Measuring Your Zero Trust Maturity

Elizabeth Schweinsberg

Centers for Medicare and Medicaid Services

DIGITAL SERVICE AT CMS

Who Am I?

Elizabeth Schweinsberg, Digital Services Expert at U.S. Digital Service

Detailed to Centers for Medicare and Medicaid Services (CMS) for 2.5 yrs, leading their Zero Trust architecture since Summer 2021.

Longtime practitioner of Digital Forensics, Incident Response, and Threat Detection in corporate environments, turned Zero Trust "Architect".

U.S. DIGITAL SERVICE

CMS

CENTERS FOR MEDICARE & MEDICAID SERVICES

Agenda

What is Zero Trust?

Overview of the CISA Zero Trust Maturity Model

Applying Zero Trust to environments

CMS measured our Zero Trust maturity

Creating your own framework

Do the next best thing

What is Zero Trust??

It’s like trying to get to your seat at a professional sports game:

- Bag check and metal detector
- Ticket gets scanned
- When you get to your section, ticket gets checked again
- Some sections (e.g. club level) will have a 3rd ticket check

Photo from: https://www.sportsfanisland.com/products/oriole-park-at-camden-yards-mlb-baltimore-orioles-brxlz-stadium-blocks-set

Three Popular Zero Trust Frameworks

NIST SP 800-207 Zero Trust Architecture

- 7 Tenets, 3 architecture approaches

DOD Zero Trust Reference Architecture

- 7 Pillars with different functions and 3 maturity levels

CISA Zero Trust Maturity Model

- 5 Pillars with functions, 3 cross cutting functions, and 4 maturity levels

CISA Zero Trust Maturity Model

5 Pillars with functions

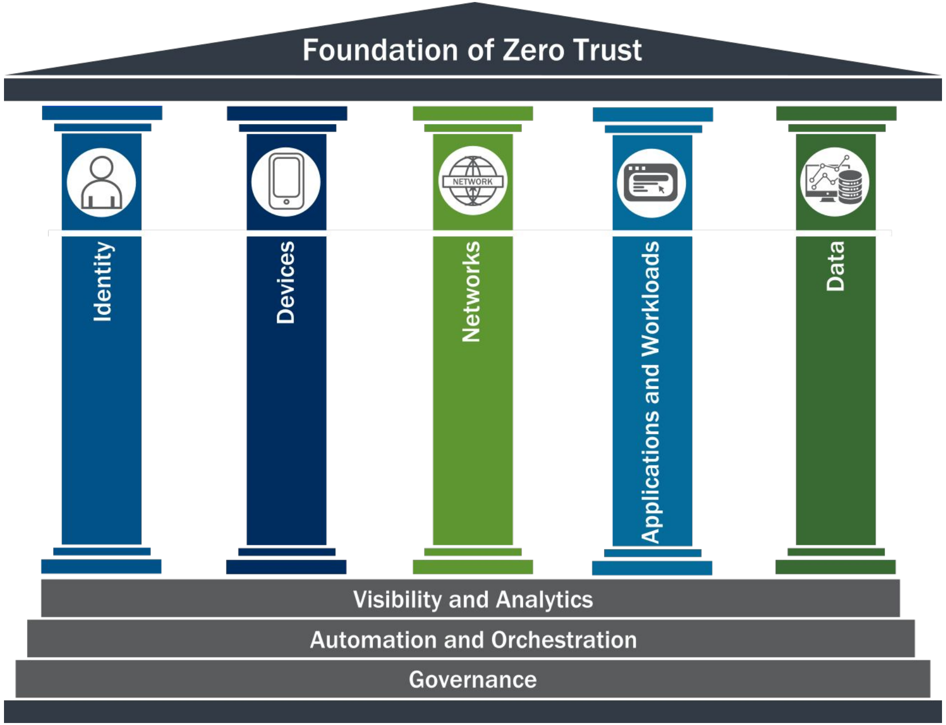
- Identity
- Devices
- Networking
- Applications and Workloads
- Data

