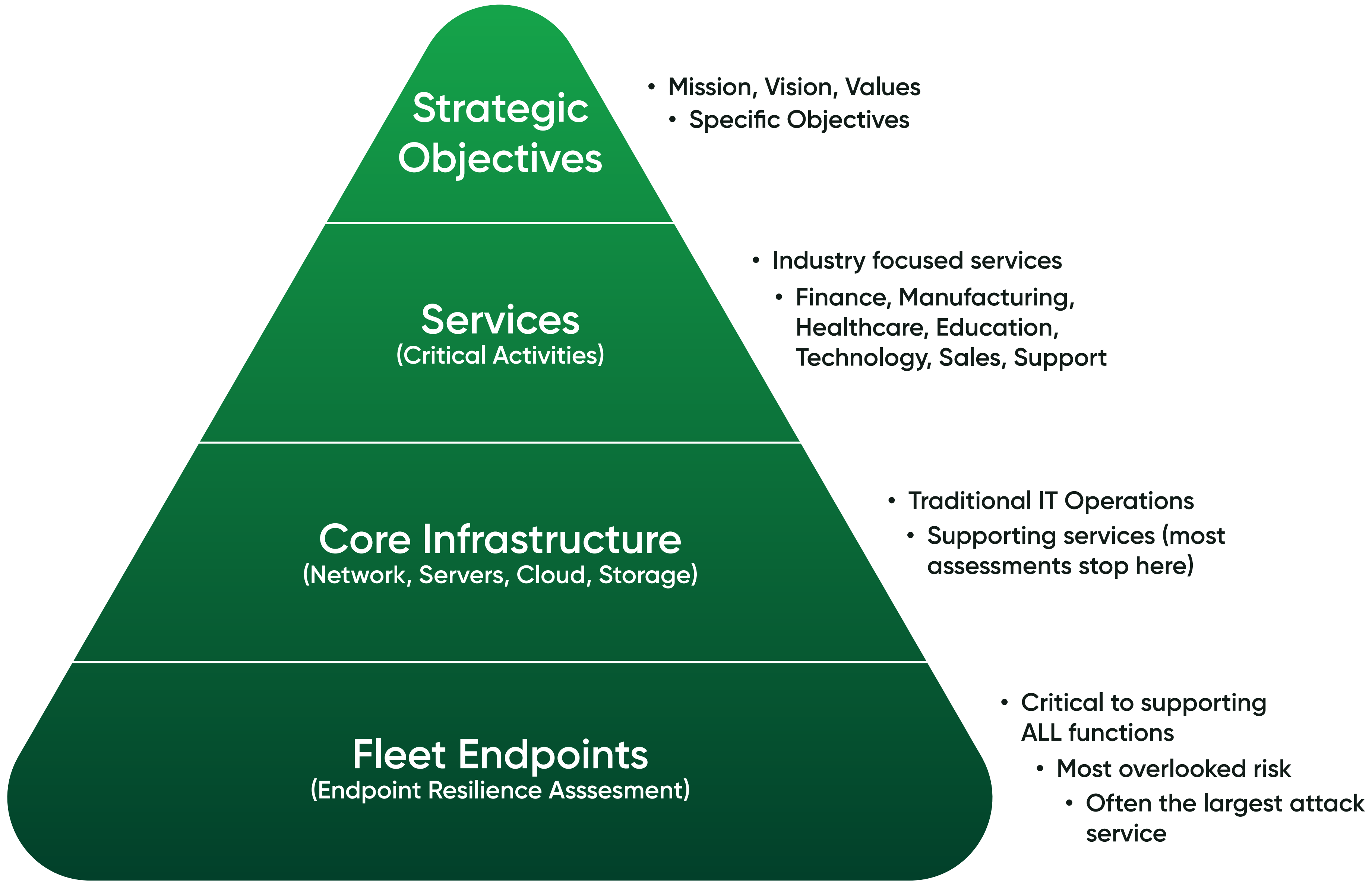
DATA SHEET

Absolute Endpoint Resilience Assessment

The Endpoint Resilience Assessment provides organizations the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions.


