Cybersecurity Baselines For Market Leading External Service Providers (ESP)

A Law, Regulation & Framework-Neutral Approach To Security, Compliance & Resilience

Why Now? Companies Need Trusted, Resilient Service Delivery

Leading External Service Providers (ESPs) utilize the Secure Controls Framework (SCF), since there is a need to efficiently and effectively demonstrate conformity with multiple Laws, Regulations & Frameworks (LRF) in an affordable manner. The SCF provides that functionality.

The SCF's ESP Baselines offer Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs) a way to prove operational maturity to clients, win larger contracts and scale with trust. Cybersecurity is a critical capability for any ESP, regardless of size or industry specialization. Issues facing ESPs include "never ending compliance" mandates that they are pulled into by client-specific obligations.

Creating an industry-wide cybersecurity baseline for ESPs is a complex goal that balances assurance needs, operational feasibility and industry diversity due to the heterogeneous ecosystem that exists.

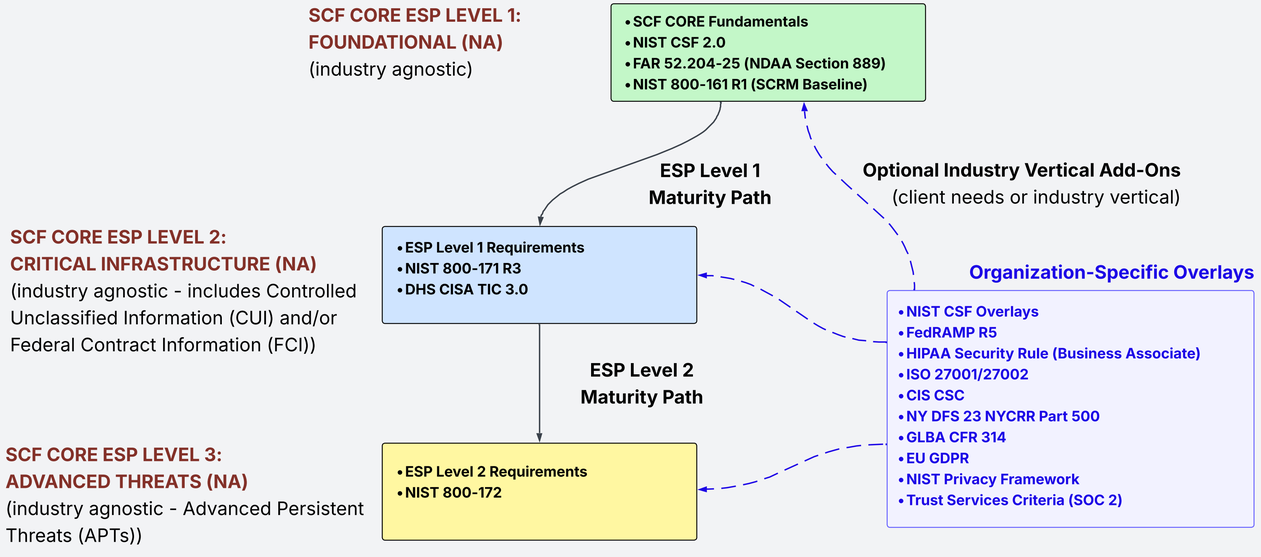
The core issues is not a "compliance vs security" debate. The ESP Baseline approach is that through implementing reasonable cybersecurity and data protection practices that are focused on security and resiliency, compliance will be a natural byproduct of those capabilities. A perfect example is with Cybersecurity Maturity Model Certification (CMMC) that utilizes NIST 800-171-based requirements - while it is a common compliance requirement, CMMC's focus on confidentiality and integrity provides limited alignment with what would be considered “industry recognized secure practices” focused on overall security and resilience.

