Portfolio of Work : Statement of Work

Note: Contents have been deleted. This is not a full version of the document.

Prepared for

TechT NZ

Date: December 2024

_____

Prepared by

Zero-Trust Interface

Author: Jean-Philippe LO SIOU

Version: 1.0

CONTENTS

Table Contents....4
Figure Contents....5
Document Control....5
Stakeholders & Audience....5
Introduction....7
Executive Summary....7
Key analysis....7
Company Background....8
Business Analysis....9
Current State – Discovery....9
Network Infrastructure....9
Existing Server Environment....10
Existing End User and Other Devices....10
Stakeholder Feedback – Analysis....11
Identified Requirements....15
Moscow Analysis....17
Project Requirements....19
Problem/Solution Overview....19
Technical Solutions Details....22
Identity and Access....22
1. Microsoft Tenant....22
2. Microsoft Entra ID....22
3. Microsoft Licenses....23
4. Azure Subscription....23
5. Implementing Identity Synchronization: Microsoft Entra Connect Sync....24
6. Manage Secure User Access....25
6.1. Identity Access Management (IAM)....25
6.2. Azure Role Based Access Control (RBAC)....25
6.3. Multi-Factor Authentication (MFA) Registration Policy (Azure | Microsoft 365)....26
6.4 Conditional Access Policy (Azure | Microsoft 365)....26
6.5 Privileged Identity Management (PIM) Administrator Approval (Microsoft 365)....26
Scalabilities Challenges....27

1. Azure Public & Private DNS....27
2. Azure Regions & Azure Availabilities zone....27
3. Azure Private Virtual Network & Azure Private Network Local Peering....27
4. Azure Resources group....28
4.1. Web Application....28
4.1.1. Azure Storage Account....28
4.1.2. Azure Service Plan & Azure Web Apps....28
4.1.3. Azure Web App Service....28
4.1.4. Azure Front Door....28
4.2. Database....29
4.2.1 Microsoft Azure SQL Database....29
5. Microsoft 365....29
5.1. Fileshare to OneDrive/SharePoint....29
5.2. SharePoint Server To Microsoft 365....30
5.2.1. SharePoint Migration tool (SPMT)....30
5.3. Microsoft Exchange to Microsoft 365....31
5.3.1. Microsoft Exchange Online....31
Security Vulnerabilities....31
1. Network Security Group & Application Security Groups....31
2. Azure Web Application Firewall....31
3. Azure DDoS Protection....31
4. Azure Role Base Access Control (RBAC)....31
Costing Analysis....32
Current Financial....32
CAPex....32
OPex....34
CAPex+OPex....35
Revenue & Profit....36
Project : Delta Cloud | Modern Workplace....37
CAPex....37
OPex....44
CAPex+OPex....45
Budget....45
Result 2024 / Project....46

Timeline 47
Project Roadmap Gantt Chart 47
Change Control 48
ITIL SVS/SVC 48
Change Approval 50
Approval Form 50
Reference List 52
Appendix 53
Execution Phase 3 : Migrate Applications to fix scalabilities issues (SupportDesk and XYZ Payroll Manager) to Azure Service Plan 53
Microsoft 365 53
FileShare to OneDrive/SharePoint 53
Microsoft Exchange Online 54

TABLE CONTENTS

Table 1 Current State | Network Infrastructure 9
Table 2 Current State | Server Environment 10
Table 3 Current State | End User And Other Devices 10
Table 4 MoSCoW Analysis 18
Table 5 Costing Analysis | Current Financial 2024 | CAPex | Estimate 33
Table 6 Costing Analysis | Operating Expenses (OPex) | Estimate 34
Table 7 Costing Analysis | Current Financial 2024 | CAPex + OPex 35
Table 8 Current Financial | CAPex | Revenue from 2018 | Estimate 36
Table 9 Current Financial | CAPex | Result from 2018 | Estimate 36
Table 10 Costing Analysis | Current Financial 2024 | Revenue Estimate 36
Table 11 Costing Analysis | Current Financial 2024 | Result Estimate 36
Table 12 Costing Analysis | Project : Delta Cloud | Modern Workplace | CAPex | Estimate 38
Table 13 Costing Analysis | Capital Expenditure (CAPex) Detail - Microsoft Azure Estimate 43
Table 14 Costing Analysis | Capital Expenditure (CAPex) Detail - Microsoft 365 Estimate 43
Table 15 Costing Analysis | Project : Delta Cloud | Modern Workplace | OPex | Estimate 44
Table 16 Costing Analysis | Project : Delta Cloud | Modern Workplace | Total CAPex + OPex 45
Table 17 Costing Analysis | Project : Delta Cloud | Modern Workplace | Budget Provisioned 45
Table 18 Costing Analysis | Project : Delta Cloud | Modern Workplace | Budget Provisioned / Estimate cost project 45

Table 19 Costing Analysis | Project : Delta Cloud | Modern Workplace | Estimate Result 2024 / Estimate cost project 46
Table 20 Gantt Chart 47
Table 21 Service Value Chain 48
Table 22 Approval Form Detail 50
Table 23 Approval Form Detail | Change 50
Table 24 Approval Form Detail | Impact 50
Table 25 Approval Form Detail | Deliverables 51
Table 26 Approval Form Detail | Key Stakeholder Sign Off 51

FIGURE CONTENTS

Figure 1 Azure Subscription - Management Groups (Mumian, 2024) 23
Figure 2 Entra Connect Sync implementation 25
Figure 6 ITILv4 - Service Value Chain (ref. More detail) 49
Figure 7 Migrate Applications to fix scalabilities issues (SupportDesk and XYZ Payroll Manager) to Azure Service Plan 53
Figure 8 What content goes where | Fileshare , OneDrive and SharePoint (MicrosoftHeidi, 2024a) 53
Figure 9 What content goes where | Windows Permissions / SharePoint (MicrosoftHeidi, 2024a) 54
Figure 10 Microsoft 365 | Exchange Online (Workflow) (more detail) (RobBagby, 2024) 55
Figure 11 Microsoft 365 | Exchange Online (Workflow) Details (RobBagby, 2024) 56

DOCUMENT CONTROL

Date	Author	Ver	Comments
01/11/2024	Jean-Philippe LO SIOU	0.1	First Drafts
11/11/2024	Jean-Philippe LO SIOU	0.2	First Release
12/11/2024	Jean-Philippe LO SIOU	0.3	Various Minor Updates - Change Solutions details
14/11/2024	Jean-Philippe LO SIOU	0.4	Various Minor Updates – Update Cost
02/12/2024	Jean-Philippe LO SIOU	1.0	Final Release

STAKEHOLDERS & AUDIENCE

The Audience for this document is:

- Operation Manager
- CIO
- IT Teams:
    - IT Team Lead
    - IT Director
    - Solution Architects
    - SME
- Stakeholders
- Other interested parties

List of Stakeholders involved:

Name	Title	Project Role	Detail
Jean-Philippe Lo Siou	Project Lead	Project Lead	Ownership of Project Delivery
Mike Spencer	C.E.O		Steering and Oversight
Joseph Jeong	IT Coordinator	Project Coordinator	
Abigail Mars	Network Administrator	Project Team Member	
Leah Bucknell	Business Analyst	Steering Committee	

INTRODUCTION

EXECUTIVE SUMMARY

This Statement of Work (SOW) with any appendices and attachments to it outlines the business analysis, project requirements, and technical solutions details for the Delta Cloud project, the terms of which are incorporated herein by reference, by and between TechT New Zealand (“TTNZ”) (“Customer”, “you”, “your”) and Zero-Trust Interface (“ZTI”, “us”, “we”, “our), and sets forth the services to be performed by us related to Delta Cloud Deployment (“project”).

This SOW represents the complete baseline for services and acceptance applicable to this project.

The objective of this project is to propose and deliver cloud-based migration strategy by resolving issues raised with the existing on-premises solution and explained in detail in the Business Requirement Section of this project. It is aim to address issues regarding the Identity and access management, the scalability struggles to keep with growing demands, the device and application management, an enhanced and responsive threat intelligence solution for security infrastructure and data privacy while being compliant with legislative compliance.

The project will provide benefits including a central management for devices and users, an advanced protection against cyber threats by leveraging AI and ensuring alignment with TTNZ expectations regarding reducing operational risks and compliant with regulatory law.

KEY ANALYSIS

TTNZ is a medium sized business with approximately 500 end users and workstations. Their head office is based in Auckland with approximately 250 end-user devices (100 Workstations, 150 laptops) and they have a Wellington Branch with approximately 120 end-user devices (50 Workstations, 70 laptops) and a Christchurch branch with approximately 50 end-user devices (20 Workstations, 30 laptops)

TechT NZ is a retail and wholesale group within NZ” All things Tech”. They are supplying several retailers.

