Cloud Platform review
Detail Report

Report für

Muster-Kunde

Max Mustermann

max.mustermann@acp.at

vertraulich

Report 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 Detailergebnisse 5

1.1 Azure Billing and Microsoft Entra ID Tenants 5

1.1.1 Cloud Solution Provider 5

1.1.2 Microsoft Entra ID Tenants **Error! Bookmark not defined.**

1.2 Governance 9

1.2.1 Sovereign Cloud **Error! Bookmark not defined.**

1.3 Identity and Access Management **Error! Bookmark not defined.**

1.3.1 Identity **Error! Bookmark not defined.**

1.3.2 Landing zones **Error! Bookmark not defined.**

1.3.3 Microsoft Entra ID **Error! Bookmark not defined.**

1.3.4 Microsoft Entra ID and Hybrid Identity **Error! Bookmark not defined.**

1.4 Management **Error! Bookmark not defined.**

1.4.1 App delivery **Error! Bookmark not defined.**

1.4.2 Data Protection **Error! Bookmark not defined.**

1.4.3 Monitoring **Error! Bookmark not defined.**

1.4.4 Operational compliance **Error! Bookmark not defined.**

1.4.5 Protect and Recover **Error! Bookmark not defined.**

1.5 Network Topology and Connectivity **Error! Bookmark not defined.**

1.5.1 Hub and spoke **Error! Bookmark not defined.**

1.5.2 Hybrid **Error! Bookmark not defined.**

1.5.3 IP plan **Error! Bookmark not defined.**

1.5.4 Internet **Error! Bookmark not defined.**

1.5.5 PaaS **Error! Bookmark not defined.**

1.5.6 Segmentation **Error! Bookmark not defined.**

1.6 Resource Organization **Error! Bookmark not defined.**

1.6.1 Naming and tagging **Error! Bookmark not defined.**

1.6.2 Regions **Error! Bookmark not defined.**

1.6.3 Subscriptions **Error! Bookmark not defined.**

1.7 Security **Error! Bookmark not defined.**

1.7.1 Access control **Error! Bookmark not defined.**

1.7.2 Encryption and keys **Error! Bookmark not defined.**

1.7.3 Operations **Error! Bookmark not defined.**

1.7.4 Overview **Error! Bookmark not defined.**

1.7.5 Secure privileged access **Error! Bookmark not defined.**

1.7.6 Service enablement framework **Error! Bookmark not defined.**

1.7.7 Sovereign Cloud **Error! Bookmark not defined.**

2 Ausgeschlossene Checks 12

1 Detailergebnisse

Die folgenden Abschnitte listen jeden geprüften Check mit Ergebnis, Nachweis und Empfehlung, gegliedert nach Kategorie.

1.1 Azure Billing and Microsoft Entra ID Tenants

1.1.1 Cloud Solution Provider

A02.01	High	**Erfüllt**

If you give a partner access to administer your tenant, use Azure Lighthouse.

Weitere Informationen: https://learn.microsoft.com/azure/lighthouse/overview

Check Description:

Azure Lighthouse ermöglicht es einem Service Provider oder Partner, delegierte Customer-Subscriptions und Resource Groups direkt aus dem eigenen Tenant zu administrieren, ohne den Kontext zu wechseln oder sich im Tenant des Kunden anzumelden.

Der Zugriff wird über Azure Delegated Resource Management mittels ARM-Templates gewährt; der Kunde behält die volle Kontrolle, kann jede Aktion des Providers über sein eigenes Activity Log auditieren und den Zugriff jederzeit widerrufen. Lighthouse integriert sich mit Standard-Azure-Tools (Azure Policy, Microsoft Sentinel, Azure Arc), unterstützt das CSP-Programm und verursacht keine zusätzlichen Kosten, kann jedoch keine Sovereign-/National-Cloud-Grenzen überschreiten.

Wird einem Partner administrativer Zugriff auf einen Tenant gewährt, sollte statt direkter Guest- oder Admin-Accounts Azure Lighthouse verwendet werden, da es der dafür vorgesehene, auditierbare und widerrufbare Mechanismus ist.

Validierungsergebnis:

1 Lighthouse ist konfiguriert

A02.02 | Low | Erfüllt

If you have a CSP partner, define and document your support request and escalation process.

Weitere Informationen: https://learn.microsoft.com/azure/cloud-adoption-framework/ready/landing-zone/design-area/azure-billing-cloud-solution-provider#design-recommendations

Check Description:

Im Cloud Solution Provider (CSP) Modell übernimmt ein Microsoft Partner den gesamten Azure-Lifecycle des Kunden - Preisgestaltung, Billing, Subscription-Provisionierung und First-Level-Support - über einen Azure Plan unter seinem Microsoft Partner Agreement.

