TZAMON

INFORMATION TECHNOLOGY

TABLE OF CONTENTS

Our Mission

Our mission is to empower businesses with the full potential of Microsoft 365, enabling them to achieve digital transformation and drive sustainable growth. We are committed to delivering seamless user experiences, tailored solutions, and exceptional customer service.

Our Mission

MICROSOFT PARTNERSHIP
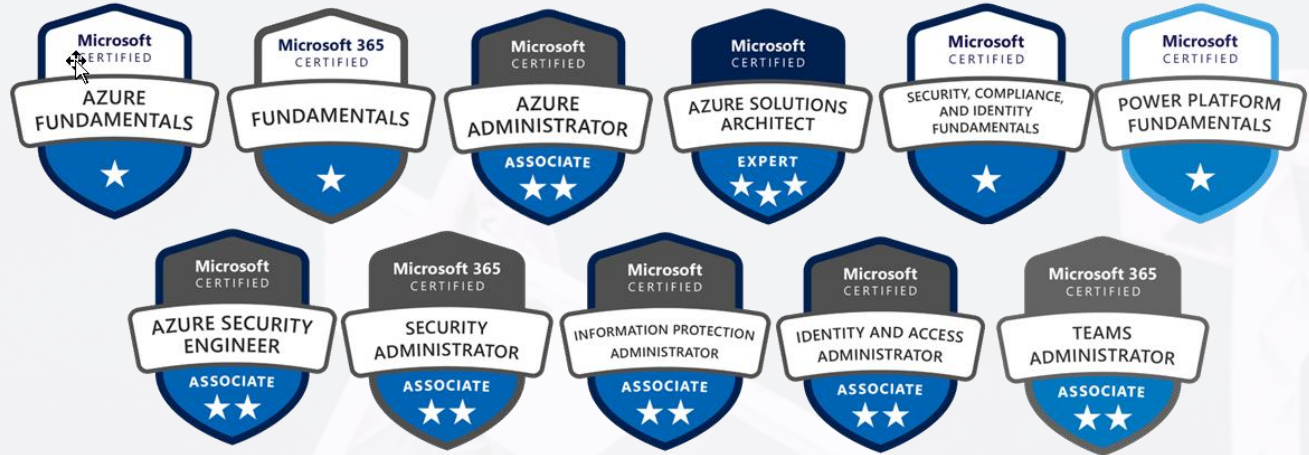
As a certified Microsoft Partner, we have demonstrated expertise in Microsoft technologies and have met stringent requirements set by Microsoft. This partnership enables us to access advanced training, technical support, and exclusive resources, allowing us to offer the best possible solutions to our clients.

TEAM & EXPERTISE

Why Choose Tzamon Information technology

Our team holds extensive experience and certifications in Microsoft technologies, ensuring top-notch service delivery

Unparalleled Expertise

We prioritize our clients' needs and goals, collaborating closely to provide personalized solutions that address their unique challenges

Customer-Centric Approach

We offer ongoing support, training, and maintenance services to ensure that our clients extract maximum value from their Microsoft 365 investment

Comprehensive Support

We offer cost-effective solutions, ensuring that our clients receive the best value for their investment

Competitive Pricing

Basic Microsoft 365 License for Waha Oil Company

Microsoft 365, Enterprise Mobility + Security, Subscriptions for Enterprises

	Microsoft 365 E3	Microsoft Defender For Office
Exchange Plan 2 (100 GB mailbox+ up to 1.5 TB archive)	●	
Exchange Online Protection	●	
SharePoint Plan 2 (1+ TB OneDrive storage)	●	
Power BI Pro		
Microsoft Entra ID Plan 1	●	
Microsoft Intune Plan 1	●	
Mobile Device Management	●	
Microsoft Defender for Cloud Apps Discovery	●	
DLP for emails & files	●	
Basic org-wide or location-wide retention policies	●	
Teams message retention policies	●	
Manual retention labels	●	
Audit (Standard)	●	
Alerts, and SIEM integration API for alerts	●	●