3 cross-cutting functions

- Visibility and Analytics
- Automation and Orchestration
- Governance

4 levels of maturity

- Traditional
- Initial
- Advanced
- Optimal



CISA Zero Trust Maturity Levels

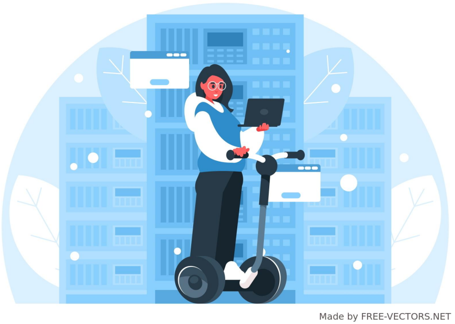
Traditional	Initial	Advanced	Optimal
● Manual configured ● Siloed pillars ● Set at provisioning ● Limited visibility	● Starting to have automation ● Some cross-pillar integration ● Time-based changes ● Aggregated visibility	● Automated wherever applicable ● Policy enforcement integrated across pillars ● Changes based on risk & posture assessments ● Centralized visibility	● Fully automated, just-in-time ● Cross-pillar interoperability with continuous monitoring ● Dynamically set for enterprise-wide ● Centralized with situational awareness

Applying Zero Trust to environments

Zero Trust in your Enterprise vs On-prem data center vs. Infrastructure as a Service (IaaS) provider

Pimlico Image from: https://commons.wikimedia.org/wiki/File:142nd_Preakness_Stakes_Pimlico_Race_Course_%2834438184460%29.jpg

Identity in Different Environments


Made by FREE-VECTORS.NET

Enterprise

Staff and Contractors using business applications

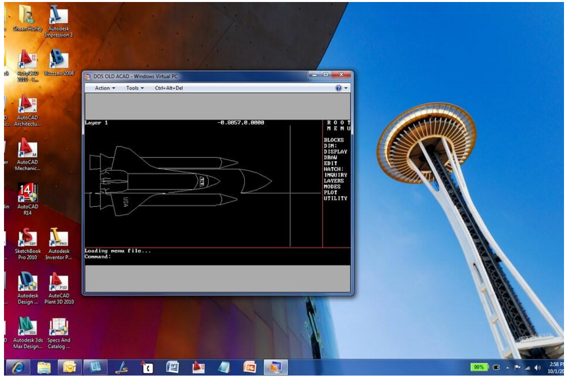
On-Prem Data Center

System administrators and developers launching software AND users of our services

IaaS

System administrators and developers launching software AND users of our services

Devices in Different Environments



```
Layer 1                    -0.8057,0.0000
```

```
Loading menu file...
Command:
```

Enterprise

Laptops and mobile phones

On-Prem Data Center

Servers in Racks

IaaS

Virtual Machines and Containers

Creating your own framework

1. Decide on which environment to evaluate
2. Change the maturity levels for each Pillar/function pair to match what you want your environment to have
3. Write questions that help you determine what level a system for the pillars and functions
4. Get teams to fill out the questionnaire
5. Grade the questionnaire
6. Give the teams feedback on their levels
7. Write up how to increase the maturity of the functions with the most room to improve

Creating an environment specific maturity model

How CMS got started

CISA vs. IaaS: Identity

Model	Function	Traditional	Initial	Advanced	Optimal
CISA	Authentication	Agency authenticates identity using either passwords or multi-factor authentication (MFA) with static access for entity identity.	Agency authenticates identity using MFA, which may include passwords as one factor and requires validation of multiple entity attributes (e.g., locale or activity).	Agency begins to authenticate all identity using phishing-resistant MFA and attributes, including initial implementation of password-less MFA via FIDO2 or PIV.	Agency continuously validates identity with phishing-resistant MFA, not just when access is initially granted.
IaaS	Authentication - Developers	Team members authenticate with Username/Password, multi-factor authentication (MFA). Access does not take into account any additional attributes.	Team members authenticate MFA, which may include passwords as one factor. Also incorporates 1 additional attribute into access (e.g. SASE use or a device signal).	Team members authenticate via phishing-resistant MFA. Initial access accepts at least one device level or proofing signal for dynamic access control.	Team member's identity is continuously validated, not only for initial access but also throughout the lifecycle of the session; only uses phishing-resistant MFA. Uses dynamic, attribute-based access control.