The solution is a tiered approach to establish ESP-focused baselines that are based on common, reasonably-expected frameworks to address client needs for secure, compliant and resilient service providers. The Secure Controls Framework (SCF) Council created the following three baselines:

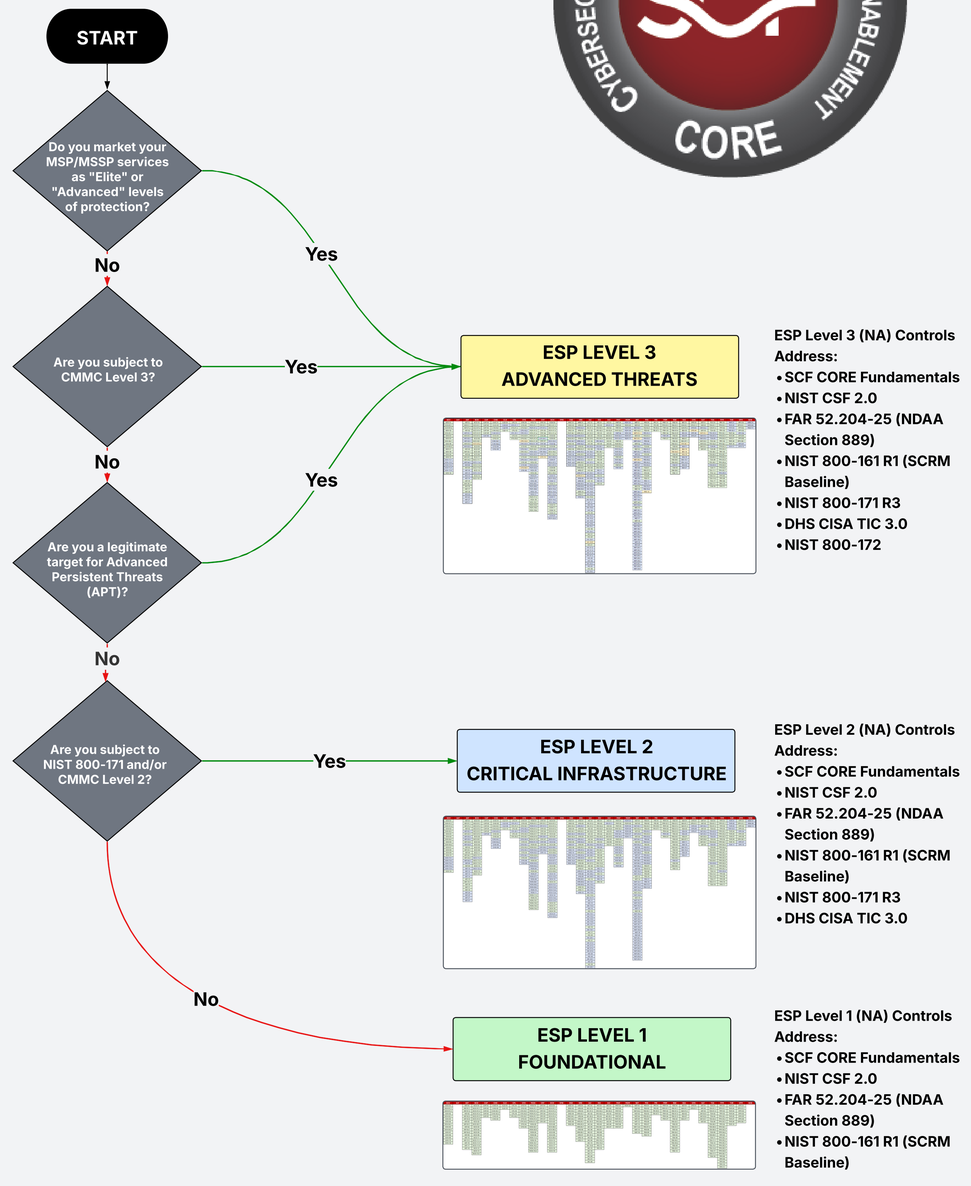
ESP Level 1: Foundational (NA) - Focused on building credibility for security, compliance and resilience capabilities.
ESP Level 2: Critical Infrastructure (NA) - Enhanced reliability for sensitive/regulated data environments.
ESP Level 3: Advanced Threats (NA) - Robust capabilities necessary to protect from more advanced threats.

The metaframework nature of the SCF enables ESPs to add-on industry vertical overlays to address the unique LRF that apply to its business model (e.g., HIPAA business associate, FedRAMP, NY DFS 23NYCRR Part 500, etc.).