Basic Microsoft 365 License for Waha Oil Company

Microsoft 365, Enterprise Mobility + Security, Subscriptions for Enterprises

	Microsoft 365 E3	Microsoft Defender for Office 365 (ATP)
Manual, default, and mandatory sensitivity labeling in Microsoft 365 apps	●	
Manual labeling with the AIP app and plugin	●	
Sensitivity labeling for containers in Microsoft 365	●	
Microsoft Defender Antimalware	●	
Microsoft Defender Firewall	●	
Microsoft Defender Exploit Guard	●	
Microsoft Defender Credential Guard	●	
BitLocker and BitLocker To Go	●	
Manual retention labels	●	
Basic org-wide or location-wide retention policies	●	
Safe Attachments in email		●
Safe Attachments for SharePoint, OneDrive, and Microsoft Teams		●
Safe Links in email, Office clients, and Teams		●
Advanced anti-phishing thresholds in anti-phishing policies		●
User, domain, and mailbox intelligence impersonation protection in anti-phishing policies		●

SERVICES & SOLUTIONS

MAIN
SERVICES & SOLUTIONS
CATEGORIES

COMPLIANCE & GOVERNANCE

SECURITY OPERATION

MANAGEMENT SOLUTIONS

MANAGEMENT SOLUTIONS

- Azure ARC
- Endpoint Management:
  - Intune
  - MECM
- E-Mail Management:
  - Exchange Online
  - Exchange Server
- Document Management:
  - SharePoint
- Power Platform

Azure ARC

Azure Arc is a bridge that extends the Azure platform to help you build applications and services with the flexibility to run across datacenters, at the edge, and in multicloud environments

Disconnected

Datacenter

Edge

Endpoint Management

Microsoft Intune

is a cloud-based endpoint management solution. It manages user access to organizational resources and simplifies app and device management across your many devices, including mobile devices, desktop computers, and virtual endpoints.

Microsoft Endpoint Configuration Manager

is a systems management software product developed by Microsoft for managing large groups of computers providing remote control, patch management, software distribution, operating system deployment, and hardware and software inventory

E-Mail Management

Exchange Online

is a cloud-based messaging platform that delivers email, calendar, contacts, and tasks. can connect through clients like, Outlook desktop, Outlook on the web and Outlook mobile app

Exchange Server

Microsoft Exchange Server is a mail server and calendaring server developed by Microsoft. It runs exclusively on Windows Server operating systems

Exchange hybrid deployment
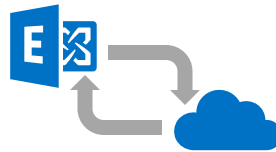
A hybrid deployment provides the seamless look and feel of a single Exchange organization between an on-premises Exchange organization and Exchange Online

Document Management

Document management controls the life cycle of documents, how they are created, reviewed, and published, and how they are ultimately disposed of or retained. Although the term "management" implies that information is controlled from the top of the organization

SharePoint
Online

SharePoint Online is a cloud-based collaboration platform offered by Microsoft as part of the Microsoft 365 suite. It enables organizations to create websites for information sharing and document collaboration

Microsoft Power Platform

The low-code platform that spans Office 365, Azure, Dynamics 365, and standalone applications

Innovation anywhere, Unlocks value everywhere.

Power BI
Business analytics

Power Apps
Application development
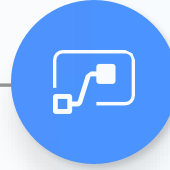
Power Automate
Process automation

Power Virtual Agents
Intelligent virtual agents

SECURITY OPERATION

- Microsoft Defender (EDR – XDR)
    - Defender for Identity
    - Defender for Endpoint
    - Defender for Office 365
    - Defender for Cloud App
- Microsoft Entra ID Protection
- Zero Trust Architecture
- TZN Cybersecurity Maturity Model
- SIEM Solution
- TZN Managed Detection and Response

Microsoft Defender

Defender for
Identity

Defender for
Endpoint

Defender for
Office 365

Defender for
Cloud App

Microsoft Entra ID Protection

Microsoft Entra ID Protection helps organizations detect, investigate, and remediate identity-based risks. These identity-based risks can be further fed into tools like Conditional Access to make access decisions or fed back to a security information and event management (SIEM) tool for further investigation and correlation.