CISA vs. IaaS: Identity > Authentication > Traditional

Model	Function	Traditional
CISA	Authentication	Agency authenticates identity using either passwords or multi-factor authentication (MFA) with static access for entity identity.
IaaS	Authentication - Developers	Team members authenticate with Username/Password, multi-factor authentication (MFA). Access does not take into account any additional attributes.

CISA vs. IaaS: Identity > Authentication > Initial

Model	Function	Initial
CISA	Authentication	Agency authenticates identity using MFA, which may include passwords as one factor and requires validation of multiple entity attributes (e.g., locale or activity).
IaaS	Authentication - Developers	Team members authenticate MFA, which may include passwords as one factor. Also incorporates 1 additional attribute into access (e.g. SASE use or a device signal).

CISA vs. IaaS: Identity > Authentication > Advanced

Model	Function	Advanced
CISA	Authentication	Agency begins to authenticate all identity using phishing-resistant MFA and attributes, including initial implementation of password-less MFA via FIDO2 or PIV.
IaaS	Authentication - Developers	Team members authenticate via phishing-resistant MFA. Initial access accepts at least one device level or proofing signal for dynamic access control.

CISA vs. IaaS: Identity > Authentication > Optimal

Model	Function	Optimal
CISA	Authentication	Agency continuously validates identity with phishing-resistant MFA, not just when access is initially granted.
IaaS	Authentication - Developers	Team member's identity is continuously validated, not only for initial access but also throughout the lifecycle of the session; only uses phishing-resistant MFA. Uses dynamic, attribute-based access control.

CISA vs. IaaS: Devices

Model	Function	Traditional	Initial	Advanced	Optimal
CISA	Governance	Agency sets some policies for the lifecycle of their traditional and peripheral computing devices and relies on manual processes to maintain (e.g., update, patch, sanitize) these devices.	Agency sets and enforces policies for the procurement of new devices, the lifecycle of non-traditional computing devices and virtual assets, and for regularly conducting monitoring and scanning of devices.	Agency sets enterprise-wide policies for the lifecycle of devices and virtual assets, including their enumeration and accountability, with some automated enforcement mechanisms.	Agency automates policies for the lifecycle of all network-connected devices and virtual assets across the enterprise.
IaaS	Governance	Team has some lifecycle policies for the digital assets in their application. They rely on manual processes to maintain the devices. Gold Images may be used.	Team has a documented device lifecycle plan, which is implemented manually. Monitoring and scanning of devices is automated. Routine patching is done monthly. Gold Images are used where possible.	Device lifecycle plan is implemented both manually and automatically. Gold Images are used where possible. Routine patching is done at least every two weeks. System automates notifications for device policy deviations.	Device lifecycle plan is automated. Gold Images are used where possible. Routine patching is done at least every two weeks. Team employs auto-remediation for device non-compliance.

CISA vs. IaaS: Devices > Governance > Traditional

Model	Function	Traditional
CISA	Governance	Agency sets some policies for the lifecycle of their traditional and peripheral computing devices and relies on manual processes to maintain (e.g., update, patch, sanitize) these devices.
IaaS	Governance	Team has some lifecycle policies for the digital assets in their application. They rely on manual processes to maintain the devices. Gold Images may be used.

CISA vs. IaaS: Devices > Governance > Initial

Model	Function	Initial
CISA	Governance	Agency sets and enforces policies for the procurement of new devices, the lifecycle of non-traditional computing devices and virtual assets, and for regularly conducting monitoring and scanning of devices.
IaaS	Governance	Team has a documented device lifecycle plan, which is implemented manually. Monitoring and scanning of devices is automated. Routine patching is done monthly. Gold Images are used where possible.

