Data#3

Azure Health Check Summary
Contoso Corporation

Please note: the data provided in this report is sample only and should be treated as such.

Release Date: 30 March 2020

Contents

Next Step Recommendations

Identity

1.1 Azure Active Directory licensing model

Azure Active Directory is available under 4 offers: -

- Free
- Basic
- Premium 1
- Premium 2

This check looks at the current licensing offer for Azure Active Directory (Azure AD) and based on the organisation type and risk profile a recommendation is created to ensure that Security from an Identity perspective is maintained by enabling advanced protection features where required.

For more information on the services that are available under P1 and P2 then refer to https://azureperiodic.data3.com.au/Assets/Azure AD-Licencing.jpg.

1.1.1 Current State

Contoso is currently using the Premium 2 model for Azure AD.

1.1.2 Recommendations

No recommendation available.

1.1.3 Next Steps

Item Number	Resolution

Table 1 Azure Active Directory licensing model

1.2 At Risk Users

Identity protection is a critical security focus for Azure and Office 365, Azure AD provides built-in mechanisms to protect and report on account breaches. Depending on the licensing model of Azure AD it is possible to fully protect identities using advanced machine learning based analytics.

Users at Risk reporting is a native function that is available with all licensing models, however the details for why a user is marked for risk is only available under P1 or P2.

This check looks at the current list of at-risk users and focuses on users that have a high impact such as accounts with key words such as Invoicing, Payable, Receiving, Sales, C level and Admin named accounts.

1.2.1 Current State

Out of the 21194 users within the Azure AD Tenant, 2287 are marked at risk, a full report has been attached below.

1.2.2 Recommendations

Implement Conditional Access Risk based policy to automatically protect users that are at High Risk.

A significant level of risk events was detected for multiple high impact user accounts. Data#3 strongly recommend immediate resolution of these events and deploy Azure Sentinel to provide advanced reporting and protection from future risk events - https://azure.microsoft.com/en-us/services/azure-sentinel.

1.2.3 Next Steps

Item Number	Resolution
2.1	Remediate Risk Detections.
2.2	Enable and configure Azure Sentinel.

Table 2 At Risk Users

1.3 On-Premises Identity configuration

A critical component of Azure is the relationship between Active Directory and Azure Active Directory. AADConnect is a service that establishes a sync or trust relationship between AD and Azure AD. This check reviews the configuration of AADConnect.

1.3.1 Current State

- Federation = True
- Password Hash Sync = False
- Passthrough Auth = False
- Seamless Single Sign-on = False

1.3.2 Recommendations

If federation is only being used for Microsoft authentication then significant benefits could be achieved by switching to modern auth options such as Password hash sync, Seamless SSO and Passthrough authentication.

1.3.3 Next Steps

Item Number	Resolution
3.1	Review current AADConnect settings and enable modern auth

Table 3 On-Premises Identity Configuration

1.4 Self Service Password Reset

Azure Self Service Password Reset (SSPR) is a feature of Azure AD that allows users to manage their password from any device, at any time, from any location, while remaining in compliance with defined security policies. Azure AD Password Reset allows users to change their expired or non-expired passwords and reset forgotten password.

Azure AD connect provides a connection between on premise Active Directory Services and Azure Active Directory. This connection can replicate a hashed password between the two directories. When configured with Password Writeback, users can self-manage their own password and lower the operational overhead of a service desk.

Azure Self Service Password Reset can be accessed directly from the following URL: https://passwordreset.microsoftonline.com/.

1.4.1 Current State

SSPR is current configured as follows: -

- SSPR Enabled Users = Selected groups
- Number of reset methods = 1
- Methods available
    - Mobile App = No
    - Mobile app code = Yes
    - Email = No
    - Mobile Phone = Yes
    - Office Phone = No
    - Security Questions = No
- Notify Users on password reset = Yes
- Notify all admins when other admin reset their password = No

A score system is used to evaluate the overall security and useability of SSPR based on certain options. Out of a max potential of 23 points the current score is 19.

1.4.2 Recommendations

Data#3 recommends enabling admin notifications.