HR systems

External identities

Workload identities

SaaS apps

Cloud infrastructure

Microsoft Entra ID

Devices

On-premises apps

Active Directory
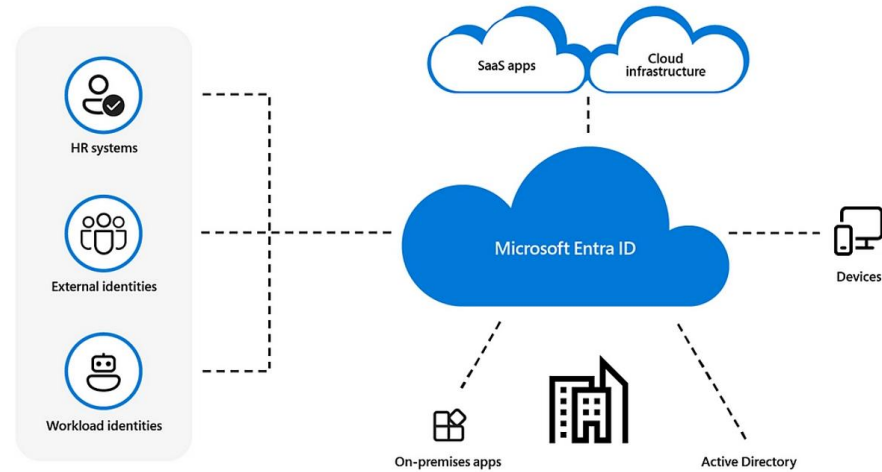
Identities—whether they represent people, services, or IoT devices—define the Zero Trust control plane. When an identity attempts to access a resource, verify that identity with strong authentication, and ensure access is compliant and typical for that identity. Follow least privilege access principles.

Ultimately, security teams are protecting data. Where possible, data should remain safe even if it leaves the devices, apps, infrastructure, and networks the organization controls. Classify, label, and encrypt data, and restrict access based on those attributes.

Once an identity has been granted access to a resource, data can flow to a variety of different endpoints—from IoT devices to smartphones, BYOD to partner-managed devices, and on-premises workloads to cloud-hosted servers. This diversity creates a massive attack surface area. Monitor and enforce device health and compliance for secure access.

Applications and APIs provide the interface by which data is consumed. They may be legacy on-premises, lifted-and-shifted to cloud workloads, or modern SaaS applications. Apply controls and technologies to discover shadow IT, ensure appropriate in-app permissions, gate access based on real-time analytics, monitor for abnormal behavior, control user actions, and validate secure configuration options.

All data is ultimately accessed over network infrastructure. Networking controls can provide critical controls to enhance visibility and help prevent attackers from moving laterally across the network. Segment networks (and do deeper in-network micro-segmentation) and deploy real-time threat protection, end-to-end encryption, monitoring, and analytics.