ESP Baseline Scoping & Add-On Capabilities (North America)



ESP Baseline Determination Flow Chart



Copyright © 2025 by Secure Controls Framework Council, LLC (SCF Council). All rights reserved.

All text, images, logos, trademarks and information contained in this document are the intellectual property of SCF Council, unless otherwise indicated. Modification of any content, including text and images, requires the prior written permission of SCF Council. Requests may be sent to support@securecontrolsframework.com.

SCF CORE EXTERNAL SERVICE PROVIDER (ESP) LEVEL 1 - FOUNDATIONAL

The Secure Controls Framework (SCF) Cybersecurity Oversight, Resilience & Enablement (CORE) External Service Provider (ESP) Level 1 control set is a foundational set of cybersecurity and data protection controls that are designed for Managed Service Providers (MSP) and Managed Security Services Providers (MSSP), regardless of size or industry specialization. The SCF CORE ESP initiative is a tiered approach to establish ESP-focused baselines that are based on common, reasonably-expected frameworks to address client needs for secure, compliant and resilient service providers.

The SCF CORE ESP Level 1 addresses thirty (30) of the SCF's Cybersecurity & Data Protection Principles:

Cybersecurity & Data Protection Governance (GOV)
Execute a documented, risk-based program that supports business objectives while encompassing appropriate cybersecurity & data protection principles that addresses applicable statutory, regulatory and contractual obligations.

Asset Management (AST)
Manage all technology assets from purchase through disposition, both physical and virtual, to ensure secured use, regardless of the asset's location.

Business Continuity & Disaster Recovery (BCD)
Maintain a resilient capability to sustain business-critical functions while successfully responding to and recovering from incidents through well-documented and exercised processes.

Capacity & Performance Planning (CAP)
Govern the current and future capacities and performance of technology assets.

Change Management (CHG)
Manage change in a sustainable and ongoing manner that involves active participation from both technology and business stakeholders to ensure that only authorized changes occur.

Cloud Security (CLD)
Govern cloud instances as an extension of on-premise technologies with equal or greater security protections than the organization's own internal cybersecurity & data privacy controls.

Compliance (CPL)
Oversee the execution of cybersecurity & data privacy controls to ensure appropriate evidence required due care and due diligence exists to meet compliance with applicable statutory, regulatory and contractual obligations.

Configuration Management (CFG)
Enforce secure configurations according to vendor-recommended and industry-recognized secure practices that enforce the concepts of "least privilege" and "least functionality" for all systems, applications and services.

Continuous Monitoring (MON)
Maintain situational awareness of security-related events through the centralized collection and analysis of event logs from systems, applications and services.

Cryptographic Protections (CRY)
Utilize appropriate cryptographic solutions and industry-recognized key management practices to protect the confidentiality and integrity of sensitive/regulated data both at rest and in transit.

Data Classification & Handling (DCH)
Enforce a standardized data classification methodology to objectively determine the sensitivity and criticality of all data and technology assets so that proper handling and disposal requirements can be followed.

Endpoint Security (END)
Harden endpoint devices to protect against reasonable threats to those devices and the data those devices store, transmit and process.

Human Resources Security (HRS)
Execute sound hiring practices and ongoing personnel management to cultivate a cybersecurity & data privacy-minded workforce.

Identification & Authentication (IAC)
Enforce the concept of "least privilege" consistently across all systems, applications and services for individual, group and service accounts through a documented and standardized Identity and Access Management (IAM) capability.

Incident Response (IRO)
Maintain a viable incident response capability that trains personnel on how to recognize and report suspicious activities so that trained incident responders can take the appropriate steps to handle incidents, in accordance with a documented Incident Response Plan (IRP).

Information Assurance (IAO)
Execute an impartial assessment process to validate the existence and functionality of appropriate cybersecurity & data privacy controls, prior to a system, application or service being used in a production environment.

Maintenance (MNT)
Proactively maintain technology assets, according to current vendor recommendations for configurations and updates, including those supported or hosted by third-parties.

Mobile Device Management (MDM)
Implement measures to restrict mobile device connectivity with critical infrastructure and sensitive/regulated data that limit the attack surface and potential data exposure from mobile device usage.