1.4.3 Next Steps

Item Number	Resolution
4.1	Enable SSPR admin notifications

Table 4 Self Service Password Reset

1.5 Conditional Access

Conditional Access Policy (CAP) allows an organisation to dynamically protect identities based on criterial and conditions for log on, such as: -

- Who you are?
- What group you are in?
- Where you are?
- What you are trying to access?
- What are you using?

- When and where did you last authenticate?

CAP extends the authentication experience by evaluating these conditions and determines what to do in the event that one or more of these conditions are not acceptable.

CAP is available under Azure AD P1 and is greatly enhanced with P2 by providing “Risk” based evaluation. For Free and Basic versions of Azure AD there are baseline policies that can be used to protect Administrative accounts.

1.5.1 Current State

Contoso is licensed for P2 and can use conditional access policy. Some custom policies were detected however it appears that they are in a testing stage.

1.5.2 Recommendations

Although support for enabling Conditional Access Policy is not available due to the Azure AD Licencing model, it is recommended to review and enable the baseline policies to protect assigned admin privileges.

1.5.3 Next Steps

Item Number	Resolution
5.1	Strengthen current conditional access policies
5.2	Implement risk-based policies

Table 5 Conditional Access

Security

2.1 Security Centre Coverage

Azure Security Centre (ASC) provides unified security management and advanced threat protection for workloads running in Azure, on-premises, and in other clouds. It delivers visibility and control over hybrid cloud workloads, active defences that reduce your exposure to threats, and intelligent detection to help you keep pace with rapidly evolving cyber attacks.

Security Centre is offered in two tiers:

The Free tier is automatically enabled on all Azure subscriptions and provides security policy, continuous security assessment, and actionable security recommendations to help organisations protect Azure resources.

The Standard tier extends the capabilities of the Free tier to workloads running in private and other public clouds, providing unified security management and threat protection across hybrid cloud workloads. The Standard tier also adds advanced threat detection capabilities, which uses built-in behavioural analytics and machine learning to identify attacks and zero-day exploits, access and application controls to reduce exposure to network attacks and malware. The Standard tier is free for the first 30 days.

This check reviews the Security Centre tier and coverage across subscription(s).

2.1.1 Current State

Contoso is currently using the free tier of ASC.

2.1.2 Recommendations

Data#3 recommends stepping up to ASC Standard for all resource types and enable Azure Sentinel to dramatically enhance security reporting and insights for Azure resources https://azure.microsoft.com/en-us/services/azure-sentinel.

2.1.3 Next Steps

Item Number	Resolution
6.1	Enable ASC Standard tier for all Subscriptions
6.2	Integrate with Azure Sentinel

