NOVENTIQ
Global expertise, local outcomes

Cybersecurity Maturity Assessment

Client:

Date:

Document properties

Title	Cybersecurity Maturity Assessment for Client Name
Classification	Confidential
Version	1.0
Date	DD.MM.GG

Version history

VERSION	COMMENTS	AUTHOR	DATE
1.0			DD.MM.GG

Executive summary

Short summary of organization current situation, identified strengths and weaknesses and possibilities for improvements.

Key findings

Most important findings regarding actual cyber risks in the organization

Key recommendations

Most important and urgent recommendations are based on actual cyber risks, findings, and Zero Trust model.

Contents

Executive summary **3**
Key findings 3
Key recommendations 3
Introduction **5**
Cybersecurity Maturity Assessment Results **6**
Current Maturity Level of organization 6
Target Maturity Level of organization 7
Details – existing situation 8
Identity 8
Devices 9
Network/Environment 10
Applications 10
Data 11
Details - Recommended Maturity Level 12
Identity 12
Devices 14
Network/Environment 14
Applications 14
Data 14
List of all recommendations **16**

Introduction

This Cybersecurity Maturity Assessment is based on The Zero Trust Maturity Model[1] that was developed by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) to help organisations implement a Zero Trust security model.

The model consists of five pillars: Identity, Devices, Network, Applications, and Data. Organisation's cybersecurity maturity is assessed in each pillar in accordance with maturity levels offered by the model – traditional, advanced an optimal.

Organisations in traditional level mostly have manual processes with very little automation, limited visibility and integrations across different environments, traditional security measures.

In advanced level, organisations have started to implement certain Zero Trust security principles and have some automation with decent visibility and integrations across cloud and on-premises environments.

Optimal level is the highest maturity level, where organisations have adopted the Zero Trust security, have fully automated workflows and full visibility into all organisation's assets and processes.

[1] CISA Zero Trust Maturity Model

Cybersecurity Maturity Assessment Results

Current Maturity Level of organization

This section (approx. 2 pages) describes existing model and identifies most important issues in more details than in Executive summary:

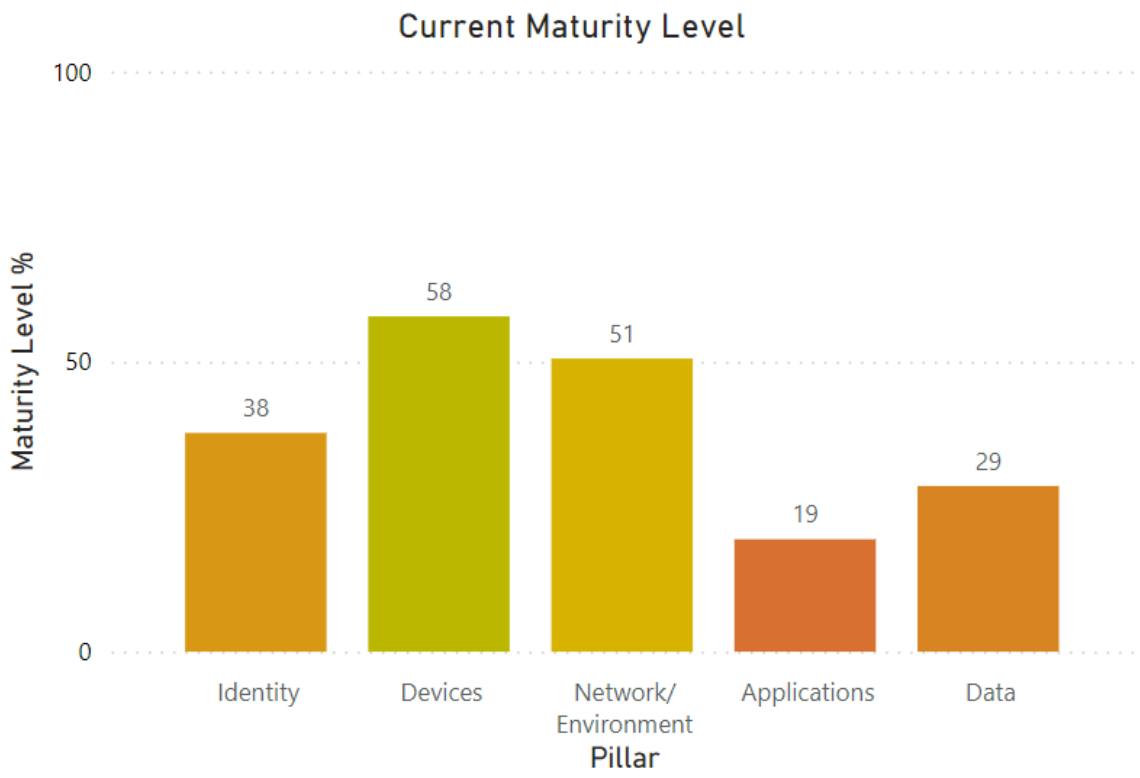

Figure 1 Current Zero Trust Maturity Level

[short summary]