COMPANY BACKGROUND

ZTI was founded in 2005 helping New Zealand businesses to get the support, technology and expertise they need to tackle the digital transformation.

Our area of expertise are:

- Defining a clear Technology Strategy
- Manage Cyber security Risk
- Implement Disaster Recovery Plan
- Control their tech project costs
- Help on the IT Support
- Meet the Modern Workplace
- Transform your environment into the Cloud

Our expertise is Cloud Management, we successfully completed a migration over on-premises to the cloud for the “Cinema NZ”. Our team is trained with different cloud provider, project management and implementation of a good Disaster Recovery solution to ensure we meet the highest technical and regulatory standards.

Our testimonials from our clients: https://www.zero-trust-int.co.nz/testimonials

BUSINESS ANALYSIS

CURRENT STATE – DISCOVERY

The on-premises infrastructure is provided as follows:

NETWORK INFRASTRUCTURE

Office Location	WAN Connection Type - Fibre Link Speed	Routers/Firewall	Managed Switches	Unmanaged Switches	Wi-Fi 6 - Access Points	Cabling	Network(s)	Comments
Auckland	SD WAN 2x 5gbps Connection High Availability - Failover Enabled	2x FortiGates HA Active-Active	8x 48 Port Switches - 4x VLANs (Stacked on Main Office Floors)	16x 24 Port Switches	16x Total - Across Floors	CAT6a	172.16.0.0/19 10.0.0.0/20	VLANs & DHCP Config; Servers, Wired, Wireless APs & Critical Workloads
Wellington	WAN Connection 1x 5gbps Connection	1x FortiGate	4x 48 Port Switches - 3x VLANs	10x 24 Port Switches	10x Total - Across Floors	CAT6a	172.15.0.0/19	VLANs & DHCP Config; Servers, Wired, Wireless
Christchurch	Starlink WAN Connection 1x 5gbps Connection	1x FortiGate	2x 48 Port Switches - 3x VLANs	6x 24 Port Switches	6x Total - Across Floors	CAT6a	172.14.0.0/19	VLANs & DHCP Config; Servers, Wired, Wireless

Table 1 Current State | Network Infrastructure

- "They use Fortinet Devices on their networking infrastructure"
- "The above inventory is available but some of them are not used because on floor configuration and number of employees."

EXISTING SERVER ENVIRONMENT

Office Location	Domain Controllers	SQL Servers	Exchange Servers	SharePoint Servers	WDS Servers	File Servers	IIS Servers	Backup Servers	Monitoring and Logging Servers	Total
Auckland	2x	4x	1x	1x	1x	2x	2x	2x	2x	17
Wellington	2x	1x	1x	1x	1x	1x	1x	1x	1x	10
Christchurch	2x	1x	1x	0x	1x	1x	0x	1x	1x	8
Total	**6**	**6**	**3**	**2**	**3**	**4**	**3**	**4**	**4**	**35**

Table 2 Current State | Server Environment

EXISTING END USER AND OTHER DEVICES

Office Location	Desktop Workstations	Staff Laptops	Total Est End-User Devices	Smartphones Android	Smartphone IOS	Total Est Handheld devices	Other IoT Devices
Auckland	100x	150x	250 Est	150x Est	100x Est	250 Est	20x Est
Wellington	50x	70x	120 Est	35x Est	25x Est	60 Est	10x Est
Christchurch	20x	30x	50 Est	25x Est	15x Est	40 Est	10x Est
		Total Est	**420 Est**			**350 Est**	

Table 3 Current State | End User And Other Devices

- ”They provide a $1200 grant to new employees to enable them to purchase a Mobile Device”
- ”Other IoT Devices are: Tablets, Kiosk(s), TVs, Touch Screens, Projectors, Fridges and more. ”

STAKEHOLDER FEEDBACK – ANALYSIS

#	Question	Answer
Q01	*“Which Apps and licenses are TTNZ currently using ?”*	• *”*TTNZ currently has multiple legacy applications: • XYZ *Payroll Manager* • *Skype for business* • *Office 2013 ”* *”Additionally, the legacy services and apps hosted through their on-premises infra”*
Q02	1- *”What does TechTNZ do ? ”* 2- *”In which field TechTNZ are specialized ? ”* 3- *”What is TechTNZ budget for the project ? ”* 4- *”Are they any other requirements from other stakeholder / department ? ”*	1-*”*TechT a retail and wholesale Group within New Zealand's "all things Tech" sourcing and supplying for several retailers within the country, under the brand "TechT New Zealand", Additionally they manage much of the "Groups" Tier 1-2 IT Support, in house! ” 2-"Everything Tech", and In-house/group Tier 1-2 Support, relevant information is above in #1 3- *”*The budget is not defined, the governance team are seeking advice and recommendations for "high-end solutions" to bring the business and output into the modern era, and based on expert advice and recommendation they can be swayed to "approve" the project teams proposed budget*”* *”*I hope this provides some clarity, and direction going forward! ”
Q03	1-*”*What kind of local security measures are in place ? ” 2-*”*What are the demands for legislative compliance ? ” 3-*”*Which apps are experiencing latency ? ”	*”*I will enquire with our wider team as more pertinent information if you may require For now, I can tell you that... TechT security related details and objectives to follow coming weeks... We aim to meet... 2- Legislation surrounding Privacy Act 2020 Compliance surrounding handling of Data and Information 3- From my understanding latency has been stable for the most part... There have occasional distributions with some of our legacy on prem file and email services, mostly around unscheduled restarts, updates and server down time*”*
	1. Are there any concerns moving from onsite to cloud?	1. "that require further analysis and cloud-based solution(s)"

	2. How does the current infrastructure impact the workload? 3. How would TechT prioritize scalability versus cost-efficiency in cloud solutions? 4. What features in cloud security are most critical to TechT? 5. Does TechT have any concerns with the subscription-based pricing?	2. ″Several mentions within case study″ 3. ″You tell us? determine critical workloads? define peak times? assume aspects to drive your ideas and solutions! ″ 4. ″End-to-End protection, Data of any form is CRITICAL″ 5. ″ Balance cost and benefits, these must be discussed, considered analyzed″ ″i.e. Solutions! Please! Collaborate and in combination, the team should be resolving/evolving the current state″
	1. ″Current "Secure access across devices" solution? ″ 2. ″ How old are the current desktop workstations ? ″	1. ″ Secure L2TP VPN for off-site Staff Access to the Domain, Workloads, e.g. Storage Spaces, Distributed Filesystem and more, with Shares, Security and Roles applying somewhat, access controls to groups/users as highlighted in scenario″ 2. ″This varies, not more than 4-5 years old, yet some devices for some staff, at each office location are more modern than others″
	What is the average yearly revenue after tax for TechT and what are their current operational expenditure costs?	Please consider the following to help support your costing analysis I. Salaries for all staff = ? II. Utilities for each office, electricity, water, internet = ? III. Office lease = ? IV. IT Infrastructure e.g. Hardware, Licensing, Subscriptions and more = ? V. Upkeep and maintenance i.e. of everything = ? VI. Total Monthly OPex = $500,000-700,000 Est VII. On average based on Q1 Q2 Q3 2024 (so far this year) Additionally, I can say that the company consistently has been in profit ranging from 10%-15% annually over the past 6 years