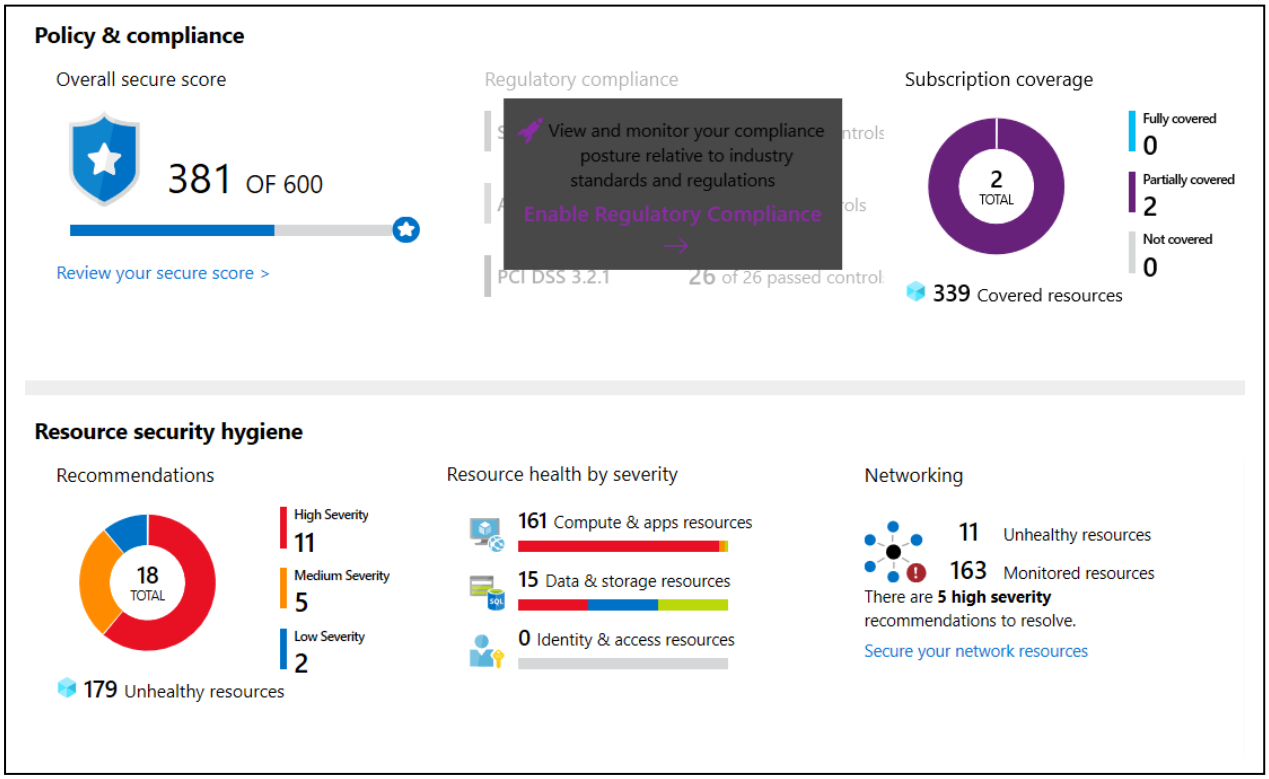
Table 6 Security Centre Coverage

2.2 Security – Current Threats

This check summarises current live security issues being reported by Security centre (if available).

2.2.1 Current State

The below images show active security issues.



Recommendation	Secure Score I...	Failed Resources	Severity
Vulnerability assessment solution should be installed on your virtual machines	+30	136 of 156 virtual machines	
Vulnerabilities in security configuration on your machines should be remediated	+30	74 of 156 virtual machines	
System updates should be installed on your machines	+26	77 of 156 virtual machines	
API App should only be accessible over HTTPS Quick Fix!	+20	1 of 1 API apps	
Endpoint protection health issues should be resolved on your machines	+14	81 of 156 virtual machines	
Disk encryption should be applied on virtual machines	+10	136 of 156 virtual machines	
Management ports should be closed on your virtual machines	+10	1 of 1 virtual machines	
Monitoring agent health issues should be resolved on your machines	+9	46 of 156 virtual machines	
Monitoring agent should be installed on virtual machine scale sets Quick Fix!	+8	1 of 4 virtual machine scal...	
Install endpoint protection solution on virtual machines	+6	64 of 156 virtual machines	
Web ports should be restricted on NSG associated to your VM	+0	3 of 156 virtual machines	
All network ports should be restricted on NSG associated to your VM	+0	2 of 156 virtual machines	
Your machines should be restarted to apply system updates	+0	2 of 156 virtual machines	
Network traffic data collection agent should be installed on Windows virtual machines (Preview) Quick Fix!	+0	1 of 1 virtual machines	

2.2.2 Recommendations

Data#3 urgently advise Contoso to investigate and address these active security issues.

2.2.3 Next Steps

Item Number	Resolution
7.1	Remediate Security Alerts

Table 7 Security – Current Threats

2.3 Break Glass Accounts

Break glass accounts can help organisations restrict privileged access within an existing Azure Active Directory environment. Such accounts are highly privileged, and they are not assigned to specific individuals. Emergency access accounts are limited to emergency or 'break glass' scenarios, situations where normal administrative accounts cannot be used. Organisations must maintain a goal of restricting the emergency account's usage to only that time during which it is necessary.