CISA vs. IaaS: Devices > Governance > Advanced

Model	Function	Advanced
CISA	Governance	Agency sets enterprise-wide policies for the lifecycle of devices and virtual assets, including their enumeration and accountability, with some automated enforcement mechanisms.
IaaS	Governance	Device lifecycle plan is implemented both manually and automatically. Gold Images are used where possible. Routine patching is done at least every two weeks. System automates notifications for device policy deviations.

CISA vs. IaaS: Devices > Governance > Optimal

Model	Function	Optimal
CISA	Governance	Agency automates policies for the lifecycle of all network-connected devices and virtual assets across the enterprise.
IaaS	Governance	Device lifecycle plan is automated. Gold Images are used where possible. Routine patching is done at least every two weeks. Team employs auto-remediation for device non-compliance.

CISA vs. IaaS: Data

Model	Function	Traditional	Initial	Advanced	Optimal
CISA	Data Encryption	Agency encrypts minimal agency data at rest and in transit and relies on manual or ad hoc processes to manage and secure encryption keys.	Agency encrypts all data in transit and, where feasible, data at rest (e.g., mission critical data and data stored in external environments) and begins to formalize key management policies and secure encryption keys	Agency encrypts all data at rest and in transit across the enterprise to the maximum extent possible, begins to incorporate cryptographic agility, and protects encryption keys (i.e., secrets are not hard coded and are rotated on a regular basis).	Agency encrypts data in use where appropriate, enforces least privilege principles for secure key management enterprise-wide, and applies encryption using up-to-date standards and cryptographic agility to the extent possible.
IaaS	Data Encryption	Team only encrypts some data stores at rest or in transit. Team relies on manual or ad hoc processes to manage and secure encryption keys.	Team encrypts all data at rest and all data in transit outside of the IaaS account. Team has begun to formalize key management policies and secure encryption keys.	Team encrypts all data at rest and in transit (both within and outside of the IaaS account) to the maximum extent possible. Team incorporates cryptographic agility into their processes and protects encryption keys.	Team encrypted data in use where appropriate. Team enforces least privilege for key management, and applies encryption using up-to-date standards and cryptographic agility to the extent possible.

CISA vs. IaaS: Data > Encryption > Traditional

Model	Function	Traditional
CISA	Data Encryption	Agency encrypts minimal agency data at rest and in transit and relies on manual or ad hoc processes to manage and secure encryption keys.
IaaS	Data Encryption	Team only encrypts some data stores at rest or in transit. Team relies on manual or ad hoc processes to manage and secure encryption keys.

CISA vs. IaaS: Data > Encryption > Initial

Model	Function	Initial
CISA	Data Encryption	Agency encrypts all data in transit and, where feasible, data at rest (e.g., mission critical data and data stored in external environments) and begins to formalize key management policies and secure encryption keys
IaaS	Data Encryption	Team encrypts all data at rest and all data in transit outside of the IaaS account. Team has begun to formalize key management policies and secure encryption keys.

CISA vs. IaaS: Data > Encryption > Advanced

Model	Function	Advanced
CISA	Data Encryption	Agency encrypts all data at rest and in transit across the enterprise to the maximum extent possible, begins to incorporate cryptographic agility, and protects encryption keys (i.e., secrets are not hard coded and are rotated on a regular basis).
IaaS	Data Encryption	Team encrypts all data at rest and in transit (both within and outside of the IaaS account) to the maximum extent possible. Team incorporates cryptographic agility into their processes and protects encryption keys.

CISA vs. IaaS: Data > Encryption > Optimal

Model	Function	Optimal
CISA	Data Encryption	Agency encrypts data in use where appropriate, enforces least privilege principles for secure key management enterprise-wide, and applies encryption using up-to-date standards and cryptographic agility to the extent possible.
IaaS	Data Encryption	Team encrypted data in use where appropriate. Team enforces least privilege for key management, and applies encryption using up-to-date standards and cryptographic agility to the extent possible.