<table>
<tr><td>QEXTRA01</td><td>What is the network I.P addressing of the on-premises architecture for the database, application and the access?</td><td>
<table>
<tr><td colspan="3">Address IP Range : 172.16.0.0/19</td></tr>
<tr><td rowspan="3">Auckland</td><td>Access</td><td>172.16.20.0 /24</td></tr>
<tr><td>Database Access</td><td>172.16.21.0 /24</td></tr>
<tr><td>Applications</td><td>172.16.22.0 /24</td></tr>
<tr><td colspan="3">HA Active-Active : 10.0.0.0/20</td></tr>
</table>
<table>
<tr><td colspan="3">Address IP Range : 172.15.0.0/19</td></tr>
<tr><td rowspan="3">Wellington</td><td>Access</td><td>172.15.20.0 /24</td></tr>
<tr><td>Database Access</td><td>172.15.21.0 /24</td></tr>
<tr><td>Applications</td><td>172.15.22.0 /24</td></tr>
</table>
<table>
<tr><td colspan="3">Address IP Range : 172.14.0.0/19</td></tr>
<tr><td rowspan="3">Christchurch</td><td>Access</td><td>172.14.20.0 /24</td></tr>
<tr><td>Database Access</td><td>172.14.21.0 /24</td></tr>
<tr><td>Applications</td><td>172.14.22.0 /24</td></tr>
</table>
</td></tr>
<tr><td>QEXTRA02</td><td>What would be the application that would need to migrate from low to high priority and their infrastructure they are using ?</td><td>
<table>
<tr><th>Applications</th><th>Priority</th><th>Impact</th><th>Servers used</th></tr>
<tr><td>TTNZ -SupportDesk</td><td>Low</td><td>Low</td><td>SQL Server + IIS Servers</td></tr>
<tr><td>XYZ Payroll Manager</td><td>Low</td><td>Low</td><td>SQL Server + IIS Servers</td></tr>
<tr><td>SharePoint</td><td>Medium</td><td>Medium</td><td>SharePoint Servers + SQL Server</td></tr>
<tr><td>File Sharing</td><td>Medium</td><td>Medium</td><td>File Servers</td></tr>
<tr><td>Windows Deployment Services</td><td>Medium</td><td>Medium</td><td>WDS Servers</td></tr>
<tr><td>Microsoft Exchange</td><td>High</td><td>Very High</td><td>Exchange Server</td></tr>
<tr><td colspan="4">Stay on-premises</td></tr>
</table>
</td></tr>
</table>

		ERP Sales | High | Very High | SQL Server + IIS Servers
QEXTRA03	What is the current Backup and Restore plan?	- ”Backup Servers with Veeam Data Backup platform” - ”Network Area Storage ” - ”Veeam Backup replication: twice a day of VMs in off-site1 through” - ”Veeam Backup: backup every day at 10:00PM” - ”Data Retention is 30 days of backup”
QEXTRA04	What is the current security policy in all windows workstation?	”All Windows workstation are built with security policy: • Users cannot install any software that is already provided • Users can only connect to the internet via VPN connection through on-premises internet. ”
QEXTRA05	Are they any periods migration cannot be implemented ?	*“Yes , from the second week of December to second week of January, there is a Change Freeze”*
QEXTRA06	How many Physical servers? Are they some virtualized servers as well ?	*“ They are 4 Physical Servers in each the 3 sites. They hosted Virtual Machines on VMware vSphere”*
QEXTRA07	Where is the fileshare directory located ?	“ \\TTNZ-AKL-FS01\fileshare” “\\TTNZ- WLG--FS01\fileshare” “\\TTNZ- CHC--FS01\fileshare”

IDENTIFIED REQUIREMENTS

"The Operations Manager, and CIO of has raised various issues that affect the current End User environment that require further analysis and need resolution including the following" :

- **« Identity and Access Management »**
    - « Difficulty managing secure access across devices, especially for remote users»
    - « User Groups and Accounts, are provisioned on AD-HOC basis, roles and accounts are cluttered and unorganized»
    - « Need for centralized identity management and access controls is essential»
- **« Scalability Challenges »**
    - « On-prem infrastructure struggles to keep up with growing demands»
    - « Need for scalable, cost-effective cloud-based solutions throughout current state on-prem workloads»
- **« Security Vulnerabilities »**
    - « Local security measures leave gaps in threat detection and response»
    - « Need for advanced protection and cyber defense capabilities»
- **« Device and Application Management »**
    - « Increasing number of devices (desktops, laptops, smartphones) needs centralized management. »
    - « Need for modernized secure device and application management»
- **« Data Governance and Compliance »**
    - «Increasing regulatory demands for security, data privacy, and legislative compliance»
    - «Need for effective solutions to manage sensitive data and ensure compliance more efficiently»
- **« Collaboration and Productivity Tools »**
    - «Inefficiencies in current collaboration between offices»
    - «Need for better integration of software services and streamline day-to-day staff productivity»
- **« Value Added-Proposition(s) »**

- «Interest in using AI products and Services to automate tasks and improve employee productivity»
- «Any other proposed adoption or migration of current workloads to enhance and streamline business operations»

«ZTI proposes a migration to certain aspect of the infrastructure from on-premises to the cloud that allowing to increase the productivity, availability, resiliency».

«As per the in-person meeting with TTNZ before starting the project we have received an in-detail list of what the issues are at TTNZ. This list will require ZTI to work for the customer for 2 months. »

MOSCOW ANALYSIS

#	Requirement	Comment/Solutions	MoSCoW
BR1	"Identity and Access Management"	• For remote users, the managing secure access across devices has been a difficulty. • The users and groups are not stored properly in the Active Directory. • A centralized identity and access management is needed with Azure Active Directory in order to make it standard for controlling the access across devices. • Provision and de-provision users and groups with roles that will reduce manual account creation or on AD-HOC basic and clutter. • Enhanced security with Multi-Factor Authentication (MFA).	**Must-Have**
BR2	"Scalability Challengers"	• Implementation to a scalable cost-effective cloud-based solution to handle growing traffic. • Migrate the essential on-prem applications to Azure cloud to scale automatically based on the workload to meet demands. • Azure hybrid solution with using the existing on-prem licenses in order to be cost-effective.	**Must-Have**
BR3	"Security Vulnerabilities"	• Implementation for an advanced protection, cyber defense capabilities and a centralized monitoring in order to resolve the weak local security in place. • Multi-Factor Authentication in place alongside with Condition Access Policies.	**Must-Have**
BR4	"Device and Application Management"	• Due to the increase of devices (Desktops, laptops, smartphones), a centralized device management solution is required to secure and manage devices and applications (Microsoft Intune)	**Must-Have**
BR5	"Data Governance and Compliance"	• Due to the increase of the regulatory compliance for security, data privacy and legislative compliance, it is required to implement a solution to maintain data privacy and meet regulatory compliance with Microsoft PurView and Compliance Manager. • An effective solution to manage sensitive data and ensure efficient compliance with ongoing regulatory. • Conduct a compliance assessment and audits.	**Must-Have**
BR7	"Value-Added Propositions"	• A Business Continuity and a Disaster Plan recovery need to be in place.	**Must-Have**
BR6	"Collaboration and Productivity Tools"	• Collaboration between Auckland, Wellington and Christchurch offices is not efficient • A better integration with communication tools to deliver a workflow to increase day-to-day productivity. • In order to improve collaboration: Microsoft Teams, SharePoint and OneDrive can be leveraged to increase collaboration and productivity across the three offices.	**Should-Have**
BR2	"Scalability Challenges"	• To have a gradual migration, a hybrid-cloud configuration can be implementing in order to slowly migrate applications from on-premises to Azure.	**Should-Have**
BR3	"Security Vulnerabilities"	• For an enhanced incident management, the implementation of Microsoft Sentinel can be a proactive solution in order to have a threat and responses strategy.	**Should-Have**
BR1	"Identity and Access Management"	• Report and Analytic on user access pattern to get better understanding how they use and be able to secure more.	**Could-Have**

BR7	"Value-Added Proposition"	• Automation tasks with AI in order to enhance productivity and reduce manual repetition tasks.	**Could-Have**
BR6	"Identity and Access Management"	• Additional AI tools in order to improve employee experience. • Help optimize work process across teams with analyzing collaboration pattern by implementing Microsoft Viva Insights.	**Could-Have**
BR8	"Upgrades investment on legacy on-prem infrastructure"	• Large upgrading on-prem Investment in profit for the cloud solutions.	Won't-Have
BR9	"Applications non-compliance with regulatory standard"	• Solutions that are not in compliance with regulatory requirements won't be in the migration to the cloud.	Won't-Have