Zero Trust

- Users
- Devices
- Data
- Applications
- Network Traffic
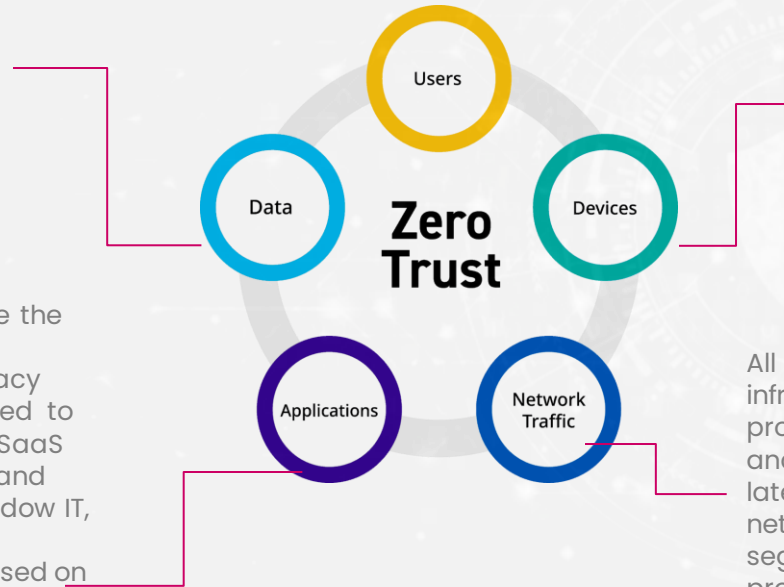
Microsoft Zero Trust Capability Mapping

Implemented in NCCoE lab (Summer 2023)

NIST

Key

- NIST Area
  - NIST Sub-Area
    - Sub-Area
- Microsoft Service

Security Analytics

Microsoft Defender XDR

Defender for Endpoint | Defender for Office 365 | Defender for Identity | Defender for Cloud Apps | Defender for Cloud

Microsoft Sentinel
- Security Information and Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)

Security telemetry from across the environment

Endpoint Security

Microsoft Entra
Conditional Access
Global Secure Access client

User

Device

Mobile Device

Devices w/ SDP

Intune
Device Management

Defender for Endpoint
Endpoint Detection and Response (EDR)

Identity, Credentials, and Access Management (ICAM)

Identity
- User
- Device

Access & Credential Mgmt.
- Authentication

Entra ID

Entra ID Governance

Federation

Governance

Secure Admin Workstations

Entra

Intune

Virtual Desktops

Azure Virtual Desktop Windows 365

Policy Enforcement / Admin

Policy
Determine Access

Grant Access

Grant Access
Software Defined Perimeter(SDP)

Entra ID
Conditional Access

Entra Internet Access

Policy Enforcement Point (PEP)

Feedback mechanisms enable continuous improvement

Entra Private Access Connector

Intune
VPN Backend Connector

Protected Resources

CLOUD APPS & WORKLOADS

Defender for Cloud Apps

Defender for Office 365

Entra Permissions Management

Defender for Cloud
Microsoft Cloud Security Benchmark

3P SaaS

Microsoft 365

Google Cloud aws Azure

Azure IaaS

ON-PREM APPS & WORKLOADS

Data

Purview *Database* *File share* *Storage*
Azure Arc Information Protection Scanner

Apps

Defender Application Guard

Infrastructure & Access

Defender for Identity

Azure Arc Azure Automanage

Data Security

	Data Loss Prevention (DLP)	Document Protection	Office 365	Cloud Infra SQL DB/Files
	Purview DLP	**Purview** Information Protection	**Intune** Mobile App Mgmt **Defender for Cloud Apps** **Purview** Information Protection	**Defender for Cloud**

SIEM Solution

Security information and event management "SIEM", is a solution that helps organizations detect, analyze, and respond to security threats before they harm business operations

Microsoft Sentinel

Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise. With Microsoft Sentinel, you get a single solution for attack detection, threat visibility, proactive hunting, and threat response.

Tzamon MDR powered by Microsoft Security includes:

* **24 x 7 Managed Detection and Response:**
  Real-time monitoring of Microsoft Sentinel alerts with full-scale investigations and response to security events supported by expert Cyber threat analysts who operate 24/7, across multiple locations within Operations Centers (SOC).

* **Increased Visibility to Resolve Every Alert**
  Collects and analyzes data from multiple data sources, including endpoint, email, user activity, and other third-party security solutions, providing visibility into risks and threats across multi-cloud and hybrid environments.

* **MDR Protection with Speed and Scale**
  Near-limitless connectivity speed to security logs and scale delivered in the cloud without the time and cost of SIEM.

