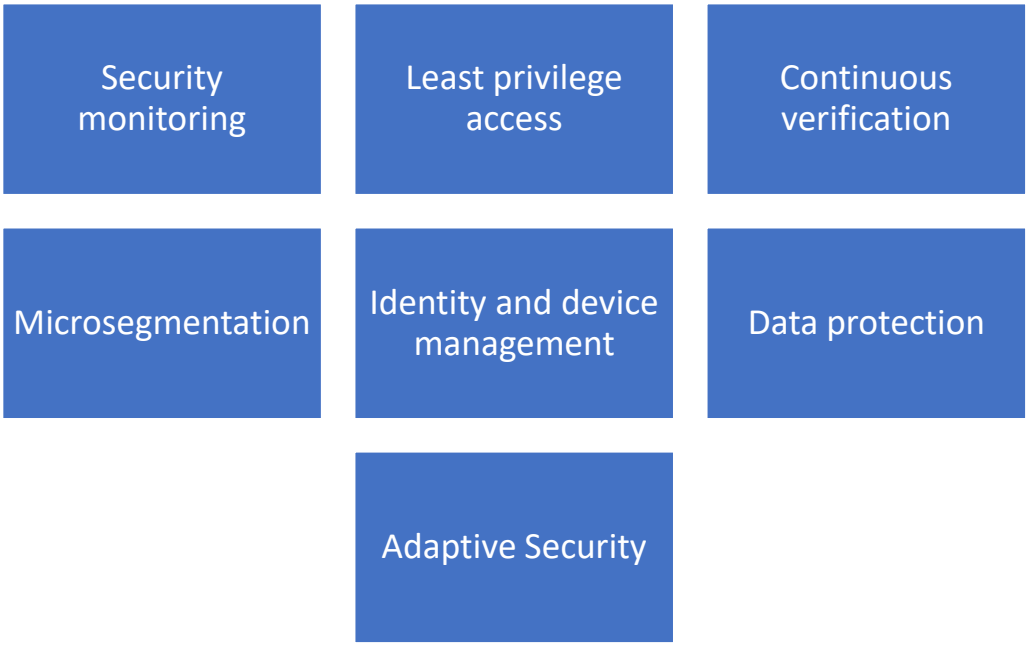
ZERO TRUST MATURITY MODEL| CISA POLICY EXPLAINED

1. Key Objectives of the Policy

CISA's Zero Trust Maturity Model (ZTMM) provides an approach to achieve continued modernization efforts related to zero trust within a rapidly evolving environment and technology landscape. This ZTMM is one of many paths that an organization can take in designing and implementing their transition plan to zero trust architectures in accordance with Executive Order (EO) 14028 "Improving the Nation's Cybersecurity."

Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. ZTA is an enterprise's cybersecurity plan that uses zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a ZTA plan.

The key objectives of the policy are:



2. Impact on Data Management and Governance

a. Enhanced data security

ZTMM has impacted on data management and Governance by improving data security through the introduction of strict access controls, granular data protection mechanisms and reduced unauthorised data exposure.

b. Improved Data Governance

ZTMM has impacted data management by introducing comprehensive data tracking across an enterprise entity, the use of precise user access logging has resulted in clear accountability for data interactions.

c. Risk mitigation

ZTMM has impacted Data Management positively as data is continuously monitored through its data flows. ZTMM has resulted in immediate threat detection due to coordinated and collaborative components of a zero trust strategy, with agency-wide buy in for a common architecture and governance policies. It has also encouraged rapid response to potential breaches enhancing good data governance.

d. Compliance management

Automated compliance tracking is being practised in entities as a result of the introduction of ZTMM. Detailed audit trails are considered a mandate in this policy. Due to the collaboration of data and inventory taking of data assets this has simplified regulatory reporting.

e. Data Integrity Preservation

Data is maintained and secured by introduction of encryption at multiple layers. Data access and changes are always verified making data a valuable asset. Unauthorised modifications of data are prevented due to enhanced security.

f. Dynamic access management

This has improved productivity by creating context-aware data permissions, real time access adjustments and role based data governance. This has also enhanced end user experiences.

g. Holistic data visibility

ZTMM has enhanced end user experiences by creating a comprehensive data landscape understanding and transparent data movement tracking. This policy has bolstered security by introducing a unified security perspective across environments.

3. How ZTMM relates to the Broader Federal Data Strategy or Government Framework

Broader Federal Data Strategy	Federal Data Strategy (FDS)
Data Security	-Strengthens protection of sensitive government data -Enforces strict access controls across agencies -Ensures data integrity in federal systems
Data Governance	-Aligns with federal data management policies -Supports standardised data handling procedures -Enhances accountability in data access
Mission Support	-Enables secure data sharing between agencies -Facilitates protected interagency collaboration -Supports data-driven decision making
Compliance	-Helps meet federal security requirements -Ensures adherence to privacy regulations -Supports FISMA and NIST guidelines

4. Potential Challenges or Considerations for Implementation of ZTMM

a. Legacy systems

Integration difficulties may occur due to the old equipment and software already used in federal agencies failing to cope with required new capabilities.

b. Existing Infrastructure

The existing infrastructure built on implicit trust will require investment to change systems and modifications to better align with zero trust principles. There is need to invest in specialised expertise, training requirements for staff resulting in high initial implementation costs.

c. Engagement and cooperation of senior leadership

Implementation of ZTMM will result in change management challenges within the federal government as some stakeholders might prefer the old methods of doing work than the new coordinated and collaborative approach ZTMM brings.

d. Transition from siloed IT systems to coordinated and collaborative approaches to data security

Agencies will be required to adopt common architecture or governance policies which can result in compatibility issues with the existing systems. A need for third party vendor management will be required which might not be welcomed as it might be considered a security threat.

e. Performance impact

There will be potential system slowdown due to upgrades and integration initiatives. Development of complex policy framework will be required to adopt the policy; this can conflict with operational continuity as there is a need to maintain business operations and minimise service disruptions. Regulatory requirements must be met for compliance issues and audit trail maintenance will be a must have policy in agencies