Table 4 MoSCoW Analysis

PROJECT REQUIREMENTS

PROBLEM/SOLUTION OVERVIEW

Business Requirements	Business Solutions
Identity and user management *TTNZ user groups and account's (on-premise active directory) are cluttered and unorganized, their users need to be synchronized to the Azure Cloud with their respective permissions.* *The customer has difficulty managing secure access across devices for remote users, a centralized identity management access control is important.*	**Microsoft Entra ID** It is the Active Directory in the cloud. It is the identity and access management service attached to an Azure tenant that contains the user accounts and password. It allows user to have access external resources or on-premises resources. We will be synchronizing TTNZ on-premises Active Directory with Entra ID. **Microsoft Azure tenant** It is an instance of Microsoft Entra ID service and represent a single organization. It provides a sole place to manage users, groups and their permissions to access resources. We will be using "TechTNZCloud.co.nz" as TTNZ unique name. In one single instance, a tenant can hold one or more subscriptions. **Microsoft Azure Subscription** It is an agreement with Microsoft and our customer to have access to Azure services. Each subscription relies on one and single Azure Tenant to authorize and authenticate users. We will use for each department in order to put resources into logical container. **Azure Identity Access Management (IAM)** It is a service in Azure that allow user and permissions management. We will setup permissions to secure the access of azure cloud. **Microsoft Entra Cloud Sync** It is a directory provisioning that involves a synchronization with on-premises Active Directory to the Microsoft Entra ID. We will be installing the provisioning agent to customer's Domain Controllers (Auckland, Wellington, Christchurch)
Scalability Challenges *TTNZ on-premises' architecture cannot keep up with the growing demands because it required scalable cloud solutions at a considered cost to*	

accommodate the IT workloads. **Increase stability, reliability, and support** *TTNZ on-premises architecture required resilient capabilities because they have 3 remote sites where employees work remotely.*	
Security Vulnerabilities *TTNZ need to enhanced security and monitoring their on-premises and cloud architecture.* *Customer's local security measure are weak and have some gaps in threat detection and response.* *It is the first barrier to protect security environment to TTNZ's azure cloud with a real-time response threat capability.*	
Device and Application Management	

Due to increase number of devices TTNZ need a centralize management device solution allowing to secure modern device and manage application	
Data Governance and Compliance *Regulatory demand for security, data privacy and legislative compliance that TTNZ need to address to. They need effective solutions for managing sensitive data and ensure that they are compliant.*	
Collaboration and Productivity Tools *TTNZ wants to improve the collaboration between offices due to its poor efficacity with a better software services integrations that will allow to streamline staff productivity daily*	
Value Added-Proposition(s)	
Automation with AI *TTNZ is interested to leverage automation with*	

AI products and service in order to improve employee productivity.	
Improve business continuity, backup and disaster recovery *TTNZ key is to be 100% to accompany retailer New Zealand business in order to achieve it, they need a good Disaster Recovery Solution*	
Optimise costings	

TECHNICAL SOLUTIONS DETAILS

IDENTITY AND ACCESS

1. MICROSOFT TENANT

We need to create a Microsoft Entra *tenant* "TechTNZCloud.co.nz" in Data center located in New Zealand due to standard regulations. In order to differentiate with the main on-premises domain name organization "TechTNZCloud.co.nz" is used to indicate the cloud purposes. In Auckland headquarter, on the main Windows Server Active Directory, we will create a forest named "TechTNZCloud.co.nz". That will allow to maintain the main and slowly migrate to the "cloud" domain name. Users and Organization Unit will be moved per lot.

2. MICROSOFT ENTRA ID

To have access to Azure Cloud Resources, each user would need to have Entra ID P1 and P2 for some users:

- 380 Users will use Microsoft Entra ID P1 (included in the Microsoft 365 E3 license), it allows user to have access on-premises and cloud resources. For Organization unit, it supports Dynamic groups that recognize with some regex to categorize user into specific group. Moreover, it allows to change on-premises users password, manage identity and group.
- 80 Users will use Microsoft Entra ID P2 (included in the Microsoft 365 E5 license), same permissions of P1, plus the possibility to add some access conditions to application and critical business data. Privilege identity management is allowing to mitigate the risks of excessive and misuses access on resources of administrators.

3. MICROSOFT LICENSES

Since TTNZ has multiple legacy licenses (Office 2013 and Skype Business), we will need to upgrade by getting license.

Each user would need a license in order to have access to Microsoft 365 and Azure, we choose the following:

- 50 Users will use Microsoft 365 F3 is specifically designed for frontline worker that need mobility and have direct contact with customer like sale representative. It does include Word, Excel, PowerPoint, OneNote and Outlook on the web and mobile. This license does not include local machine version of the office suite but however Microsoft teams is available for desktop and mobile.
- 380 Users will use Microsoft 365 E3, it includes:
  - Microsoft Entra ID Plan 1,
  - Microsoft Desktop apps (Word, Excel, PowerPoint, OneNote , Outlook, Access and Publisher),
  - SharePoint Plan 2 (10GB SharePoint storage per license)
  - Microsoft Purview for Data governance and Compliance,
  - Data Loss Prvention for emails and files
  - Microsoft Defender and Microsoft Defender for Endpoint Plan 1,
  - Device and Application Management: Microsoft Intune , Windows autopilot.
- 380 Microsoft 365 E5 Compliance to add sensitivty labels on SharePoint and OneDrive
- 80 Users will use Microsoft 365 E5, it includes:
- 450 Users will use Microsoft Teams Enterprise, it includes :

4. AZURE SUBSCRIPTION

Each subscription allows to a have granulated permissions access between Azure resources group. It follows a parent-child hierarchy as follow:

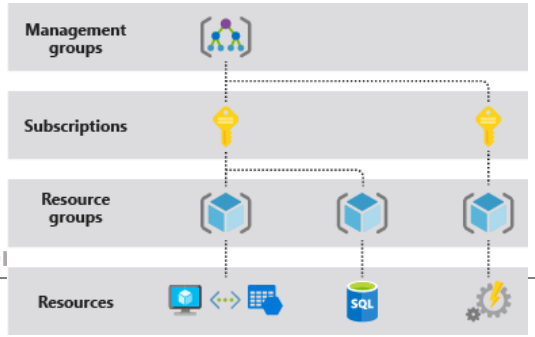

Figure 1 Azure Subscription - Management Groups (Mumian, 2024)

The definition of Azure Management group is needed. Azure Management Group sit at the top of the Azure hierarchy (Root Management Group) and provide a way to manage access, policies, and compliance across multiple Azure subscriptions. Then, below it, Azure Subscription are needed:

- HR management group / Human Resource Subscription
- Marketing management group / Marketing Subscription
- Sales management group / Sales Subscription

5. IMPLEMENTING IDENTITY SYNCHRONIZATION: MICROSOFT ENTRA CONNECT SYNC

With the use of Microsoft Entra Connect Sync provisioning agent on the Domain Controller in Auckland (TTNZ-AKL-DC01, TTNZ-AKL-DC02), Wellington (TTNZ-WLG-DC01, TTNZ-WLG-DC02), Christchurch (TTNZ-CHC-DC01, TTNZ- CHC -DC02), organization units and users are synchronizing with Entra ID. It allows high availability with its failover mechanism thru the use of multiple cloud agent installed on-premises. It can provision disconnected forest allowing fast project integration.

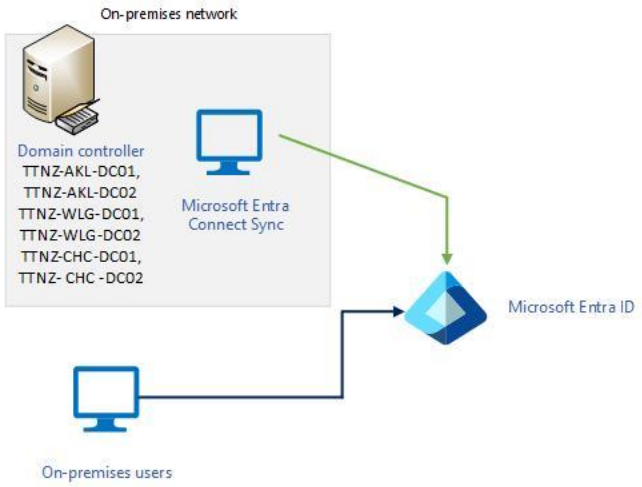

Figure 2 Entra Connect Sync implementation

6. MANAGE SECURE USER ACCESS

6.1. IDENTITY ACCESS MANAGEMENT (IAM)

Users can be assigned roles and permissions into different Azure Hierarchy. There are these hierarchy of layers:

- Microsoft Entra ID >
  - Within Entra ID > Root Management Hierarchy
    - Within Root Management Hierarchy > Management groups >
      - Azure Subscriptions >
        - Resource Groups

6.2. AZURE ROLE BASED ACCESS CONTROL (RBAC)

Users can be assigned roles and permissions into different Azure Hierarchy. There are these hierarchy of layers:

- Microsoft Entra ID >
  - Within Entra ID > Root Management Hierarchy

- Within Root Management Hierarchy > Management groups >
  - Azure Subscriptions >
    - Resource Groups

6.3. MULTI-FACTOR AUTHENTICATION (MFA) REGISTRATION POLICY (AZURE | MICROSOFT 365)

6.4 CONDITIONAL ACCESS POLICY (AZURE | MICROSOFT 365)

6.5 PRIVILEGED IDENTITY MANAGEMENT (PIM) ADMINISTRATOR APPROVAL (MICROSOFT 365)

In order to give the right permissions to the right person at the right time, we implement PIM. It allows to manage and grant high privilege for a temporary user that need administrator roles or to improve governance and security for administrator roles. It helps TTNZ to mitigate risks with the misuse of privilege access.