Nur der Partner, nicht der Kunde, kann neue Subscriptions oder einen Azure Plan bereitstellen, und Partner können Subscriptions nach definierten Kriterien suspendieren; der Kauf von Azure Reservations kann über die Customer-Permissions-Funktion im Partner Center an den Kunden delegiert werden.

Organisationen sollten den Support-Case-, Eskalations- und Self-Service-Subscription-Prozess mit ihrem CSP-Partner von Anfang an klar definieren und dokumentieren - nicht erst im Ernstfall herausfinden - und für Administer-on-Behalf-of-Zugriffe Azure Lighthouse nutzen, wobei Partner von der veralteten DAP auf die enger abgegrenzte GDAP umstellen sollten.

Jeder Benutzer, der Subscriptions auf Invoice-Section-, Billing-Profile- oder Billing-Account-Ebene anlegen kann, muss mit Multi-Faktor-Authentifizierung abgesichert sein, und Partner sollten Customer-Subscriptions im eigenen, ordnungsgemäß governten Entra Tenant des Kunden bereitstellen statt in einem partnerverwalteten Tenant.

Validierungsergebnis:

Kein Kommentar vorhanden.

A01.02 | Low | Erfüllt

Use Multi-Tenant Automation approach to managing your Microsoft Entra ID Tenants.

Weitere Informationen: https://learn.microsoft.com/azure/cloud-adoption-framework/ready/landing-zone/design-area/multi-tenant/automation

Check Description:

Erstrecken sich Azure Landing Zones über mehrere Microsoft Entra Tenants, sollten Plattform-Deployment und -Betrieb dennoch konsistent automatisiert werden - über einen von zwei Ansätzen, je nachdem, warum mehrere Tenants bestehen.

Ansatz 1 (vollständige Isolation) hält Git Repository, CI/CD Pipeline und Automation-Identitäten pro Tenant vollständig getrennt - heute erforderlich, da Managed Identities Cross-Tenant-Szenarien in der General Availability nicht unterstützen, was jedoch pro Tenant einen eigenen Account für Administratoren bedeutet. Ansatz 2 nutzt eine einzelne Application Registration im verwaltenden Tenant mit je einem Service Principal in jedem verwalteten Tenant, sodass Pipelines sich überall mit einem Credential authentifizieren können - üblich bei MSP-Szenarien mit dem Deployment-Stamps-Pattern.

Da diese gemeinsame App Registration ein hochprivilegiertes Credential darstellt, muss sie aktiv im SIEM überwacht werden, mit automatisierter Reaktion auf High-Severity-Alerts. Azure Lighthouse ähnelt Ansatz 2, kann aber nicht für die vollständige Plattformautomatisierung genutzt werden, da es keine Zuweisung von Owner-, User Access Administrator- oder DataActions-gewährenden Rollen unterstützt.

Validierungsergebnis:

Es ist nur ein Tenant notwendig

A01.03 | High | Erfüllt

Use Azure Lighthouse for Multi-Tenant Management with the same IDs.

Weitere Informationen: https://learn.microsoft.com/azure/cloud-adoption-framework/ready/landing-zone/design-area/multi-tenant/lighthouse

Check Description:

Azure Lighthouse ermöglicht skalierbares, auditierbares Multitenant-Management, indem ein verwaltender Tenant delegierte Subscriptions oder Resource Groups in anderen Tenants administrieren kann - ohne Guest-B2B-Accounts oder separate Anmeldungen.

Es funktioniert sowohl für Single- als auch für Multitenant-Landing-Zones, integriert sich mit Azure Policy, Microsoft Sentinel und Azure Arc, kann aber keine Sovereign-Cloud-Grenzen überbrücken und delegiert nur Subscriptions oder Resource Groups, nicht ganze Management Groups oder Tenants.

Azure Lighthouse sollte bidirektional zwischen Tenants eingesetzt werden, um Guest-Accounts pro Tenant überflüssig zu machen und das Cross-Tenant-Management zu vereinfachen - in Kombination mit Privileged Identity Management (eligible statt standing Authorizations, wobei Entra ID P2 nur im verwaltenden Tenant erforderlich ist). Ein dokumentiertes Pattern nutzt Lighthouse zudem, um Azure Policy für Private Endpoint DNS Zones automatisch von einem Hub-Tenant in Spoke-Tenants zu verlinken.

Validierungsergebnis:

1 Lighthouse ist konfiguriert

1.2 Governance

E01.01	High	**Erfüllt**

Leverage Azure Policy strategically, define controls for your environment, using Policy Initiatives to group related policies.