Target Maturity Level of organization

This section (approx. 2 pages) describes optimal in organisation context (not always according to ZT) model in more details than in Executive summary.

Target model is based on our recommendations, organization capabilities, strategy, and risk appetite.

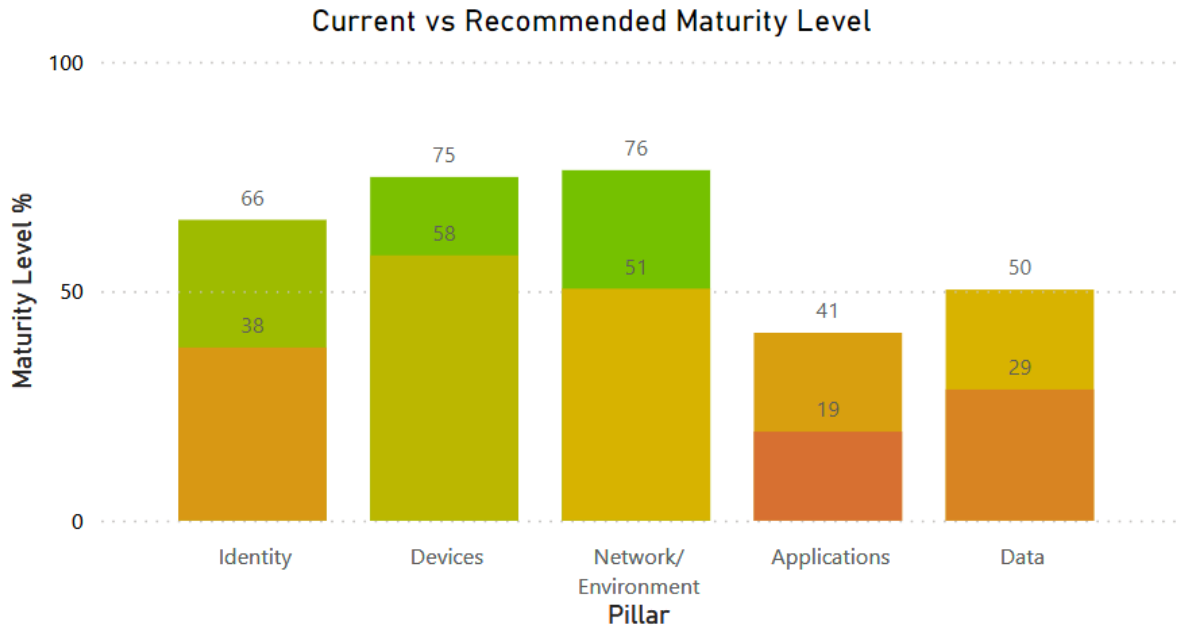

Figure 2 Current vs Recommended Zero Trust Maturity Level

[short summary of actions to get to target level]

Details – existing situation

This section describes in details existing situation in each pillar of Zero trust model