SCALABILITIES CHALLENGES

1. AZURE PUBLIC & PRIVATE DNS

Domain name configuration in Azure is needed, it is as follow:

- The creation of an Azure Public DNS, “techtnzcloud.co.nz”, allowing external name resolution to the Azure Cloud Services. It will allow the users to have access to custom apps with a sub custom domain “apps.techtnzcloud.co.nz”
- The creation of an Azure Private DNS, “private.techtnzcloud.co.nz “, allowing to create domain name resolution within Azure Private Virtual Network.

(*ref.* *Appendix :* **Migrate Applications to fix scalabilities issues (SupportDesk and XYZ Payroll Manager) to Azure Service Plan** **)**

2. AZURE REGIONS & AZURE AVAILABILITIES ZONE

We are going to set up two Azure Regions different and two availabilities zones set. These are separated data centers within an Azure Region.

It is as follow:

- North Auckland with Availability 1 and Availability 2
- East Australia with Availability 1 and Availability 2

3. AZURE PRIVATE VIRTUAL NETWORK & AZURE PRIVATE NETWORK LOCAL PEERING

For the Private Virtual Network Addressing, it is recommended to use IP Addresses that is not used on-premise. That will allow not overlapping IP addresses.

To follow the network separation (Application/Database) as on-premises, the networking addressing as follow:

- Private Virtual Network IP: 10.40.0.0/16
- North Auckland Region:
  - Applications Subnet: 10.40.1.0/28 (14 hosts usable)
  - Database Subnet: 10.40.2.0/28 (14 hosts usable)
- East Australia Region:
  - Applications Subnet: 10.40.1.0/28 (14 hosts usable)
  - Database Subnet: 10.40.2.0/28 (14 hosts usable)

The Webserver (IIS Servers) communicate to the database with the help of Azure Private Network Local Peering. It is routing the traffic internally within Microsoft Network and not over the internet or a gateway.

4. AZURE RESOURCES GROUP

The following Resources group are present:

- TTNZ-SupportDesk= Active Region | Azure Region: North Auckland | Availability 1 & Availability 2
  - hold "*TTNZ-SupportDesk*"
- TTNZ-SupportDesk-FO = Standby region | Azure Region: East Australia | Availability 1 & Availability 2
  - hold "*TTNZ- SupportDesk -FO*" and is built using ARM template based off "*TTNZ-SupportDesk*".
- TTNZ-Payroll= Active Region | Azure Region: North Auckland | Availability 1 & Availability 2
  - hold "*TTNZ-Payroll*"
- TTNZ- Payroll -FO = Standby region | Azure Region: East Australia | Availability 1 & Availability 2
  - hold "TTNZ *-Payroll -FO*" and is built using ARM template based off "TTNZ-Payroll".

4.1. WEB APPLICATION

4.1.1. AZURE STORAGE ACCOUNT

A backup of the "TTNZ-SupportDesk" application and the XYZ-Payroll manager is deployed to Blob Storage to their according Azure Resources group.

4.1.2. AZURE SERVICE PLAN & AZURE WEB APPS

The Azure Service Plan use Premium V2. Web App Service is created on a Windows with latest version of ASP.NET and linked to a blob storage in order to install the web applications.

4.1.3. AZURE WEB APP SERVICE

It has a build-in load-balancer. Depending on the traffic, Web App Service is autoscaling to increase or decrease the number of Virtual Machines instances. By default, "TTNZ-SupportDesk" and the XYZ-Payroll manager are configured to have a minimum of 2 instances to a maximum of 6 instances.

4.1.4. AZURE FRONT DOOR

It is caching "TTNZ-SupportDesk" and "*TTNZ-Payroll*" content and act as a load-balancer that holds the Public IP Address where the traffic is routed between our WebApp Instances. (ref. ***Appendix : Migrate Applications to fix scalabilities issues (SupportDesk and XYZ Payroll Manager) to Azure Service Plan*** **)**

4.2. DATABASE

4.2.1 MICROSOFT AZURE SQL DATABASE

The hyperscale service tier can provide scaling vertically (scale-up) to accommodate heavy workloads when needed and if not needed, to scale down. Also, it can be scale horizontally by providing one or multiples read-only replicas allowing to offload the workflow of the main database. This hyperscale scale capabilities present high performance due to the higher transaction log sending and a faster time to commit no matter the volumes of data.

*(ref. **Appendix : Migrate Applications to fix scalabilities issues (SupportDesk and XYZ Payroll Manager) to Azure Service Plan**)*

5. MICROSOFT 365

5.1. FILESHARE TO ONEDRIVE/SHAREPOINT

5.2. SHAREPOINT SERVER TO MICROSOFT 365

5.2.1. SHAREPOINT MIGRATION TOOL (SPMT)

5.3. MICROSOFT EXCHANGE TO MICROSOFT 365

5.3.1. MICROSOFT EXCHANGE ONLINE

SECURITY VULNERABILITIES

1. NETWORK SECURITY GROUP & APPLICATION SECURITY GROUPS

The Webserver server is in Application Security Group as “ASG-WEB”.

The Database server (SQL Server) is in Application Security Group as “ASG-DB”.

- “ASG-WEB” is attached to a Network Security Group rule as an inbound traffic where ports 80,443 are allowed.
- “ASG- DB” is attached to a Network Security Group rule as an inbound traffic where destination port 3306 is allowed but a restricted access with outbound security rules where denies access to the internet.

2. AZURE WEB APPLICATION FIREWALL

It is used on top of Azure Front Door in order to protect the traffic flowing into the front-end application. It is web application protection at layer 7. Traffic directly to the Web Service Apps is blocked in order to prioritize traffic to go through the Azure Front Door.

3. AZURE DDOS PROTECTION

DDoS attack is to jam the traffic and exhaust the compute of an application. Azure DDoS protection is combined with the Azure Web application to protect at layer 3 and 4 to the network layers.

4. AZURE ROLE BASE ACCESS CONTROL (RBAC)

Role and permission assigned to Azure Web Apps (*ref. Web Application*) and SQL server (*ref. Database*) as follow:

- System Administrator group: Global Administrator
- Database Administrator group: Contributor Role

COSTING ANALYSIS

CURRENT FINANCIAL

CAPEX

Current Financial 2024 (NZD)				
Capital Expenditure (CAPex) (NZD)				
Description	**Detail**		**Cost (low estimate - high estimate)**	Periodicity
License Software	Microsoft SQL Server + CAL	estimate	$2,500 - $3,000	*one time off*
License Software	Windows Server 2022 + CAL	estimate	$20,000 - $22,000	*one time off*
License Software	Microsoft Office 2013	estimate	$20,000 - $25,000	*one time off*
License Software	Skype for Business	estimate	$10,000 - $13,000	*one time off*
License Software	XYZ Payroll Manager License	estimate	$10,000 - $15,000	*one time off*
License Software	ERP Software	estimate	$15,000- $20,000	*one time off*
Office Furniture	Chairs	estimate	$224,500 - $704,500	*one time off*
Office Furniture	Standing Desk	estimate	$65,000 - $179,500	*one time off*
Office Furniture	Printer paper, pen, and miscellaneous Auckland, Wellington, Christchurch furniture	estimate	$5,000 - $8,000	*one time off*
User Devices	Desktop Computer (170 est)	estimate	$204,000 - $253,000	*one time off*
User Devices	Laptops (250 est)	estimate	$100,000 - $174,000	*one time off*