An organisation might need to use an emergency access account in the following situations:

- The user accounts are federated, and the federation is currently unavailable because of a cell-network break or an identity-provider outage. For example, if the identity provider host in your environment has gone down, users might be unable to sign in when Azure AD redirects to their identity provider.
- The administrators are registered through Azure Multi-Factor Authentication, and all their individual devices are unavailable. Users might be unable to complete Multi-Factor Authentication to activate a role. For example, a cell network outage is preventing them from answering phone calls or receiving text messages, the only two authentication mechanisms that they registered for their device.
- The person with the most recent global administrative access has left the organisation. Azure AD prevents the last global administrator account from being deleted, but it does not prevent the account from being deleted or disabled on-premises. Either situation might make the organisation unable to recover the account.

There should be two ’break glass’ accounts and they should be cloud-only accounts that use the *.onmicrosoft.com domain and that are not federated or synchronised from an on-premises environment.

The accounts should not be associated with any individual user in the organisation. Organisations need to ensure that the credentials for these accounts are kept secure and known only to individuals who are authorised to use them.

An account password for an emergency access account is usually separated into two or three parts, written on separate pieces of paper, and stored in secure, fireproof safes that are in secure, separate locations.

2.3.1 Current State

There are no accounts that conform to the 'break glass' configuration.

2.3.2 Recommendations

Data#3 recommend implementing break glass accounts and implement Privileged Identity Management (PIM).

2.3.3 Next Steps

Item Number	Resolution
8.1	Implement break glass accounts

Table 8 Break Glass Accounts

2.4 Admin permissions

Role Based Access Control (RBAC) is critical to ensure that Azure resources and organisation data are protected and governed appropriately. Least privileged access models reduce the risk impact and surface area damage if an individual account is compromised. No single user account should ever have full rights to every resource in Azure (excluding 'break glass' accounts)

Azure contains role-based groups for non-top-level functions that should be used in place of the Global Admin (GA) role as well as subscription level roles to perform isolated administrative tasks. There exists a third level of access control with Resource Groups that should always be used to provide granular access to collections of resources.

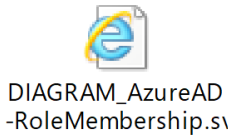
Under no circumstances should day to day accounts be used for Azure administration as the risk profile for these types of accounts is dramatically higher than dedicated restricted and locked down accounts.

2.4.1 Current State

Refer to the below attached list of privileged role membership for Azure AD.

Service accounts (based on naming convention) were detected in one or more admin roles and access permissions should be reviewed for these accounts and Discretionary Access Controls (DACL) implemented to grant the permissions that the accounts require rather than adding them to a top-level admin role.

Day to day named user accounts were detected and based on the level of access these accounts present a significant risk to the organisation. A large number of service accounts with high levels of access was detected.


DIAGRAM_AzureAD -RoleMembership.sv


REPORT_All-Privileged-Roles.csv

2.4.2 Recommendations

Review the Role membership and restrict access to the high privilege roles as appropriate, Implement Resource Group level delegation of access to minimise the potential attack surface area for a compromised account.

Turn on multi-factor authentication and register all other highly-privileged single-user non-federated admin accounts. Note, highly-privileged should also extend to accounts that can have a financial impact on the organisation (Accounts Payable, Accounts Invoicing for example).

Require Azure Multi-Factor Authentication (MFA) at sign-in for all individual users who are permanently assigned to one or more of the Azure AD admin roles:

- Global administrator
- Privileged Role administrator
- Exchange Online administrator
- SharePoint Online administrator

2.4.3 Next Steps

Item Number	Resolution
9.1	Limit global admin role to break glass accounts
9.2	Review and restrict service account rights
9.3	Strengthen Conditional Access Policies to enforce MFA for Admin roles

Table 9 Admin Permissions

Resource Configuration and Governance

3.1 Classic Resources

Azure Classic resource deployments otherwise known as Azure Service Manager (ASM) were depreciated in 2017 with the classic Azure portal removed in January 2018. Azure currently supports the operation and deployment of Classic VNETS\Virtual Machines and Storage Accounts. However, new deployments should utilise the current deployment methodology of Azure Resource Manager (ARM).

3.1.1 Current State

No classic resources were detected.

3.1.2 Recommendations

N/A

3.1.3 Next Steps

Item Number	Resolution

Table 10 Classic Resources

3.2 Resources outside of Australia

Certain organisations are required to maintain border of sovereignty for Azure hosted workloads and data.