* **Integrated Automation Enhanced with Expertise**
  Integrated cross-product automation layer that ingests all alerts generated to automate and coordinate. prevention, defensive responses, and remediation across all platforms.

* **Ongoing Building and Tuning of Azure Sentinel Alerts**
  Simplified implementation tailored to your unique environment, providing custom configurations, and ensuring limited operational interruption.

* **Custom Correlations**
  Analyst developed unique searches, custom correlations, and tracking integrated with threat intelligence providing contextual insights unique to your enterprise.

* **Built-in Automation and Orchestration**
  Integrated, proprietary playbooks designed to automate responses, enabling the ability to fully automate routine operations to recurring types of alerts and/or automated responses to specific alerts.

* **Threat Intelligence Integration**
  threat intelligence amplifies and enriches correlations to create custom insights.

* **Hunting**
  We'll dedicated hunting team proactively investigates activity that standard detections can miss.
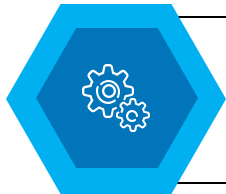
TZN Cybersecurity Maturity Model

TZN Cybersecurity Maturity model is a set of cybersecurity practices, standards, and processes developed and published by Tzamon professional team, divided into 4 levels and compatible with the NIST cybersecurity framework.

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

NIST FRAMEWORK

These levels conform to the highest international standards in the field of cybersecurity:

CMMC 2.0
Cybersecurity Maturity Model Certification

CYBERSECURITY MATURITY MODEL
CERTIFICATION
CENTER OF EXCELLENCE
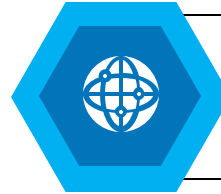
ISO 27001
International Organization for Standardization

Information Security Management
ISO 27001 Certified

COMPLIANCE & GOVERNANCE

- Data governance
    - Retention
    - Deletion
    - Backup
    - Restore
- Information protection
    - Data classification
    - Data loss prevention
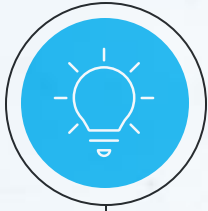- Auditing