Network Security (NET)
Architect and implement a secure and resilient defense-in-depth methodology that enforces the concept of "least functionality" through restricting network access to systems, applications and services.

Physical & Environmental Security (PES)
Protect physical environments through layers of physical security and environmental controls that work together to protect both physical and digital assets from theft and damage.

Data Privacy (PRI)
Align data privacy practices with industry-recognized data privacy principles to implement appropriate administrative, technical and physical controls to protect regulated personal data throughout the lifecycle of systems, applications and services.

Project & Resource Management (PRM)
Operationalize a viable strategy to achieve cybersecurity & data privacy objectives that establishes cybersecurity as a key stakeholder within project management practices to ensure the delivery of resilient and secure solutions.

Risk Management (RSK)
Proactively identify, assess, prioritize and remediate risk through alignment with industry-recognized risk management principles to ensure risk decisions adhere to the organization's risk threshold.

Secure Engineering & Architecture (SEA)
Utilize industry-recognized secure engineering and architecture principles to deliver secure and resilient systems, applications and services.

Security Operations (OPS)
Execute the delivery of cybersecurity & data privacy operations to provide quality services and secure systems, applications and services that meet the organization's business needs.

Security Awareness & Training (SAT)
Foster a cybersecurity & data privacy-minded workforce through ongoing user education about evolving threats, compliance obligations and secure workplace practices.

Technology Development & Acquisition (TDA)
Develop and/or acquire systems, applications and services according to a Secure Software Development Framework (SSDF) to reduce the potential impact of
undetected or unaddressed vulnerabilities and design flaws.

Third-Party Management (TPM)
Execute Supply Chain Risk Management (SCRM) practices so that only trustworthy third-parties are used for products and/or service delivery.

Threat Management (THR)
Proactively identify and assess technology-related threats, to both assets and business processes, to determine the applicable risk and necessary corrective action.

Vulnerability & Patch Management (VPM)
Leverage industry-recognized Attack Surface Management (ASM) practices to strengthen the security and resilience systems, applications and services against evolving and sophisticated attack vectors.

The SCF CORE ESP Level 1 includes mapping to requirements found in SCF CORE Fundamentals, NIST CSF 2.0, FAR 52.204-25 (NDAA Section 889) and NIST SP 800-161 R1 C-SCRM Baseline:

GOV	AAT	AST	BCD	CAP	CHG	CLD	CPL	CFG	MON	CRY	DCH	EMB	END	HRS	IAC	IRO	IAO	MNT	MDM	NET	PES	PRI	PRM	RSK	SEA	OPS	SAT	TDA	TPM	THR	VPM	WEB
GOV-01		AST-01	BCD-01	CAP-01	CHG-01	CLD-01	CPL-01	CFG-01	MON-01	CRY-01	DCH-01		END-01	HRS-01	IAC-01	IRO-01	IAO-01	MNT-01	MDM-02	NET-01	PES-01	PRI-01	PRM-01	RSK-01	SEA-01	OPS-01	SAT-01	TDA-01	TPM-01	THR-01	VPM-01	
GOV-01.1		AST-01.1	BCD-01.1	CAP-02	CHG-02	CLD-10	CPL-01.2	CFG-02	MON-01.1	CRY-01.1	DCH-01.1		END-03	HRS-02	IAC-01.2	IRO-02	IAO-02	MNT-02		NET-02	PES-02	PRI-05	PRM-01.1	RSK-01.1	SEA-01.1	OPS-01.1	SAT-02	TDA-01.1	TPM-01.1	THR-02	VPM-01.1	
GOV-01.2		AST-01.2	BCD-01.2	CAP-03	CHG-02.1		CPL-02	CFG-02.1	MON-01.3	CRY-03	DCH-01.2		END-03.2	HRS-03	IAC-01.3	IRO-02.4	IAO-02.4	MNT-03		NET-02.2	PES-02.1	PRI-05.5	PRM-02	RSK-01.3	SEA-01.2		SAT-03	TDA-01.2	TPM-02	THR-03	VPM-02	
GOV-02		AST-02	BCD-01.4	CAP-04	CHG-02.2		CPL-03	CFG-02.5	MON-01.4	CRY-04	DCH-01.3		END-04	HRS-03.1	IAC-02	IRO-02.5	IAO-03	MNT-03.1		NET-03	PES-03	PRI-07.1	PRM-03	RSK-01.4	SEA-02		SAT-03.5	TDA-02	TPM-03	THR-04	VPM-03	
GOV-02.1		AST-02.3	BCD-01.5	CAP-05	CHG-03		CPL-03.2	CFG-02.7	MON-01.7	CRY-05	DCH-01.4		END-04.1	HRS-04	IAC-02.2	IRO-03	IAO-03.1	MNT-05		NET-04	PES-03.3		PRM-04	RSK-01.5	SEA-07		SAT-03.6	TDA-04	TPM-03.1	THR-05	VPM-05	
GOV-03		AST-02.8	BCD-01.6		CHG-04			CFG-03	MON-01.8	CRY-07	DCH-02		END-04.4	HRS-05	IAC-03	IRO-04	IAO-03.2	MNT-05.1		NET-05	PES-05		PRM-07	RSK-02	SEA-07.1		SAT-03.7	TDA-04.2	TPM-03.2	THR-07	VPM-06	
GOV-04		AST-03	BCD-02					CFG-03.2	MON-01.12	CRY-09	DCH-03		END-06	HRS-05.1	IAC-03.5	IRO-04.2	IAO-05	MNT-05.2		NET-12	PES-06			RSK-02.1			SAT-04	TDA-06	TPM-03.3	THR-09	VPM-06.1	
GOV-04.1		AST-03.1	BCD-02.1					CFG-04	MON-02		DCH-06		END-08	HRS-05.3	IAC-04	IRO-05	IAO-06	MNT-06		NET-14	PES-07			RSK-03				TDA-06.1	TPM-04	THR-10		
GOV-05		AST-04	BCD-03					CFG-05	MON-02.1		DCH-06.2			HRS-05.7	IAC-05	IRO-06.1	IAO-07	MNT-07		NET-14.5	PES-07.5			RSK-03.1				TDA-06.2	TPM-04.1			
GOV-05.2		AST-04.1	BCD-04						MON-02.6		DCH-06.3			HRS-06	IAC-06	IRO-07				NET-15	PES-08			RSK-04				TDA-06.3	TPM-04.3			
GOV-07		AST-04.2	BCD-05						MON-03		DCH-08			HRS-06.1	IAC-07	IRO-08				NET-18	PES-09			RSK-04.1				TDA-09	TPM-04.4			
GOV-08		AST-09	BCD-06						MON-06		DCH-09			HRS-07	IAC-07.2	IRO-09					PES-10			RSK-05				TDA-09.1	TPM-05			
GOV-09		AST-15	BCD-11						MON-11.3		DCH-09.3			HRS-10	IAC-08	IRO-10								RSK-06				TDA-11	TPM-05.1			
GOV-15		AST-15.1	BCD-11.1						MON-16		DCH-13			HRS-11	IAC-09	IRO-10.2								RSK-06.1				TDA-11.1	TPM-05.2			
GOV-16		AST-16	BCD-11.5						MON-16.1		DCH-15				IAC-10	IRO-10.4								RSK-06.2				TDA-14	TPM-05.3			
		AST-17	BCD-11.6						MON-16.2		DCH-17				IAC-10.8	IRO-13								RSK-09				TDA-14.1	TPM-05.4			
		AST-18	BCD-12						MON-16.3		DCH-18				IAC-15	IRO-16								RSK-09.1				TDA-14.2	TPM-05.5			
			BCD-13						MON-16.4		DCH-19				IAC-16									RSK-12				TDA-17	TPM-05.6			
			BCD-13.1												IAC-17													TDA-17.1	TPM-05.7			
															IAC-20													TDA-18	TPM-06			
															IAC-21														TPM-08			
															IAC-28														TPM-09			
																													TPM-10			
																													TPM-11			

ESP Level 1
ESP Level 2
ESP Level 3

Copyright © 2025 by Secure Controls Framework Council, LLC (SCF Council). All rights reserved.