This check reviews all resources and reports on resources that are not deployed within the 4 available Australia Datacenters.

- Australia East (Sydney)
- Australia Southeast (Melbourne)
- Canberra 1 (Canberra)
- Canberra 2 (Canberra)

3.2.1 Current State

Refer to the attached summary for resources that are currently running outside of the Four Australian Datacenters, this list excludes global services such as Azure AD.

REPORT_All-Non-Australian.csv

3.2.2 Recommendations

Data#3 can assist Contoso with resource evaluation of services outside of Australia and co-ordinate a planned relocation of resources.

3.2.3 Next Steps

Item Number	Resolution
11.1	Review resources outside of Australia and relocate to AU region

Table 11 Resources outside of Australia

3.3 Un-Tagged Resources

Tagging resources in Azure is mission critical and ensures that deployments are managed effectively. Tagging comprises of Key Pair identifiable metadata that should be assigned to every resource in Azure, at a minimum the following rules should be applied to each resource: -

- What this is?
- What is it for?
- Who owns it?
- Who pays for it?
- What is its development status?

Ultimately tagging allows for accountability, programmatic action, resource governance and cost management. An example of this is if every resource is tagged appropriately then an Automation Runbook can be used to enumerate all resources that are not tagged as “Production” and stop\resize\de-allocate after hours to optimise cost.

This check enumerates all resources and provides a tag effectiveness percentage.

3.3.1 Current State

Contoso appear to be utilising tags, however the total number of tagged resources is 1770 out of 2069.

The below table lists the total Tag percentage for each subscription.

Subscription Name	Number of Resources	Tagged Count	Percentage
Contoso-Core-Services-Prod	2025	1735	86
Contoso-Info-Mgmt-PROD	44	35	80

3.3.2 Recommendations

Data#3 can assist Contoso with the design and deployment of an effective tagging methodology, remediate current missing tags and setup subscription policies to enforce future tag application.

3.3.3 Next Steps

Item Number	Resolution
12.1	Design Tag Policy requirements
12.2	Implement Tagging policy
12.3	Remediate missing tags

Table 12 Un-Tagged Resources

3.4 Subscription Policies

Policies play a key role in the long-term control and governance application of Azure resources. Many aspects of this health check can be neutralised via policies.

For example, if this check revealed resources outside of Australia then the “Allowed Locations” policy would have prevented those deployments by applying forced control over where resources can be deployed.

Another valid example is “Allowed Resource Types”, if there will never be a need to deploy the current largest VM (m208 vm with 208 cores and 5.7 Terabytes of memory) then that can be removed from the allowed list.

3.4.1 Current State

Contoso is currently partially using policies to control certain aspects of resource deployments.

3.4.2 Recommendations

Data#3 strongly suggest designing an organisation governance model for Azure and deploying a suitable policy hierarchy to support the long-term usage of Azure.

3.4.3 Next Steps

Item Number	Resolution
13.1	Design Policy structure (Governance model)
13.2	Remediate policy compliance on subscriptions