Strategic Objectives
• Mission, Vision, Values
• Specific Objectives
Services
(Critical Activities)
• Industry focused services
• Finance, Manufacturing, Healthcare, Education, Technology, Sales, Support
Core Infrastructure
(Network, Servers, Cloud, Storage)
• Traditional IT Operations
• Supporting services (most assessments stop here)
Fleet Endpoints
(Endpoint Resilience Asssesment)
• Critical to supporting ALL functions
• Most overlooked risk
• Often the largest attack service

Endpoints are critical to supporting the organization's strategic objectives, the services that support those objectives, and the core technical infrastructure that enables those services. Endpoints also represent one of the largest attack surfaces of most organizations. Threat actors frequently leverage weaknesses and vulnerabilities on these endpoints to gain an initial foothold into the organization. They are then able to maintain persistence, escalate privileges, move laterally to higher value systems, and ultimately exfiltrate sensitive organizational data, disrupt services, or extort payments via ransomware.

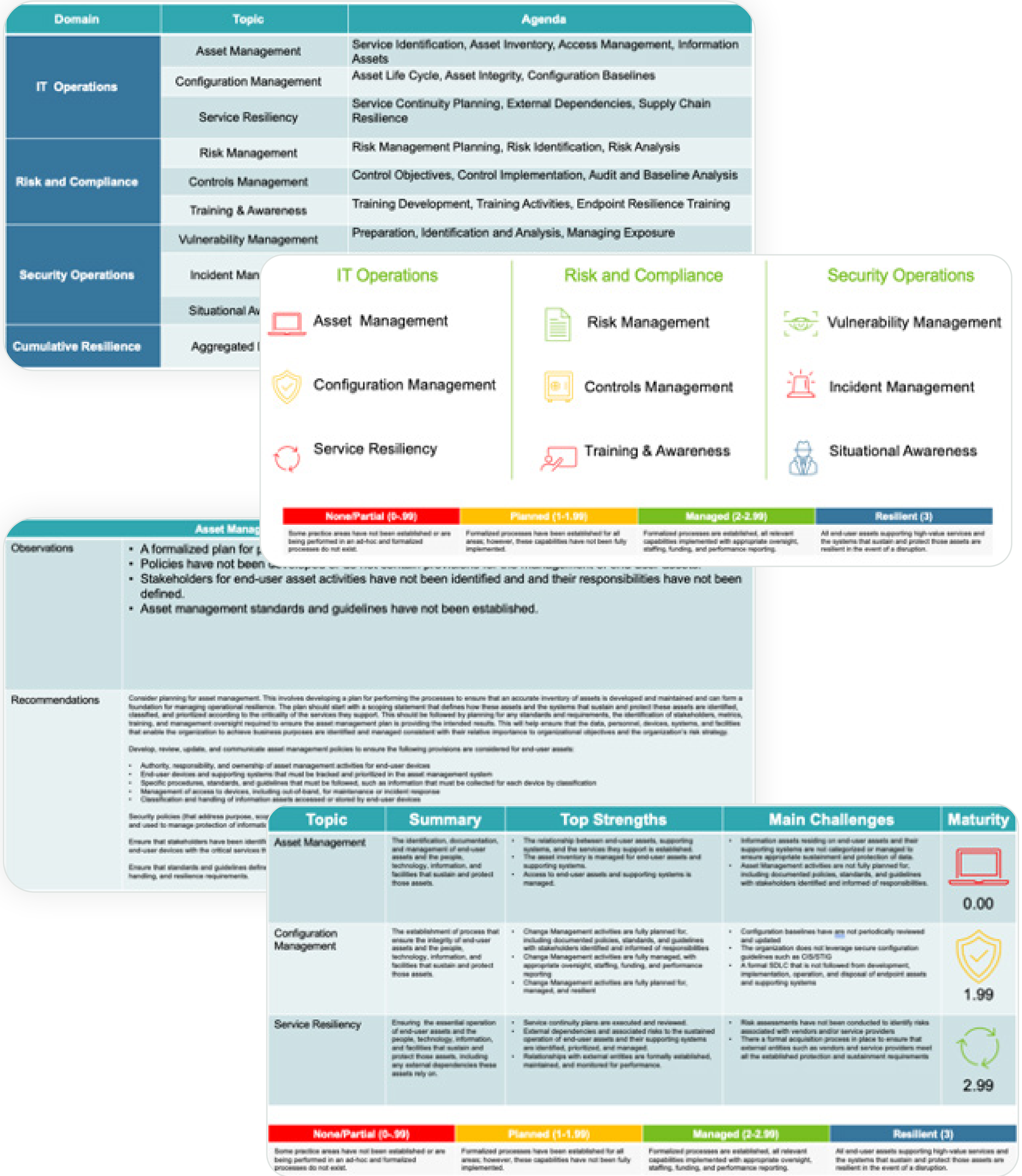
Most traditional assessments are mainly focused on the core infrastructure without taking a service-oriented approach, and only provide a cursory review of the security posture and capabilities necessary for endpoint resilience. The Endpoint Resilience Assessment takes this traditional approach a step further by providing an in-depth evaluation of cyber security and resilience from an end-user asset perspective. This identifies critical sustainment and protection gaps in addition to providing recommendations that help ensure organizations are prepared for and adapt to changing conditions and are able to withstand and recover rapidly from disruptions.