User Devices	Smartphones Android (210 est) with discounted mobile plan or only device only ($1200 voucher)	estimate	$4,200 - $252,000	*one time off*
User Devices	Smartphones IoS (140 est) with discounted mobile plan or only device only ($1200 Voucher)	estimate	$8,400 - $168,000	*one time off*
Other IoT Devices	Tablets, Kiosk(s), TVs, Touch Screens, Projectors, Fridges and more. (40 est)	estimate	$48,000 - $56,000	*one time off*
Networking	Firewall : Fortigate FG-100F Enterprise Firewall (4 est)	estimate	$16,440 - $18,000	*one time off*
Networking	Managed Switch : Fortinet FS-148-E 48 Ports (14 est)	estimate	$16,254 - $19,600	*one time off*
Networking	Unmanaged Switch : Fortinet-FG-124E - Swtich 24 Ports (32 est)	estimate	$52,832 - $60,800	*one time off*
Server Hardware	Racks, Ethernet Cable, Power UPC	estimate	$28,000 - $30,000	*one time off*
Server Hardware	Servers Lenovo TD350 (12 est)	estimate	$48,636 - $72,000	*one time off*
Backup device	NAS	estimate	$3,000 - $3,200	*one time off*
	Totals estimate (one time off)		$894,762- $2,091,600	*one time off*
License Software	VMware vSphere Essentials Plus - 3-Year Prepaid Commit	estimate	$8,499 - $9,600	*yearly*
License Software	Fortinet FortiSwitch Comprehensive Support	estimate	$77.00 - $150.00	*yearly*
License Software	Fortinet Basic + FortiCare license	estimate	$1960 - $3000	*yearly*
License Software	ERP Sales License for 450 users	estimate	$112,500 - $135,000	*yearly*
License Software	Veeam Data Backup platform	estimate	$25,500 - $30,000	*yearly*
License Software	Veeam Data Platform Essentials NAS Capacity	estimate	$800- $900	*yearly*
	Totals estimate (yearly)		**$149,336- $178,650**	*yearly*
	Totals estimate CAPex (one time off + yearly)		**$1,011,674- $2,222,250**	

Table 5 Costing Analysis | Current Financial 2024 | CAPex | Estimate

OPEX

Operating Expenses (OpEx) (NZD)				
Description	**Detail**		**Cost (low estimate - high estimate)**	Periodicity
Rent and Utilties	Renting Business Location, Internet, Electricity , Water and other utilities	estimate	$650,000 - $980,000	*yearly*
Wages	Salaries 20 Full-Time employees	estimate	$650,000 - $648,000	*yearly*
Wages	Salaries 120 part-time employees	estimate	$864,000 - $1,152,000	*yearly*
Wages				*yearly*
Services				*yearly*
Services fees				*yearly*
Services fees				*yearly*
Support IT				*yearly*
Support IT				*yearly*
Support IT				*yearly*
		Totals estimate OpEx (yearly)	**$6,793,000- $8,300,000**	

Table 6 Costing Analysis | Operating Expenses (OPex) | Estimate

CAPEX+OPEX

Current Financial 2024 (NZD)	
Totals CapEX + OPEX	
Totals CapEx (yearly) + Totals OpEx (yearly)	$6,942,336 - $8,478,650

Table 7 Costing Analysis | Current Financial 2024 | CAPex + OPex

REVENUE & PROFIT

Revenue (NZD)							
	2018	2019	2020	2021	2022	2023	2024
Low	10 000 000	11 000 000.0	12 100 000.0	13 310 000.0	14 641 000.0	16 105 100.0	17 715 610.0
High	15 000 000	16 500 000.0	18 150 000.0	19 965 000.0	21 961 500.0	24 157 650.0	26 573 415.0

Table 8 Current Financial | CAPex | Revenue from 2018 | Estimate

Result (NZD)							
	2018	2019	2020	2021	2022	2023	2024
Low	3 057 664	3 363 430.4	3 699 773.4	4 069 750.8	4 476 725.9	4 924 398.4	5 416 838.3
High	6 521 350	7 499 552.5	8 249 507.8	9 074 458.5	9 981 904.4	10 980 094.8	12 078 104.3

Table 9 Current Financial | CAPex | Result from 2018 | Estimate

Note : " the company consistently has been in profit ranging from 10%-15% annually over the past 6 years"

Revenue (estimate 2024 from Q1, Q2, Q3) (NZD)	
Total	$17,715,610 - $26,573,451

Table 10 Costing Analysis | Current Financial 2024 | Revenue Estimate

Result / Profit (estimate 2024 from 2023 and Q1, Q2, Q3) (NZD)	
Total	$5,416,838 - $12,078,104

Table 11 Costing Analysis | Current Financial 2024 | Result Estimate

CAPEX

Project : Delta Cloud | Modern Workplace					
Capital Expenditure (CAPex) (NZD)					
Description	**Detail**	**Vendors**		**Cost (low estimate - high estimate)**	Periodicity
Preparation Phase 1	Configure Azure environment with licenses	Microsoft Azure	estimate	$53,833 - $64,856	*monthly*
Preparation Phase 1	Configure Microsoft Tenant environment with licenses	Microsoft 365			
Preparation Phase 2	Configure Added Values : Monitoring	Microsoft Azure			
Preparation Phase 3	Deliverable Identity and Secure Access Management	Microsoft 365			
Preparation Phase 4	Deliverable Implementing Identity Synchronization	Microsoft 365			
Totals estimate monthly				**$53,833 - $64,856**	
Execution Phase 3	Migrate Applications to fix scalabilities issues (SupportDesk and XYZ Payroll Manager) to Azure Service Plan	Microsoft Azure	estimate	$1,310.25 - $2,500.00	*one time off*
Totals estimate (one time off)				$1,310.25 - $2,500.00	
Totals estimate yearly				**$645,996 - $778,272**	

Totals estimately CAPex (one time off + yearly)	**$647,306 - $780,772**

Table 12 Costing Analysis | Project : Delta Cloud | Modern Workplace | CAPex | Estimate

Detail Capital Expenditure (CAPex) (NZD)					
Microsoft Azure Estimate					
Service category	**Service type**	**Region**	**Description**	**Estimated monthly cost**	**Estimated upfront cost**
Compute	App Service	East US	Premium V2 Tier; 2 P1V2 (1 Core(s), 3.5 GB RAM, 250 GB Storage) x 31 Days; Windows OS; 2 SNI SSL Connections; 2 IP SSL Connections; 2 Custom Domains; 2 Standard SLL Certificates; 2 Wildcard SSL Certificates	$577,31	$1 310,25

Support		Support			
		Licensing Program	Microsoft Customer Agreement (MCA)		
		Billing Account			
		Billing Profile			
				Total	
Disclaimer					

All prices shown are in New Zealand – Dollar ($) NZD. This is a summary estimate, not a quote. For up to date pricing information please visit https://azure.microsoft.com/pricing/calculator/

Table 13 Costing Analysis | Capital Expenditure (CAPex) Detail - Microsoft Azure Estimate

Detail Capital Expenditure (CapEx) (NZD)			
Microsoft 365 Estimate			
Description	price /user /month	users	total
Microsoft 365 F3			
Microsoft 365 E3 (no Teams)			
Microsoft 365 E5 Compliance			
Microsoft 365 E5 (no Teams)			
Microsoft Teams Enterprise			
Totals monthly			

Table 14 Costing Analysis | Capital Expenditure (CAPex) Detail - Microsoft 365 Estimate

With migrating Payroll manager, SupportDesk application, SharePoint Server, Microsoft Exchange into Microsoft Azure/365

TTNZ can decommissioned those servers:

- SQL Servers x4 (we leave 2x because of the ERP Sales that need SQL Servers)
- Exchange Servers x3
- SharePoint Server x2
- Files Servers x3 (we leave 1x in Auckland to have a replication in case of disaster)

Those servers are virtualized 2 Physical Servers located in the 3 sites. We can take the opportunity to sell 6 of the 12 servers. ($24,318 can be recuperated : $4,053 per server / ref *CAPex-Line*)

OPEX

Project : Delta Cloud | Modern Workplace				
Operating Expenses (OpEx) (NZD)				
Description	**Detail**		**Cost (low estimate - high estimate)**	Periodicity
Zero-Trust Interface Training	Implement the Cloud infrastructure with its network and Devices connected, any related other incident or technical support			*per hour*
				estimate Annual cost
Wages	Hiring 5 System and Database Administrator			*yearly*
		Totals yearly		

Table 15 Costing Analysis | Project : Delta Cloud | Modern Workplace | OPex | Estimate

CAPEX+OPEX

Project : Delta Cloud Totals CapEX + OPEX	
Totals yearly	

Table 16 Costing Analysis | Project : Delta Cloud | Modern Workplace | Total CAPex + OPex

BUDGET

Budget Provisioned "Project Delta Cloud | Modern Workplace"	
Totals yearly	

Table 17 Costing Analysis | Project : Delta Cloud | Modern Workplace | Budget Provisioned

Estimate Budget provisionned / Estimate Cost Project Delta Cloud		
	Low Estimate	High Estimate
Budget	1 400 000	1 700 000
Total Cost Project Delta Cloud	1 336 556	1 545 022
Ratio %	95%	91%

Table 18 Costing Analysis | Project : Delta Cloud | Modern Workplace | Budget Provisioned / Estimate cost project