All text, images, logos, trademarks and information contained in this document are the intellectual property of SCF Council, unless otherwise indicated. Modification of any content, including text and images, requires the prior written permission of SCF Council. Requests may be sent to support@securecontrolsframework.com.

SCF CORE EXTERNAL SERVICE PROVIDER (ESP) LEVEL 2 - CRITICAL INFRASTRUCTURE

The Secure Controls Framework (SCF) Cybersecurity Oversight, Resilience & Enablement (CORE) External Service Provider (ESP) Level 2 control set is a cybersecurity and data protection controls that are designed for Managed Service Providers (MSP) and Managed Security Services Providers (MSSP) that support critical infrastructure (e.g., military, government, utilities, healthcare, transportation, etc.). The SCF CORE ESP initiative is a tiered approach to establish ESP-focused baselines that are based on common, reasonably-expected frameworks to address client needs for secure, compliant and resilient service providers.

The SCF CORE ESP Level 2 addresses thirty-one (31) of the SCF's Cybersecurity & Data Protection Principles:

Cybersecurity & Data Protection Governance (GOV)
Execute a documented, risk-based program that supports business objectives while encompassing appropriate cybersecurity & data protection principles that addresses applicable statutory, regulatory and contractual obligations.

Asset Management (AST)
Manage all technology assets from purchase through disposition, both physical and virtual, to ensure secured use, regardless of the asset's location.

Business Continuity & Disaster Recovery (BCD)
Maintain a resilient capability to sustain business-critical functions while successfully responding to and recovering from incidents through well-documented and exercised processes.

Capacity & Performance Planning (CAP)
Govern the current and future capacities and performance of technology assets.

Change Management (CHG)
Manage change in a sustainable and ongoing manner that involves active participation from both technology and business stakeholders to ensure that only authorized changes occur.

Cloud Security (CLD)
Govern cloud instances as an extension of on-premise technologies with equal or greater security protections than the organization's own internal cybersecurity & data privacy controls.

Compliance (CPL)
Oversee the execution of cybersecurity & data privacy controls to ensure appropriate evidence required due care and due diligence exists to meet compliance with applicable statutory, regulatory and contractual obligations.

Configuration Management (CFG)
Enforce secure configurations according to vendor-recommended and industry-recognized secure practices that enforce the concepts of "least privilege" and "least functionality" for all systems, applications and services.

Continuous Monitoring (MON)
Maintain situational awareness of security-related events through the centralized collection and analysis of event logs from systems, applications and services.

Cryptographic Protections (CRY)
Utilize appropriate cryptographic solutions and industry-recognized key management practices to protect the confidentiality and integrity of sensitive/regulated data both at rest and in transit.

Data Classification & Handling (DCH)
Enforce a standardized data classification methodology to objectively determine the sensitivity and criticality of all data and technology assets so that proper handling and disposal requirements can be followed.

Endpoint Security (END)
Harden endpoint devices to protect against reasonable threats to those devices and the data those devices store, transmit and process.

Human Resources Security (HRS)
Execute sound hiring practices and ongoing personnel management to cultivate a cybersecurity & data privacy-minded workforce.

Identification & Authentication (IAC)
Enforce the concept of "least privilege" consistently across all systems, applications and services for individual, group and service accounts through a documented and standardized Identity and Access Management (IAM) capability.

Incident Response (IRO)
Maintain a viable incident response capability that trains personnel on how to recognize and report suspicious activities so that trained incident responders can take the appropriate steps to handle incidents, in accordance with a documented Incident Response Plan (IRP).

Information Assurance (IAO)
Execute an impartial assessment process to validate the existence and functionality of appropriate cybersecurity & data privacy controls, prior to a system, application or service being used in a production environment.

Maintenance (MNT)
Proactively maintain technology assets, according to current vendor recommendations for configurations and updates, including those supported or hosted by third-parties.

Mobile Device Management (MDM)
Implement measures to restrict mobile device connectivity with critical infrastructure and sensitive/regulated data that limit the attack surface and potential data exposure from mobile device usage.

Network Security (NET)
Architect and implement a secure and resilient defense-in-depth methodology that enforces the concept of "least functionality" through restricting network access to systems, applications and services.