The assessment is delivered through four interactive workshops spanning IT Operations, Risk and Compliance, and Security Operations, and a leadership-focused Cumulative Resilience workshop covering domain oversight across all topic areas. These workshops will focus on the organization's maturity across asset management, configuration management, service resiliency, risk management, controls management, training and awareness, vulnerability management, incident management, and situational awareness.

- ✓ In-depth assessment of resilience from a fleet endpoint perspective across IT Operations, Risk and Compliance, and Security Operations
- ✓ Identify key control gaps and device management weaknesses prior to attacker exploitation
- ✓ Implement recommendations to improve resilience for endpoints for asset management, configuration management, service resiliency, risk management, controls management, training and awareness, vulnerability management, incident management, and situational awareness

Reach out to your account executive to discuss how **Absolute's Professional Services** can help.

SAMPLE ASSESSMENT



Domain	Topic	Agenda
IT Operations	Asset Management	Service Identification, Asset Inventory, Access Management, Information Assets
	Configuration Management	Asset Life Cycle, Asset Integrity, Configuration Baselines
	Service Resiliency	Service Continuity Planning, External Dependencies, Supply Chain Resilience
Risk and Compliance	Risk Management	Risk Management Planning, Risk Identification, Risk Analysis
	Controls Management	Control Objectives, Control Implementation, Audit and Baseline Analysis
	Training & Awareness	Training Development, Training Activities, Endpoint Resilience Training
Security Operations	Vulnerability Management	Preparation, Identification and Analysis, Managing Exposure
	Incident Man	
	Situational Aw	
Cumulative Resilience	Aggregated	

IT Operations	Risk and Compliance	Security Operations
Asset Management	Risk Management	Vulnerability Management
Configuration Management	Controls Management	Incident Management
Service Resiliency	Training & Awareness	Situational Awareness

None/Partial (0-.99)	Planned (1-1.99)	Managed (2-2.99)	Resilient (3)
Some practice areas have not been established or are being performed in an ad-hoc and formalized processes do not exist.	Formalized processes have been established for all areas; however, these capabilities have not been fully implemented.	Formalized processes are established, all relevant capabilities implemented with appropriate oversight, staffing, funding, and performance reporting.	All end-user assets supporting high-value services and the systems that sustain and protect those assets are resilient in the event of a disruption.

Asset Manag

Observations	• A formalized plan for p • Policies have not been • Stakeholders for end-user asset activities have not been identified and and their responsibilities have not been defined. • Asset management standards and guidelines have not been established.
Recommendations	Consider planning for asset management. This involves developing a plan for performing the processes to ensure that an accurate inventory of assets is developed and maintained and can form a foundation for managing operational resilience. The plan should start with a scoping statement that defines how these assets and the systems that sustain and protect these assets are identified, classified, and prioritized according to the criticality of the services they support. This should be followed by planning for any standards and requirements, the identification of stakeholders, metrics, training, and management oversight required to ensure the asset management plan is providing the intended results. This will help ensure that the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. Develop, review, update, and communicate asset management policies to ensure the following provisions are considered for end-user assets: • Authority, responsibility, and ownership of asset management activities for end-user devices • End-user devices and supporting systems that must be tracked and prioritized in the asset management system • Specific procedures, standards, and guidelines that must be followed, such as information that must be collected for each device by classification • Management of access to devices, including out-of-band, for maintenance or incident response • Classification and handling of information assets accessed or stored by end-user devices Security policies that address purpose, sco and used to manage protection of informatio Ensure that stakeholders have been identi end-user devices with the critical services th Ensure that standards and guidelines define handling, and resilience requirements.