Table 13 Subscription Policies

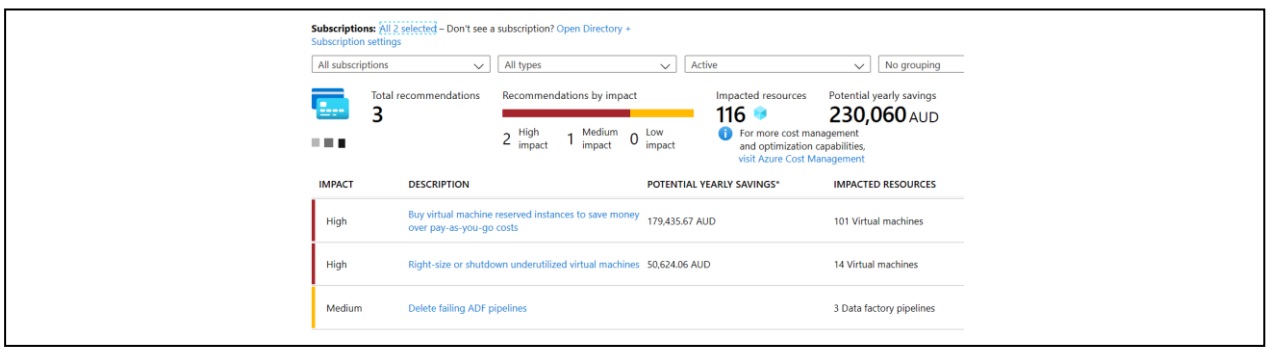
3.5 Reserved Instance Application

Reserved instances (RI) can provide a significant discount over pay-as-you-go prices. With reserved instances, organisations can pre-purchase the base costs for virtual machines, SQL Managed Instances and Application Service Environment.

Discounts will automatically apply to new or existing applicable services that have the same size and region as the RI.

3.5.1 Current State

RI Cost saving opportunities are available: -



3.5.2 Recommendations

Data#3 can work with Contoso to decide where and how RI can be applied to optimise resource cost usage over a three-year term.

3.5.3 Next Steps

14.1	Implement cost saving recommendations

Table 14 Reserved Instance Application

3.6 Azure Hybrid Use Benefit

Azure Hybrid Use Benefit (AHUB) allows an organisation to extend Windows Server\Client and SQL on-premises licensing into Azure.

AHUB is available to organisations who own eligible SQL Server and/or Windows Server licenses with active Software Assurance or the equivalent qualifying subscription licenses below: -

- Windows Server Datacenter edition with Software Assurance
- Windows Server Standard Edition with Software Assurance
- SQL Server Enterprise Core with Software Assurance
- SQL Server Standard Core with Software Assurance

This check looks at the current VM deployments and if the deployments are ARM based, Windows Operating system and not deprovisioned then eligible VMs are listed here.

Important note, this check looks at the current application of AHUB and does not factor in eligibility from a licensing perspective.

3.6.1 Current State

Refer to the reference document here for a full list of VMs that are eligible for AHUB.

3.6.2 Recommendations

Contoso currently operate in a sub optimal manner and further cost saving opportunities could be realised if AHUB is fully applied to eligible workloads.

Contoso currently cannot apply AHUB to several workloads due to ASM resource type deployments, these resources will need to be migrated to ARM prior to AHUB application.

3.6.3 Next Steps

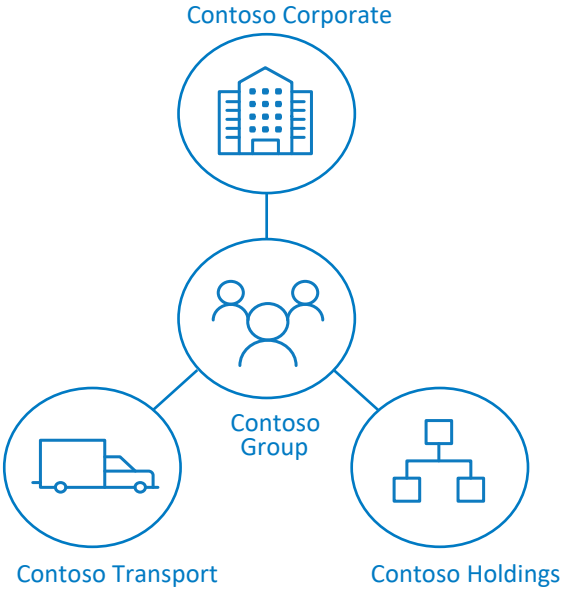
Item Number	Resolution
15.1	Enable Azure Hybrid Use Benefit where eligible

Table 15 Azure Hybrid Use Benefit

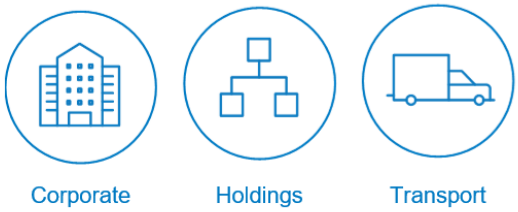
3.7 Tenant\Subscription Topology

Azure Tenant and Subscriptions should map to the Organisation hierarchy for ease of management and portability of infrastructure.