RESULT 2024 / PROJECT

Estimate Result 2024 / Estimate Cost Project Delta Cloud		
	Low Estimate	**High Estimate**
Result 2024	**5 416 838**	**12 078 104**
Total Cost Project Delta Cloud	**1 336 556**	**1 545 022**
Ratio %	25%	13%

Table 19 Costing Analysis | Project : Delta Cloud | Modern Workplace | Estimate Result 2024 / Estimate cost project

TIMELINE

PROJECT ROADMAP GANTT CHART

Note: Mid December and Mid-January, TTNZ has a “change freeze” period due to Holidays, no migration or change in production can occurred during this time. (ref Stakeholder Analysis)

Timeline Sept 2025 - April 2026																																								
8 Months			Sept				Oct				Nov				Dec				Jan				Feb				Mar				April										
#	Tasks	Week #	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	#	21	#	#	#	#	#	#	#	#	#	#	31	#					
1	**Phase 1 Initiation Phase**	1																																						
1,1	Project Scope : Identify Objectives and Requirement	1																																						
1,2	Identify Audiences and Stakeholders	1																																						
1,3	Create a Project Team Charter	1																																						
1,4	Draft a Communication Plan	1																																						
2	**Phase 2 Evaluate and Planning**	4																																						
2,1	Discovery of current infrastructure	2																																						
2,2	Identification applications for migration	2																																						
2,3	Identify Risk and Mitigation in Risk Registry	1																																						
3	**Phase 3 Design**	4																																						
3,1	Design Solutions Options	2																																						
3,2	Prepare Statement of Work	3																																						
3,3	Draft Design and Build	1																																						
4	**Phase 4 Preparation**	6																																						
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	#	21	#	#	#	#	#	#	#	#	#	#	31	#					

Table 20 Gantt Chart

CHANGE CONTROL

ITIL SVS/SVC

Service Value Chain - Details			
Step	Activities	Input	Output
1	Demand	TTNZ's Operations Manager, and CIO of has raised various issues that affect the current End User environment	List of Issues made by Operations Manager and CIO
2	Engage	TTNZ contact ZTI and describe the issues list the resolutions that need to be addressed and wants to have cloud solutions	ZTI draft Business Requirement from the TTNZ's demand
3	Plan	ZTI need to resolve different issues regarding: Identity and Access Management Scalabilities Challenges Security Vulnerabilities Device and Application Management Collaboration and Productivity Tools Value Added-Proposition(s) A.I Products and services	ZTI need to plan an on-site to discover the on-premises environment.s

Table 21 Service Value Chain

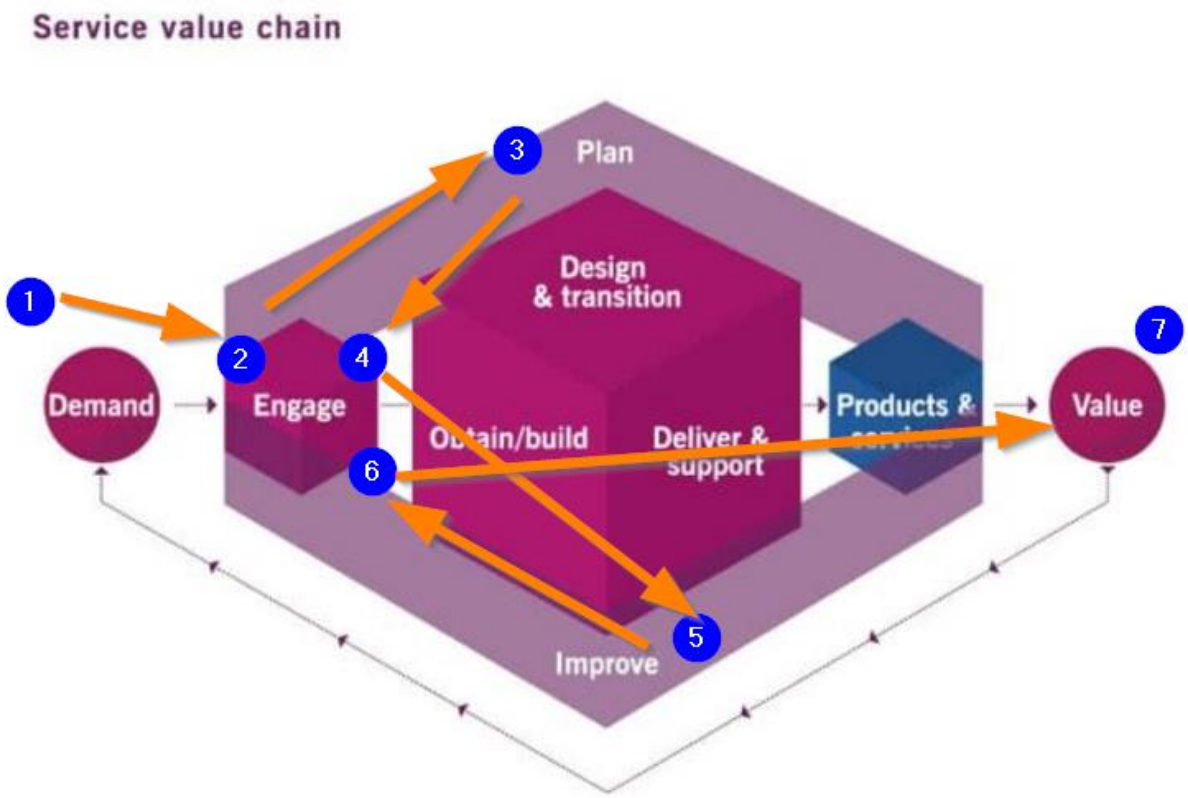

Figure 3 ITILv4 - Service Value Chain (ref. More detail)

CHANGE APPROVAL

APPROVAL FORM

Project Name	**Delta Cloud**	**Ref Number**	***CHA-DC-01***
Approval Stakeholder	*C.T.O*	**Company**	*Zero-Trust Interface*
Project Team Lead	*JP LO SIOU*	**Form Request Date**	***27.11.2024***
Form Requestor	*Jean-Philippe LO SIOU*	**Approval Required Date**	***28.11.2024***

Table 22 Approval Form Detail

Change Management - Requested Details	
Change 1	*Cost License Microsoft 365*
Change 2	*Migrate files to OneDrive /SharePoint*
Change 3	
Change 4	

Table 23 Approval Form Detail | Change

Change Management - Impact Analysis		**Doc Vers**
Change 1	*No impact on user*	***1.0a***
Change 2	*End-user won't have access to files / folders between 4 hours to 6 hours*	***1.0a***
Change 3		***1.0a***
Change 4		***1.0a***

Table 24 Approval Form Detail | Impact

Change Management - Scope of Work			
Deliverables	**Est. Hours**	**Resources Req**	**Delivery Date**
Preparation Azure environment	***80hrs***		***11/12/2024***
OneDrive Business / SharePoint	***80hrs***		***20/12/2024***

Table 25 Approval Form Detail | Deliverables

Key Stakeholder Sign Off				
Title	**Company**	**Name**	**Signature**	**Date**
CEO	*TTNZ*	*Mike*	***Mike R***	***28/11/2024***
CFO	*TTNZ*	*Roger*	***Roger S***	***28/11/2024***
CTO	*TTNZ*	*Alex*	***Alex H***	***29/11/2024***
			Decision	**Approved**
			Comment	

Table 26 Approval Form Detail | Key Stakeholder Sign Off

REFERENCE LIST

Referencing APA 7 List

1. *OwenRichards. (2024, January 11). Quickstart: Create a Microsoft Entra tenant - Microsoft identity platform. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/entra/identity-platform/quickstart-create-new-tenant*
2. *Barclayn. (2024, May 22). What is Microsoft Entra ID? - Microsoft Entra. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/entra/fundamentals/whatis*
3. *Rwike. (2024, May 31). What is identity and access management (IAM)? - Microsoft Entra. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/entra/fundamentals/introduction-identity-access-management*
4. *Barclayn. (2024a, March 22). Add an existing Azure subscription to your tenant - Microsoft Entra. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/entra/fundamentals/how-subscriptions-associated-directory*
5. *Justinha. (2023, October 6). Common deployment scenarios for Microsoft Entra Domain Services - Microsoft Entra ID. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/entra/identity/domain-services/scenarios#azure-ad-ds-for-hybrid-organizations*
6. *Billmath. (2024, April 26). What is Microsoft Entra Cloud Sync? - Microsoft Entra ID. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/entra/identity/hybrid/cloud-sync/what-is-cloud-sync*
7. *Justinha. (2023b, October 6). Overview of Microsoft Entra Domain Services - Microsoft Entra ID. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/entra/identity/domain-services/overview*
8. *Justinha. (2023b, October 6). Common deployment scenarios for Microsoft Entra Domain Services - Microsoft Entra ID. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/entra/identity/domain-services/scenarios#azure-ad-ds-for-hybrid-organizations*
9. *Mumian. (2024, June 21). Manage resource groups - Azure portal - Azure Resource Manager. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal*