Identity

Level 38% – (low) Advanced

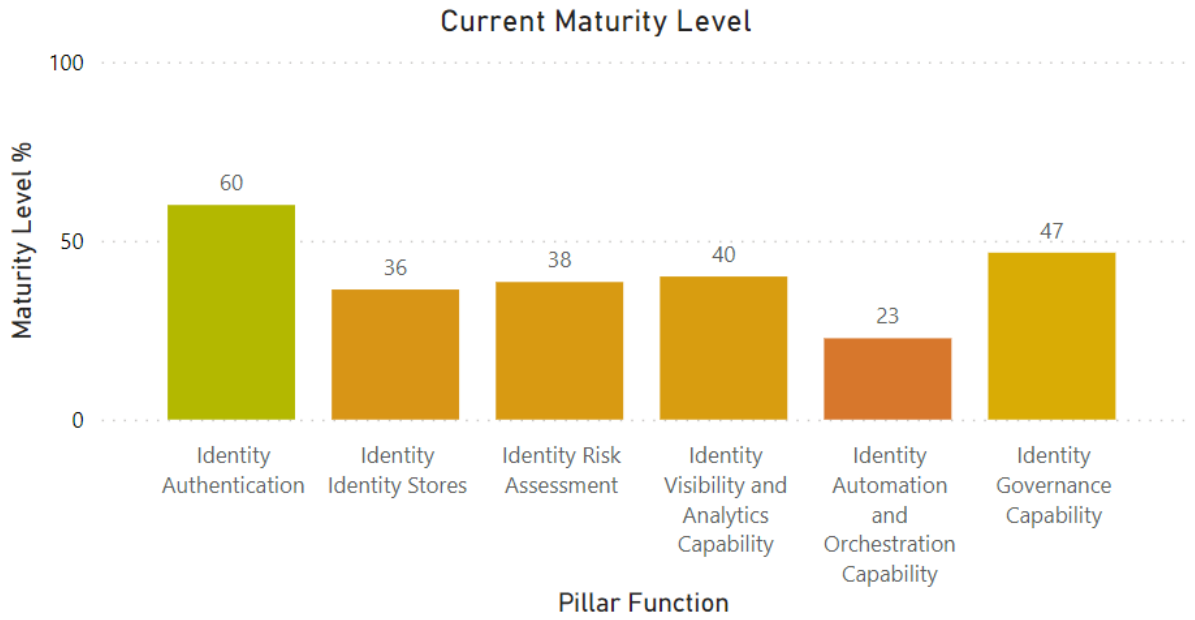

Figure 3 Current Zero Trust Maturity Level for Identity Pillar

Authentication

Level – (high) Advanced

Organisation has implemented Microsoft authenticator app for multi-factor authentication. However, there are still some legacy systems that uses password authentication. Authentication decisions are made at initial access only.

Identity stores

Level – (low) Advanced

Organisation's main identity store is Microsoft Active Directory integrated together with Azure Active Directory. There are some legacy systems with separate identity stores that are not integrated with the central identity store. Central IAM system is not used.

Risk Assessment

Level – (low) Advanced

Organisation uses Privileged Access Management (PAM) tools for Azure Active Directory access management, and separate administrator account for other systems. Only remote administrator connections require MFA. More than 20% of

users have administrative privileges on their workstations. There are no different authentication scenarios for different use cases, such as conditional access rules, requiring MFA from unrecognized locations, or for specific apps. The organization does not analyse user behaviour with real-time data and advanced ML algorithms to determine risk and deliver ongoing protection.

Visibility and Analytics Capability

Level – (low) Advanced

User identity events are sent to organisation's SIEM solution – Sentinel. However, it is not being closely monitored. Not all actions with privileged accounts/privileged tasks are audited. Organisation is not using advanced algorithms to analyse user behaviour across systems.

Automation and Orchestration Capability

Level – (mid) Traditional

The organization is using Single Sign-On (SSO) capabilities for most systems. Self-service password reset is enabled for user accounts in AAD/AD. User identities are not automatically created or updated with input from an HR system. However, organisation's helpdesk/ticketing system is used for tracking (initiating, approving) user role changes. The organization does not use an IAM system or similar solution for central user role and access management. User accounts do not get automatically suspended after the termination of employment, but there is a manual process in place.

Governance Capability

Level – (mid) Advanced

The organization has a formal policy defined for credential requirements and enforces credential requirements using static rules. There is a manual regular process for reviewing user accounts and their permissions to get rid of unnecessary accounts and permissions. Shared accounts are used for standard users, but not for privileged tasks. The organization only partly has a formal policy describing identity lifecycle management.