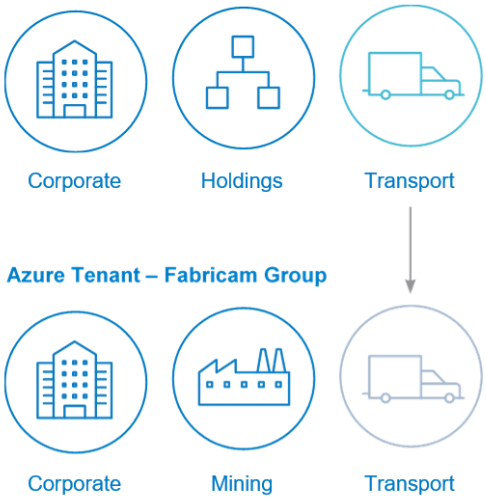
For example, using a fake company as a reference. Contoso Group is made up of 2 discreet business units with a governing unit sitting on the top



A recommended Subscription model would be as follows. This model allows for core shared applications to be hosted and shared from the Corporate Subscription. Each of the other two lines of business can deploy their infrastructure within each of their subscriptions.



The Major benefit of this topology is that if the group sold off a line of business to another organisation, then the entire subscription can be detached and move to the new incumbent.



This methodology applies to Governmental Departments as well. Machinery of Government changes can be extremely expensive. Migrating infrastructure from Department A to Department B requires a large amount of planning and effort and the ability to detach and attach an entire subscription dramatically simplifies this process.

3.7.1 Current State

Contoso operate within a single Tenant and is licensed under Azure AD Premium 2.

Contoso operate within a multiple Subscription topology with DEV | TEST | PROD named workloads, the subscription offer is EA.

Subscription name	Subscription ID	My role	Current cost
		Reader	A$6,727.51
		Reader	A$88,135.47

3.7.2 Recommendations

It is recommended that Contoso complete a planning workshop to gain an understanding of how they control subscriptions and which layout best fits their end goals. Further cost saving opportunities exist by establishing an EA Dev\Test subscription for non-production workloads.

3.7.3 Next Steps

Item Number	Resolution
16.1	Review Subscription topology
16.2	Implement EA Dev\Test

Table 16 Tenant\Subscription Topology

Summary of Next Steps

The below table list the summary of next steps that Contoso should review and action via Data#3 Professional or Managed Services. Where possible a priority has been included to focus on the high impact recommendations based on Data#3's extensive experience with managing organisations in Azure.

To reduce the response time for Data#3 to provide a proposal to work through the findings select the Yes box next to each item and send this page to your account representative or sales specialist.

Item Number	Resolution	Data#3 Engagement?
2.1	Remediate Risk Detections.	☐ - Yes
2.2	Enable and configure Azure Sentinel	☐ - Yes
3.1	Review current AADConnect settings and enable modern auth	☐ - Yes
4.1	Enable SSPR admin notifications	☐ - Yes
5.1	Strengthen current conditional access policies	☐ - Yes
5.2	Implement risk-based policies	☐ - Yes
6.1	Enable ASC Standard tier for all Subscriptions	☐ - Yes
6.2	Integrate with Azure Sentinel	☐ - Yes
7.1	Remediate Security Alerts	☐ - Yes
8.1	Implement break glass accounts	☐ - Yes
9.1	Limit global admin role to break glass accounts	☐ - Yes
9.2	Review and restrict service account rights	☐ - Yes
9.3	Strengthen Conditional Access Policies to enforce MFA for Admin roles	☐ - Yes
11.1	Review resources outside of Australia and relocate to AU region	☐ - Yes
12.1	Design Tag Policy requirements	☐ - Yes
12.2	Implement Tagging policy	☐ - Yes
13.1	Design Policy structure (Governance model)	☐ - Yes
13.2	Remediate policy compliance on subscriptions	☐ - Yes
14.1	Implement cost saving recommendations	☐ - Yes
15.1	Enable Azure Hybrid Use Benefit where eligible	☐ - Yes
16.1	Review Subscription topology	☐ - Yes

16.2	Implement EA Dev\Test	☐ - Yes