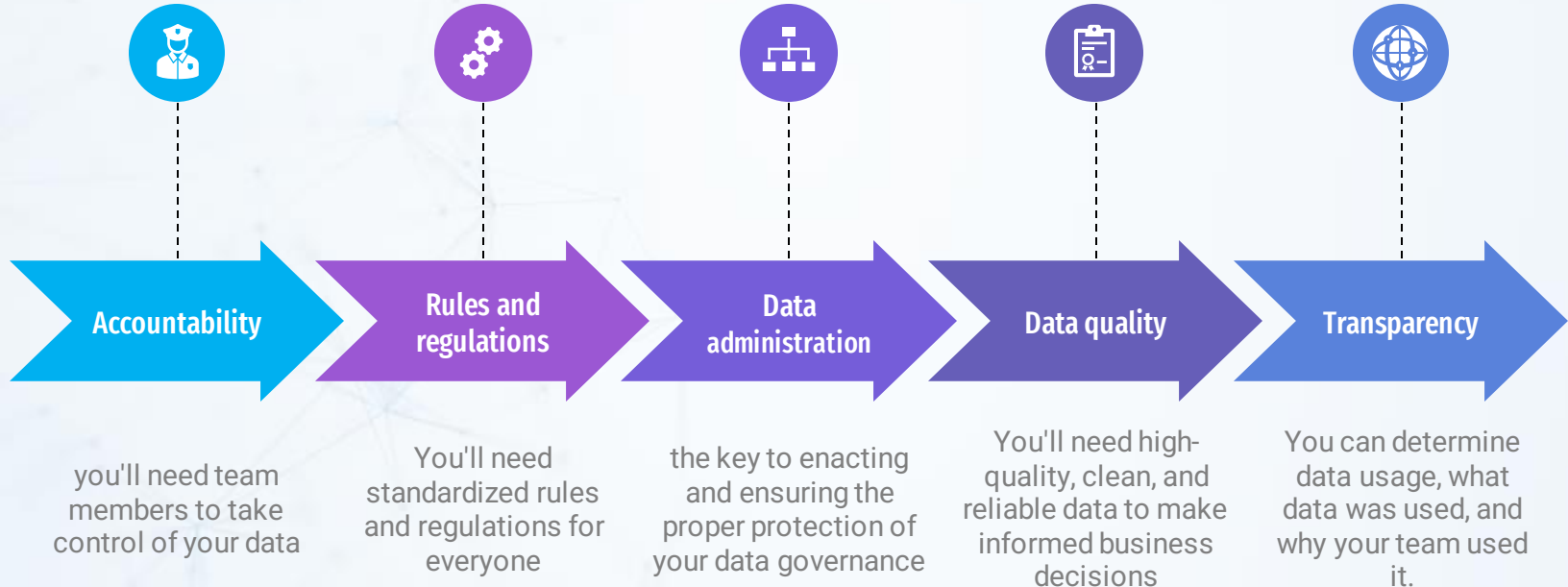# Data Lifecycle Management

Creation | Storage | Archival | Disposal

Data governance

collection of processes, policies, roles, metrics, and standards that ensures an effective and efficient use of information. This also helps establish data management processes that keep your data secured, private, accurate, and usable throughout the data life cycle

Accountability

Rules and regulations

Data administration

Data quality

Transparency

you'll need team members to take control of your data

You'll need standardized rules and regulations for everyone

the key to enacting and ensuring the proper protection of your data governance

You'll need high-quality, clean, and reliable data to make informed business decisions

You can determine data usage, what data was used, and why your team used it.

Microsoft Information Protection

Understand your data landscape and important data across your hybrid environment

Know Your Data

Apply flexible protection actions including encryption, access restrictions and visual markings

Protect Data

Prevent Data Loss

Prevent accidental oversharing of sensitive information

Auditing

Help organizations effectively respond to security events, forensic investigations, internal investigations, and compliance obligations.

Thousands of user and admin operations performed in dozens of Microsoft 365 services and solutions are captured, recorded, and retained in your organization's unified audit log.

Audit records for these events are searchable by security ops, IT admins, insider risk teams, and compliance and legal investigators in your organization.

This capability provides visibility into the activities performed across your Microsoft 365 organization.

Data Protection Baseline Assessment

Assess performance relative to key data protection standards and regulations.

Based on elements from:

- **NIST CSF** - National Institute of Standards and Technology Cybersecurity Framework
- **ISO** - International Organization for Standardization
- **FedRAMP** - Federal Risk and Authorization Management Program
- **GDPR** - General Data Protection Regulation of the European Union

Recommendations for improvement together with implementation guidance.

New and updated scenarios are published regularly.

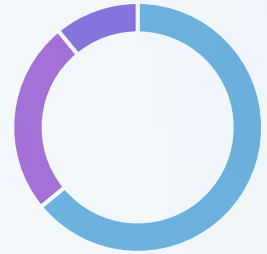**Your compliance score: 69%**

14598/21033 points achieved

Your points achieved ⓘ
129/6564

Microsoft managed points achieved ⓘ
14469/14469

Assessment

▪ Technical   ▪ Documentation   ▪ Operation ▪

Key improvement actions

Not completed	Completed	Out of scope
503	7	0

Improvement action	Impact	Test status	Group	Action type
Control your Azure Information Protection tenant key	+27 points	● None	Default Group	Technical
Issue public key certificates	+27 points	● None	Default Group	Operational
Activate Azure Rights Management	+27 points	● None	Default Group	Technical
Use IRM for Exchange Online	+27 points	● None	Default Group	Technical

THANKS

Does anyone have any questions?

Info@tzamon.ly