Devices

Compliance Monitoring

Level – (mid) Optimal

Data Access

Level – (low) Traditional

Asset Management

Level – (low) Advanced

Visibility and Analytics Capability

Level – (low) Optimal

Automation and Orchestration Capability

Level – (mid) Traditional

Governance Capability

Level – (high) Advanced

Network/Environment

Level – (mid) Advanced

Network Segmentation

Level – (high) Advanced

Threat Protection

Level – (high) Advanced

Encryption

Level – (high) Optimal

Visibility and Analytics Capability

Level – (mid) Advanced

Automation and Orchestration

Level – (low) Advanced

Governance Capability

Level – (high) Traditional

Applications

Level – (mid) Traditional

Access Authorization

Level – (mid) Traditional

Threat protection

Level – (mid) Traditional

Accessibility

Level – (mid) Traditional

Application Security

Level – (low) Traditional

Visibility and Analytics Capability

Level – (low) Traditional

Automation and Orchestration Capability

Level – (high)Traditional

Governance Capability

Level – (high) Advanced

Data

Level – (high) Traditional

Inventory management

Level – (high) Advanced

Description of the situation

Access Determination

Level – (mid) Traditional

Description of the situation

Encryption

Level – (high) Traditional

Description of the situation

Visibility and Analytics Capability

Level – (low) Traditional

Description of the situation

Automation and Orchestration Capability

Level – (high) Traditional

Description of the situation

Governance Capability

Level – (high) Traditional

Description of the situation.

Details - Recommended Maturity Level

This section describes in detail target maturity level and actions to achieve it in each pillar of Zero trust model. Target model is based on our recommendations, organization capabilities, strategy, and risk appetite.

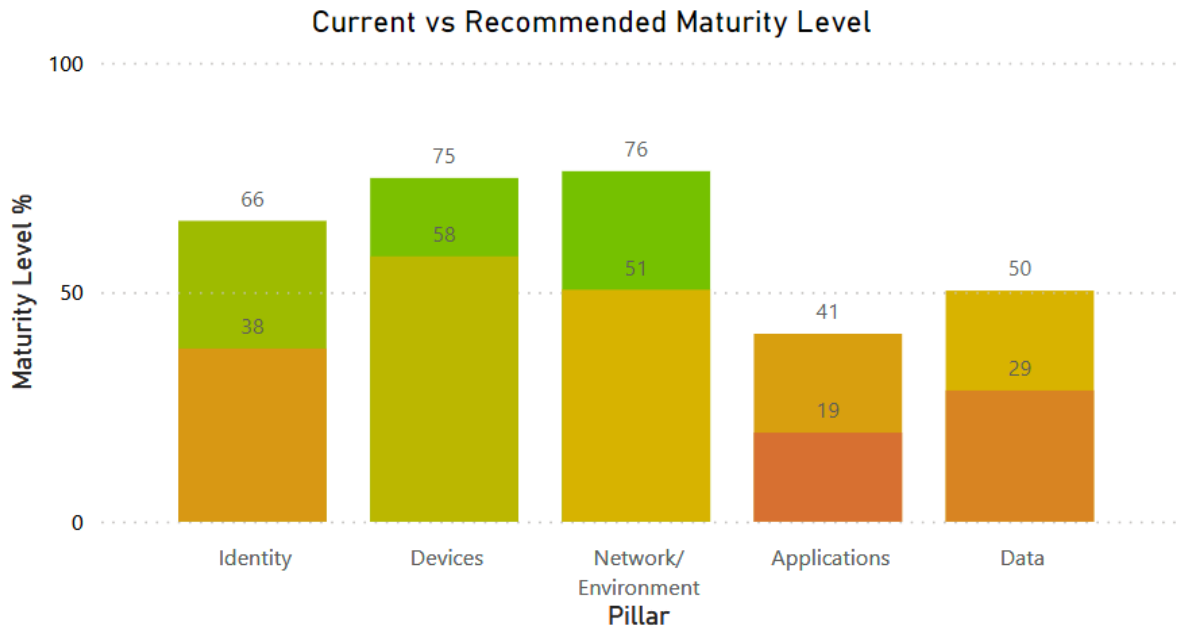

Figure 4 Current vs Recommended Zero Trust Maturity Level

Identity

Recommended Maturity Level – (High) Advanced (increase by 28%)