Collecting data at scale

Survey questions for fun and profit

Creating Questions: Identity

Authentication

Q. Which Multifactor Authentication methods are available?

❑ Email
❑ SMS
❑ OTP or Push from authenticator app (Google Authenticator or DUO)
❑ OTP from a hardware token
❑ PIV/certificate
❑ FIDO2/WebAuthn
❑ None

Authentication

Q. Is Multifactor Authentication required?

❑ Yes
❑ No

Creating Questions: Devices

Device Governance

Q. Do you have a documented device lifecycle plan?

❑ Yes
❑ No

Device Governance

Q. At what frequency are patches deployed?

❑ Automatically when a patch is released
❑ Weekly
❑ Every 2 Weeks
❑ Monthly
❑ Longer

Creating advice on how to improve Zero Trust maturity

Function Breakdown

Device	**A**	**Identity**	**A**	**Network**	**A**	**Apps**	**O**	**Data**	**T**
Compliance Monitoring	A	Identity Stores - Developers	A	Network Segmentation	O	Access Authorization - Users	O	Inventory Management*	N/A
Data Access*	N/A	Identity Stores - Users	A	Threat Protection	T	Access Authorization - APIs	O	Data Labeling	A
Asset Management		Identity Stores - APIs	A	Encryption	O	Threat Protections	O	Access Determination	T
Automation and Orchestration	A	Authentication - Users	A	Automation and Orchestration	T	Application Security	A	Encryption*	N/A
Visibility and Analytics	O	Authentication - Developers	A	Visibility and Analytics	T	Accessibility*	N/A	Logging	T
Governance	A	Authentication - NPEs	A	Governance	T	Automation and Orchestration	O	Automation and Orchestration	A
		Risk Assessment	A			Visibility and Analytics	A	Visibility and Analytics	T
		Automation and Orchestration	A			Governance	O	Governance	A
		Visibility and Analytics	A						
		Governance	A						

* We did not collect enough data on these functions to evaluate.

T - Traditional
A - Advanced
O - Optimal

Find the highs and lows

Which functions have the most room for improvement?

    What is the lowest average score(s)?

Which functions have the least room for improvement?

    What is the highest average score(s)?

Which functions can teams improve themselves?

Which functions need to be improved by the team running the IaaS organization?

Find the areas that are the most different

High variance implies there is not enough guidance in an area.

Low variance implies there is probably a strong standard for a function.

- Which functions have the most variance (e.g. high standard deviation)?
- Which functions have the least variance (e.g. low standard deviation)?