APPENDIX

EXECUTION PHASE 3 : MIGRATE APPLICATIONS TO FIX SCALABILITIES ISSUES (SUPPORTDESK AND XYZ PAYROLL MANAGER) TO AZURE SERVICE PLAN

Figure 4 Migrate Applications to fix scalabilities issues (SupportDesk and XYZ Payroll Manager) to Azure Service Plan

MICROSOFT 365

FILESHARE TO ONEDRIVE/SHAREPOINT

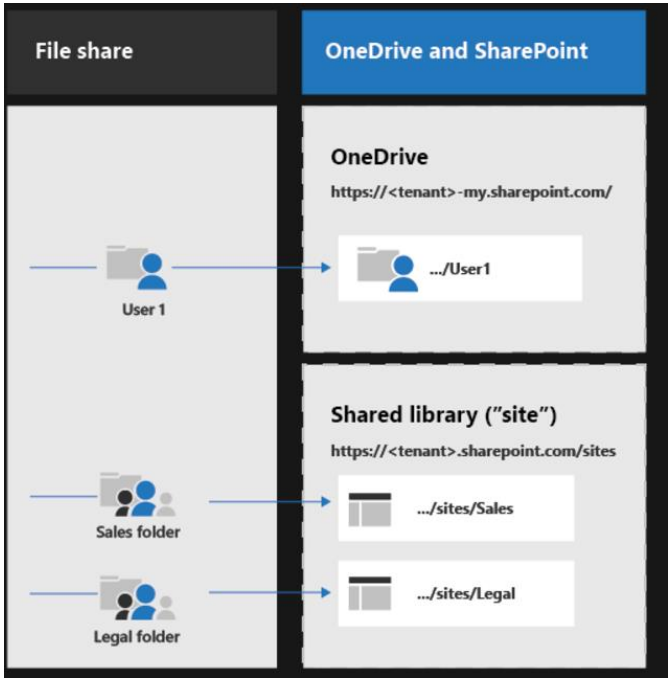

Figure 5 What content goes where | Fileshare , OneDrive and SharePoint (MicrosoftHeidi, 2024a)

Windows file share permissions	SharePoint item access	SharePoint role
Full control	Full control	Full control
Modify	Modify	Contribute
Read and execute	Read and execute	Read
List folder contents	List folder contents	Read
Read	Read	Read
Write	Write	Contribute

Figure 6 What content goes where | Windows Permissions / SharePoint (MicrosoftHeidi, 2024a)

MICROSOFT EXCHANGE ONLINE

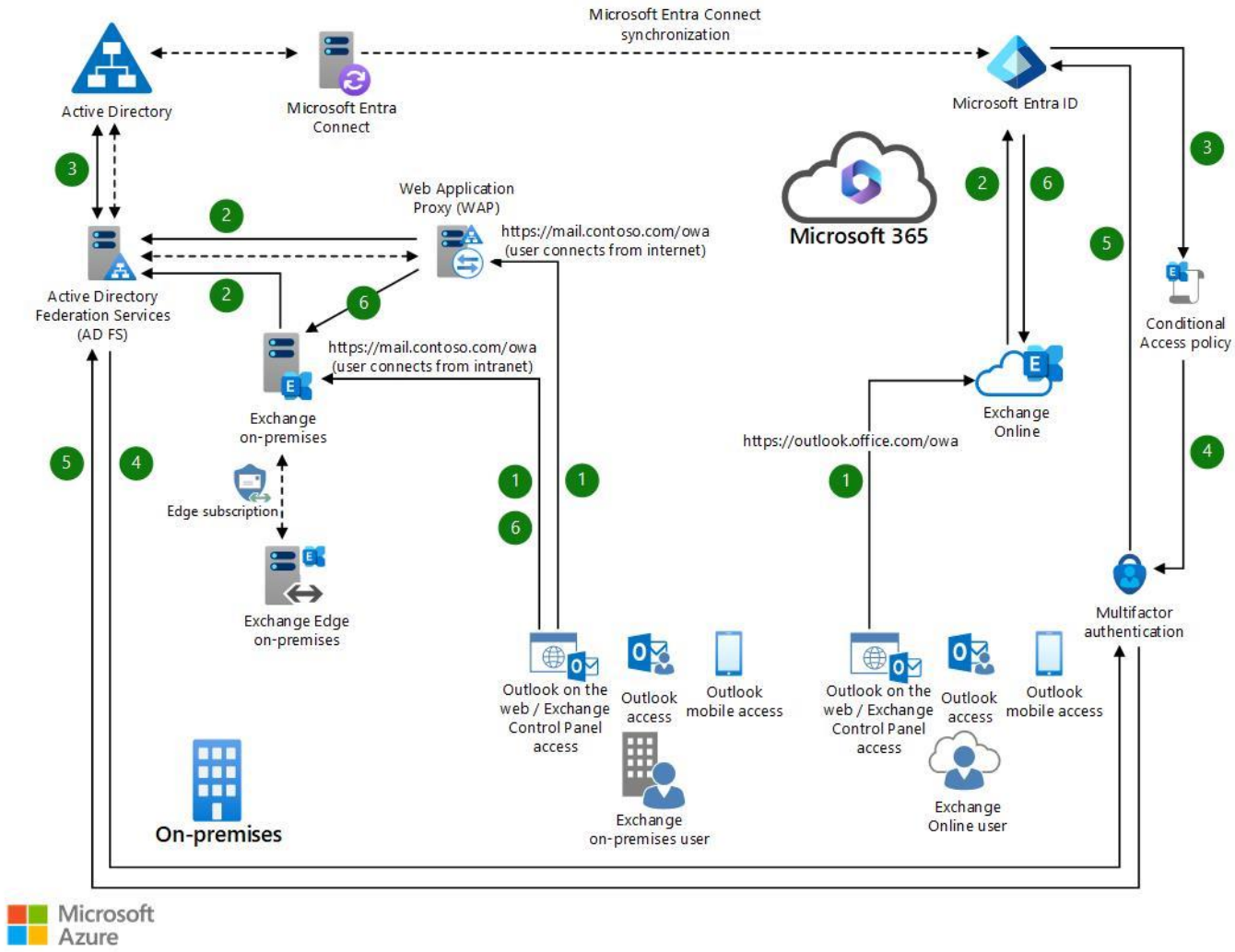

Figure 7 Microsoft 365 | Exchange Online (Workflow) (more detail) (RobBagby, 2024)

Workflow (Exchange Online)

1. The user starts Outlook profile configuration by entering an email address. Outlook mobile connects to the AutoDetect service.
2. The AutoDetect service makes an anonymous AutoDiscover V2 request to Exchange Online to get the mailbox. Exchange Online replies with a 302 redirect response that contains the ActiveSync URL address for the mailbox, pointing to Exchange Online. You can see an example of this type of request here.
3. Now that the AutoDetect service has information about the endpoint of the mailbox content, it can call ActiveSync without authentication.
4. As described in the connection flow here, Exchange responds with a 401 challenge response. It includes an authorization URL that identifies the Microsoft Entra endpoint that the client needs to use to get an access token.
5. The AutoDetect service returns the Microsoft Entra authorization endpoint to the client.
6. The client connects to Microsoft Entra ID to complete authentication and enter sign-in information (email).
7. If the domain is federated, the request is redirected to Web Application Proxy.
8. Web Application Proxy proxies the authentication request to AD FS. The user sees a sign-in page.
9. The user enters credentials to complete authentication.
10. The user is redirected back to Microsoft Entra ID.
11. Microsoft Entra ID applies an Azure Conditional Access policy.
12. The policy can enforce restrictions based on the user's device state if the device is enrolled in Microsoft Endpoint Manager, enforce application protection policies, and/or enforce multifactor authentication. You can find a detailed example of this type of policy in the implementation steps described here.
13. The user implements any policy requirements and completes the multifactor authentication request.
14. Microsoft Entra ID returns access and refresh tokens to the client.
15. The client uses the access token to connect to Exchange Online and retrieve the mailbox content.

Figure 8 Microsoft 365 | Exchange Online (Workflow) Details (RobBagby, 2024)