Weitere Informationen: https://learn.microsoft.com/azure/governance/policy/overview

Check Description:

Azure Policy setzt organisatorische Standards durch, indem Ressourceneigenschaften (und zunehmend auch die Identität des Anfragenden) gegen JSON-definierte Regeln ausgewertet werden, mit einem Compliance-Dashboard bis auf Ebene einzelner Ressourcen und Policies; die Effects reichen von Audit und AuditIfNotExists über Deny bis zu Append, Modify und DeployIfNotExists, und nicht konforme Ressourcen können über Remediation-Tasks automatisch behoben werden, ohne sie neu zu erstellen.

Gruppieren Sie zusammengehörige Policy-Definitionen in Initiatives – empfohlen selbst bei nur einer einzigen Policy –, damit später weitere Controls ergänzt werden können, ohne neue Assignments anlegen und verwalten zu müssen.

Assignments verknüpfen Definitionen bzw. Initiatives mit einem Scope (Management Group, Subscription, Resource Group oder Ressource); das System arbeitet strikt nach Deny/Evaluate, sodass Child-Scopes ausgeschlossen werden können, ein großzügigeres Assignment jedoch nie ein strengeres Deny auf einem übergeordneten Scope überschreiben kann.

Best Practice ist es, mit Audit/AuditIfNotExists zu beginnen, bevor man auf Enforcement umstellt, Policies auf höheren Scopes zu definieren und auf Child-Scopes zuzuweisen sowie Policy als Code zu verwalten – unter Beachtung fixer Limits wie 500 Definitionen und 200 Initiatives pro Scope.

Validierungsergebnis:

15 Initiativen sowie 24 Zuweisungen und 9 einzelne Richtlinien sind konfiguriert

G02.13 | Medium | Erfüllt

For Sovereign Landing Zone, use Azure Key Vault managed HSM to store your secrets and credentials.

Weitere Informationen: https://learn.microsoft.com/en-us/industry/sovereign-cloud/sovereign-public-cloud/capabilities/external-key-management

Check Description:

Für Sovereignty-Anforderungen erfüllt das Standard-Azure-Key-Vault-Managed-HSM bereits für die meisten Organisationen selbst strenge regulatorische Vorgaben, da es FIPS-140-3-Level-3-validierte Hardware, Single-Tenant-Isolation und eine kundengesteuerte Security Domain bietet, die alleinige administrative Kontrolle gewährleistet, obwohl Microsoft die zugrunde liegende Infrastruktur betreibt.

Verwenden Sie Azure Key Vault Managed HSM als Standard-Sovereignty-Control für Secrets und Credentials in einer Sovereign Landing Zone, ohne den operativen Aufwand für den Betrieb physischer HSM-Hardware.

Nur für die kleinere Gruppe von Organisationen mit einer zwingenden rechtlichen oder vertraglichen Anforderung, dass Schlüsselmaterial die von Microsoft betriebene Infrastruktur überhaupt nicht berührt, sollte die Preview-Funktion External Key Management (EKM) in Betracht gezogen werden, bei der der eigentliche Key über einen vom Kunden betriebenen EKM-Proxy auf einer kundengesteuerten HSM außerhalb von Azure verbleibt.

EKM tauscht Verfügbarkeit, Performance und operative Einfachheit gegen physische Schlüsselkontrolle ein und sollte als letztes Mittel betrachtet werden, nicht als generelles Upgrade gegenüber dem Standard-Managed-HSM.

Validierungsergebnis:

Keine Sovereign Landing Zone notwendig.

Dieser Musterreport gibt Ihnen einen Einblick in Aufbau und Inhalt unserer Analysen.

Die oben genannten Checks sind beispielhaft ausgewählt.

Unser vollständiges Portfolio umfasst über 250 Prüfungen, die im Rahmen einer tatsächlichen Analyse individuell auf Ihre Umgebung abgestimmt werden.

2 Ausgeschlossene Checks

Die folgenden 108 Checks wurden für diesen Kunden bewusst ausgeschlossen (Not Applicable) und fließen daher nicht in Score, KPIs oder die Bewertungstabellen der Management Summary ein.

ID	Severity	Kategorie	Anforderung
A03.01	Medium	Azure Billing and Microsoft Entra ID Tenants	Set up a Notification Contact email address to ensure notifications are sent to an appropriate group mailbox.
A03.02	Low	Azure Billing and Microsoft Entra ID Tenants	Use departments and accounts to map your organization's structure to your enrollment hierarchy which can help with separating billing.
Und weitere Checks			