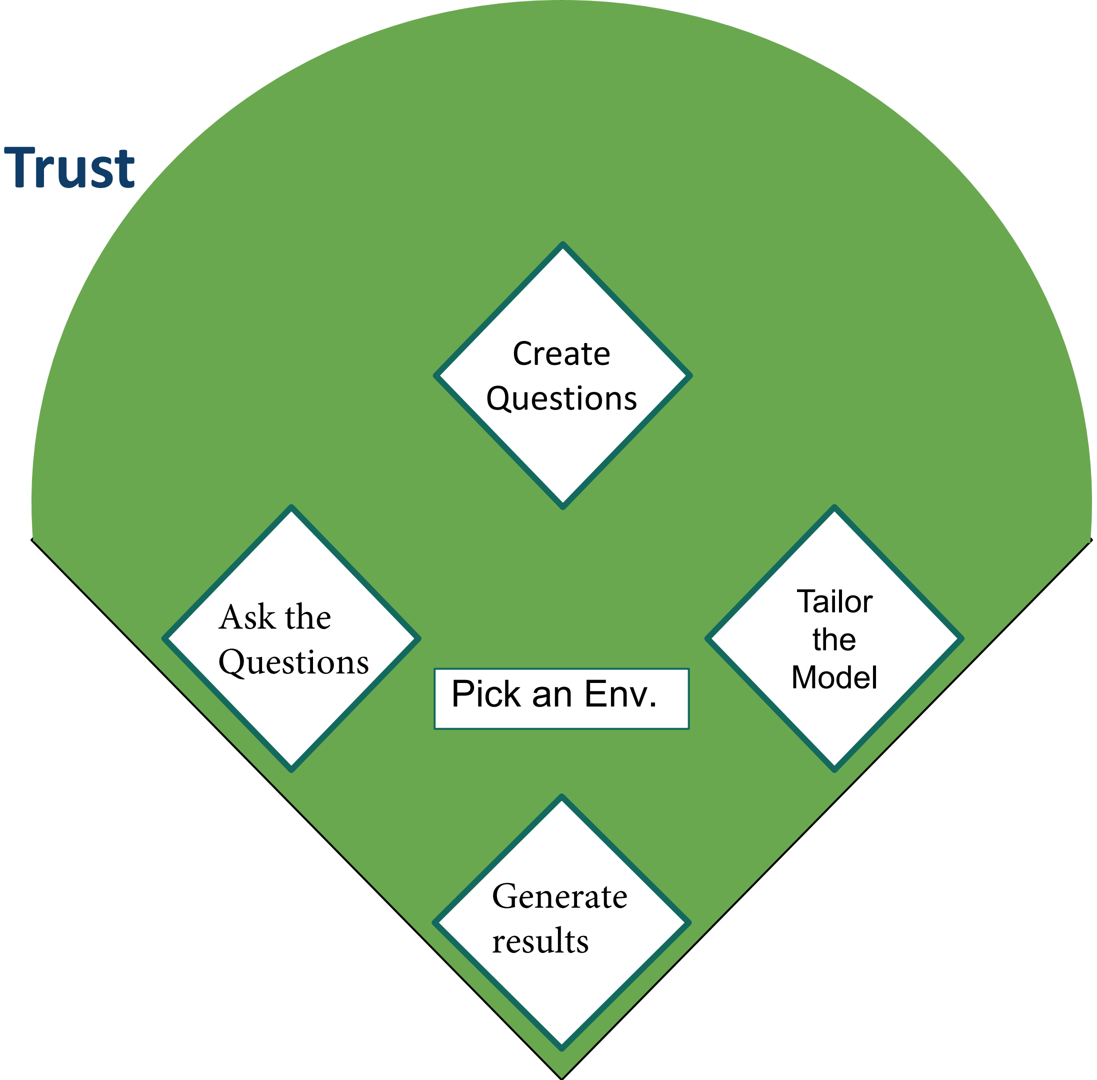
Note: I am not a data scientist, but I am pretty good at spreadsheets.

Measuring your own Zero Trust maturity

Pick an environment.

Draft a team to write the model.

Run the bases and score a home run!



Creating your own framework

1. Decide on which environment to evaluate
2. Change the maturity levels for each Pillar/function pair to match what you want your environment to have
3. Write questions that help you determine what level a system for the pillars and functions
4. Get teams to fill out the questionnaire
5. Grade the questionnaire
6. Give the teams feedback on their levels
7. Write up how to increase the maturity of the functions with the most room to improve

Some parts of Zero Trust take a long time

Moving to passwordless authentication

Deploying CDM and EDR on every device

Fully micro-segmenting your network

Adding real-time risk analytics to application access authorization

Completely automated data inventory and tagging

But somethings you can do now with what you have

Incremental progress builds momentum

What is one improvement in each pillar?

❑ Enable additional MFA options, maybe turn some off
❑ Make sure everyone has a device lifecycle plan, and an explicit patching cadence
❑ Add encryption to data in transit in your IaaS accounts
❑ Standardize expectations for static application security testing
❑ Add encryption to data at rest in your IaaS accounts

DIGITAL SERVICE AT CMS

Elizabeth Schweinsberg

elizabeth.schweinsberg@cms.hhs.gov

elizabeth.m.schweinsberg@omb.hhs.gov

@bethlogic on Twitter