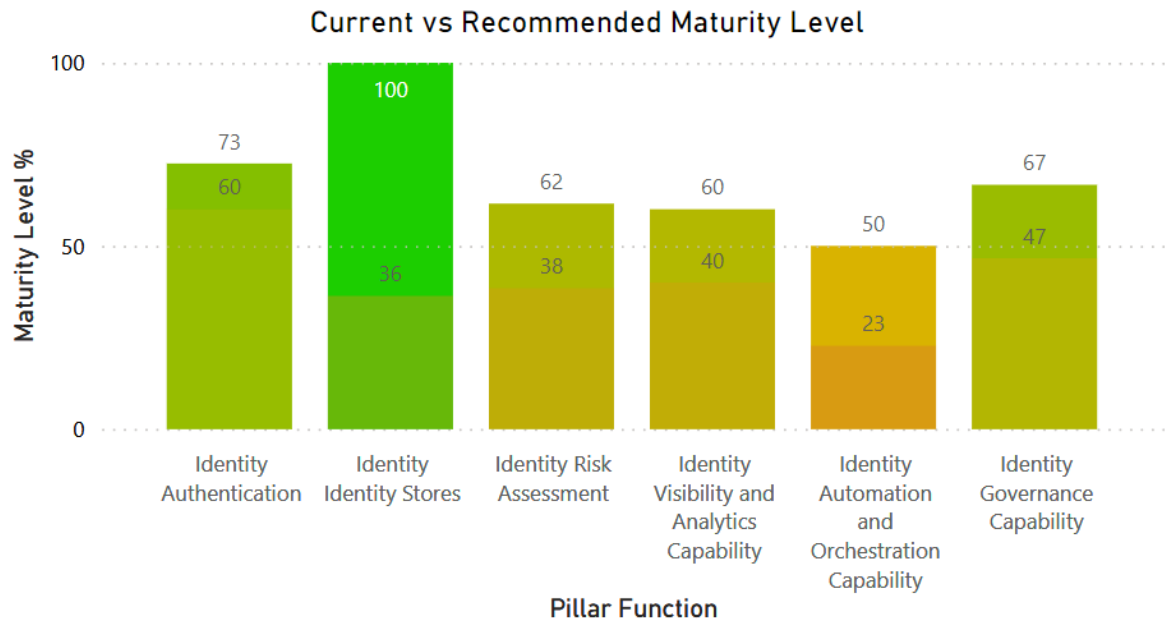

Figure 5 Current vs Recommended Zero Trust Maturity Level for Identity Pillar

Actions to Achieve Recommended Maturity Level

Following recommendations should be implemented if organisation wants to achieve recommended Zero Trust maturity level (see Figure 5).

Firstly, the main focus should be on consolidating all user identities and roles in one central system. This can be achieved by using organisation's AD/AAD as the identity store for all systems as well as for role management. This would allow for SSO capabilities to be leverage across all applications.

Organisation should:

- Identify apps that are not integrated with AD/AAD and build a roadmap for integrating them.
- Evaluate if your AAD/AD can be used for centralized user and role management across all systems and accounts.

Secondly,

…

Optional Recommendations

Following recommendations are optional and should be implemented if organisation wants to achieve higher Zero Trust maturity level.

Firstly, organisation should implement continuous authentication methods like risk-based conditional access in AAD and configure dynamic risk-based rules for credential requirements. Additionally, organisation should take advantage of ...

Secondly,

…

Devices

Recommended Maturity Level – (Low) Optimal (increase by 17%)

Actions to Achieve Recommended Maturity Level

Optional Recommendations

Following recommendations are optional and should be implemented if organisation wants to achieve

Network/Environment

Recommended Maturity Level – (Low) Optimal (increase by 25%)

Actions to Achieve Recommended Maturity Level

Following recommendations should be implemented if organization wants to achieve recommended Zero Trust maturity level (see **Error! Reference source not found.**).

Firstly,

Optional Recommendations

Following recommendations are optional and should be implemented if organisation wants to achieve higher Zero Trust maturity level.

Applications

Recommended Maturity Level – (Low) Advanced (increase by 22%)

Actions to Achieve Recommended Maturity Level

Following recommendations should be implemented if organisation wants to achieve recommended Zero Trust maturity level (see **Error! Reference source not found.**).

Optional Recommendations

Following recommendations are optional and should be implemented if organisation wants to achieve higher Zero Trust maturity level.

Data

Recommended Maturity Level – (Mid) Optimal (increase by 21%)

Actions to Achieve Recommended Maturity Level

Following recommendations should be implemented if organisation wants to achieve recommended Zero Trust maturity level (see **Error! Reference source not found.**).

Optional Recommendations

Following recommendations are optional and should be implemented if organisation wants to achieve higher Zero Trust maturity level.

List of all recommendations

Recommended actions

N.	Recommendation text	Process	Technology	Investments

Optional recommendations

N.	Recommendation text	Process	Technology	Investments

Column descriptions:

- Process - indicates that changes in processes are required.
- Technology - indicates that changes in system settings/configurations are required.
- Investments - indicates that additional investments are required for technology, software and/or consultations.