CISA Zero Trust Maturity Model audit checklist

Traditional stage

✔	Audit controls	Examples of audit evidence
	IDENTITY PILLAR	
☐	Access to information resources is granted via a password and/or MFA	*Access controls policies, procedures; screenshots of access control processes*
☐	Risk assessments performed periodically on how user identity is confirmed	*Sample risk assessment reports*
	DEVICE PILLAR	
☐	Device compliance with cybersecurity standards and guidance is nominally assessed	*Reports on device compliance assessments; screenshots of device security features enabled*
☐	Inventory of cybersecurity devices is available and regularly updated	*Example of device inventory report; screenshots of inventory schedules*
	NETWORK/ENVIRONMENT PILLAR	
☐	Network perimeter is periodically assessed	*Reports on network perimeter assessments; screenshots of perimeter security status*
☐	Network traffic is minimally encrypted	*Screenshots of steps taken to encrypt network traffic*
	APPLICATION WORKLOAD PILLAR	
☐	Security for resources is handled locally	*Screenshots of security features for applications*
☐	Access to cloud resources is available	*Screenshots of data storage resources; contracts with cloud providers*
	DATA PILLAR	
☐	Some data is inventoried	*Screenshots of data inventories*
☐	Data is occasionally encrypted	*Screenshots of steps taken to encrypt data*

Advanced stage

✔	Audit controls	Examples of audit evidence
	IDENTITY PILLAR	
☐	Access is granted using MFA	*Access controls policies, procedures; screenshots of access control processes*
☐	Expanded identity controls are in place on site and for cloud-based services	*Documents listing identity controls; screenshots of data access processes for on-site and cloud services*

	DEVICE PILLAR	
☐	Device compliance is reviewed and enforced	*Reports on assessments of device compliance; policy for device security enforcement*
☐	Device status must be established before it can be accessed	*Policies for device status and access; screenshots of device access procedures*
	NETWORK/ENVIRONMENT PILLAR	
☐	Network perimeter is more segmented and rigorously protected for inbound and outbound traffic	*Reports on network perimeter assessments; screenshots of perimeter security status*
☐	Network traffic is regularly analyzed for anomalies	*Screenshots of network traffic analyses and results identified*
	APPLICATION WORKLOAD PILLAR	
☐	Centralized authentication is used for access	*Screenshots of application authentication steps; policies for application authentication*
☐	Cybersecurity is embedded in some application workflows	*Screenshots of application cybersecurity steps; policies for application cybersecurity*
	DATA PILLAR	
☐	Least privilege access has been established	*Policies for data access; screenshots of data access rules and procedures*
☐	Data at rest is encrypted, especially in off-site locations	*Screenshots of steps taken to encrypt data; policies for data encryption*

Optimal stage

✔	**Audit controls**	**Examples of audit evidence**
	IDENTITY PILLAR	
☐	User identity is continually validated for access	*Access controls policies, procedures; screenshots of access control processes*
☐	AI is used to analyze identity	*Access controls policies, procedures; screenshots of access control processes*
	DEVICE PILLAR	
☐	Device security is continually monitored and assessed	*Policies for device status and access; screenshots of device security features and procedures*
☐	Risk analysis data supports user access	*Risk analysis reports detailing device access*
	NETWORK/ENVIRONMENT PILLAR	
☐	Secure microperimeters in use and regularly updated	*Reports on network perimeter assessments; screenshots of perimeter security status; policies for network perimeter security*
☐	AI supports threat identification and protection	*Screenshots of perimeter security features and processes*
☐	All network traffic is encrypted	*Screenshots of steps taken to encrypt network traffic; policies stating that all traffic must be encrypted*

	APPLICATION WORKLOAD PILLAR	
☐	Access to applications is continuously monitored and revalidated	*Access controls policies, procedures; screenshots of access control processes; reports on application security performance*
☐	Cybersecurity elements embedded in all application workflows	*Policy on cybersecurity in all application workflows; screenshots of security features in applications*
	DATA PILLAR	
☐	All data is encrypted, whether in motion or at rest	*Screenshots of steps taken to encrypt data; policies stating that all data must be encrypted*
☐	Proactive data management processes in place	*Policies regarding data management; screenshots of data-identifying cybersecurity components*