.05	Security	Enable Defender Cloud Workload Protection Plans for Azure Resources on all subscriptions.
High	G03.06	Security	Enable Endpoint Protection on IaaS Servers.
High	G04.02	Security	Enable container soft delete for the storage account to recover a deleted container and its contents.

1.3 Bewertung nach Kategorie

Kategorie	Erfüllt	Offen	Score	Abdeckung
Azure Billing and Microsoft Entra ID Tenants	5/6	1	83.3%	100%
Governance	10/15	5	66.7%	100%
Identity and Access Management	13/22	9	59.1%	100%
Management	12/23	11	52.2%	100%
Network Topology and Connectivity	24/39	15	61.5%	100%
Resource Organization	11/14	3	78.6%	100%
Security	10/28	18	35.7%	100%