Topic	Summary	Top Strengths	Main Challenges	Maturity
Asset Management	The identification, documentation, and management of end-user assets and the people, technology, information, and facilities that sustain and protect those assets.	• The relationship between end-user assets, supporting systems, and the services they support is established. • The asset inventory is managed for end-user assets and supporting systems. • Access to end-user assets and supporting systems is managed.	• Information assets residing on end-user assets and their supporting systems are not categorized or managed to ensure appropriate sustainment and protection of data. • Asset Management activities are not fully planned for, including documented policies, standards, and guidelines with stakeholders identified and informed of responsibilities.	0.00
Configuration Management	The establishment of process that ensure the integrity of end-user assets and the people, technology, information, and facilities that sustain and protect those assets.	• Change Management activities are fully planned for, including documented policies, standards, and guidelines with stakeholders identified and informed of responsibilities • Change Management activities are fully managed, with appropriate oversight, staffing, funding, and performance reporting • Change Management activities are fully planned for, managed, and resilient	• Configuration baselines have are not periodically reviewed and updated • The organization does not leverage secure configuration guidelines such as CIS/STIG • A formal SDLC that is not followed from development, implementation, operation, and disposal of endpoint assets and supporting systems	1.99
Service Resiliency	Ensuring the essential operation of end-user assets and the people, technology, information, and facilities that sustain and protect those assets, including any external dependencies these assets rely on.	• Service continuity plans are executed and reviewed. • External dependencies and associated risks to the sustained operation of end-user assets and their supporting systems are identified, prioritized, and managed. • Relationships with external entities are formally established, maintained, and monitored for performance.	• Risk assessments have not been conducted to identify risks associated with vendors and/or service providers • There a formal acquisition process in place to ensure that external entities such as vendors and service providers meet all the established protection and sustainment requirements	2.99

None/Partial (0-.99)	Planned (1-1.99)	Managed (2-2.99)	Resilient (3)
Some practice areas have not been established or are being performed in an ad-hoc and formalized processes do not exist.	Formalized processes have been established for all areas; however, these capabilities have not been fully implemented.	Formalized processes are established, all relevant capabilities implemented with appropriate oversight, staffing, funding, and performance reporting.	All end-user assets supporting high-value services and the systems that sustain and protect those assets are resilient in the event of a disruption.

ALIGNMENT

CISA Cyber Resilience Review (CRR) Domains • NIST CSF • NIST Cyber Resilience Controls

Absolute Endpoint Resilience Assessment

		CISA CRR DOMAIN	Asset Management	Controls Management	Configuration Management	Vulnerability Management	Incident Management	Service Continuity Mgmt.	Risk Management	External Dependencies Mgmt.	Training & Awareness	Situation Awareness
NIST SPECIAL PUBLICATION 800-160, VOL. 2	Access Control	AC	✓	✓			✓					
	Awareness & Training	AT									✓	✓
	Audit & Accountability	AU		✓	✓		✓					
	Assessment, Authorization & Monitoring	CA					✓		✓			✓
	Configuration Management	CM	✓	✓	✓							
	Contingency Planning	CP	✓	✓			✓	✓	✓	✓		
	Identification & Authentication	IA	✓	✓	✓							
	Incident Response	IR					✓					✓
	Maintenance	MA			✓							
	Physical & Environmental Protection	PE					✓	✓		✓		
	Planning	PL						✓		✓		
	Program Management	PM	✓						✓	✓		✓
	Risk Assessment	RA				✓	✓		✓			✓
	Systems & Services Acquisition	SA		✓	✓	✓	✓		✓			
	System & Communication Protection	SC	✓	✓	✓		✓		✓			
	System & Information Integrity	SI	✓	✓	✓	✓	✓	✓	✓			✓
	Supply Chain Risk Management	SR								✓		
NIST CYBERSECURITY FRAMEWORK CORE	Identify	ID	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Detect	DE			✓	✓	✓			✓		
	Protect	PR	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Respond	RS				✓	✓	✓				✓
	Recover	RC					✓	✓	✓			

ABSOLUTE®

Absolute Software makes security **work**. We empower mission-critical performance with advanced cyber resilience. Embedded in more than 600 million devices, our cyber resilience platform delivers endpoint-to-network access security coverage, ensures automated security compliance, and enables operational continuity. Nearly 21,000 global customers trust Absolute to protect enterprise assets, fortify security and business applications, and provide a frictionless, always-on user experience.

Learn More