Physical & Environmental Security (PES)
Protect physical environments through layers of physical security and environmental controls that work together to protect both physical and digital assets from theft and damage.

Data Privacy (PRI)
Align data privacy practices with industry-recognized data privacy principles to implement appropriate administrative, technical and physical controls to protect regulated personal data throughout the lifecycle of systems, applications and services.

Project & Resource Management (PRM)
Operationalize a viable strategy to achieve cybersecurity & data privacy objectives that establishes cybersecurity as a key stakeholder within project management practices to ensure the delivery of resilient and secure solutions.

Risk Management (RSK)
Proactively identify, assess, prioritize and remediate risk through alignment with industry-recognized risk management principles to ensure risk decisions adhere to the organization's risk threshold.

Secure Engineering & Architecture (SEA)
Utilize industry-recognized secure engineering and architecture principles to deliver secure and resilient systems, applications and services.

Security Operations (OPS)
Execute the delivery of cybersecurity & data privacy operations to provide quality services and secure systems, applications and services that meet the organization's business needs.

Security Awareness & Training (SAT)
Foster a cybersecurity & data privacy-minded workforce through ongoing user education about evolving threats, compliance obligations and secure workplace practices.

Technology Development & Acquisition (TDA)
Develop and/or acquire systems, applications and services according to a Secure Software Development Framework (SSDF) to reduce the potential impact of
undetected or unaddressed vulnerabilities and design flaws.

Third-Party Management (TPM)
Execute Supply Chain Risk Management (SCRM) practices so that only trustworthy third-parties are used for products and/or service delivery.

Threat Management (THR)
Proactively identify and assess technology-related threats, to both assets and business processes, to determine the applicable risk and necessary corrective action.

Vulnerability & Patch Management (VPM)
Leverage industry-recognized Attack Surface Management (ASM) practices to strengthen the security and resilience systems, applications and services against evolving and sophisticated attack vectors.

Web Security (WEB)
Ensure the security and resilience of Internet-facing technologies through secure configuration management practices and monitoring for anomalous activity.

The SCF CORE ESP Level 2 includes mapping to requirements found in SCF CORE Fundamentals, NIST CSF 2.0, FAR 52.204-25 (NDAA Section 889), NIST SP 800-161 R1 C-SCRM Baseline, NIST SP 800-171 R3 and DHS CISA TIC 3.0:

GOV	AAT	AST	BCD	CAP	CHG	CLD	CPL	CFG	MON	CRY	DCH	EMB	END	HRS	IAC	IRO	IAO	MNT	MDM	NET	PES	PRI	PRM	RSK	SEA	OPS	SAT	TDA	TPM	THR	VPM	WEB
GOV-01		AST-01	BCD-01	CAP-01	CHG-01	CLD-01	CPL-01	CFG-01	MON-01	CRY-01	DCH-01		END-01	HRS-01	IAC-01	IRO-01	IAO-01	MNT-01	MDM-01	NET-01	PES-01	PRI-01	PRM-01	RSK-01	SEA-01	OPS-01	SAT-01	TDA-01	TPM-01	THR-01	VPM-01	WEB-01
GOV-01.1		AST-01.1	BCD-01.1	CAP-02	CHG-02	CLD-02	CPL-01.1	CFG-02	MON-01.1	CRY-01.1	DCH-01.1		END-03	HRS-02	IAC-01.2	IRO-02	IAO-01.1	MNT-02	MDM-02	NET-02	PES-02	PRI-05	PRM-01.1	RSK-01.1	SEA-01.1	OPS-01.1	SAT-02	TDA-01.1	TPM-01.1	THR-02	VPM-01.1	WEB-06
GOV-01.2		AST-01.2	BCD-01.2	CAP-03	CHG-02.1	CLD-06	CPL-01.2	CFG-02.1	MON-01.2	CRY-01.5	DCH-01.2		END-03.2	HRS-02.1	IAC-01.3	IRO-02.4	IAO-02	MNT-03	MDM-03	NET-02.1	PES-02.1	PRI-05.5	PRM-02	RSK-01.3	SEA-01.2	OPS-03	SAT-02.2	TDA-01.2	TPM-02	THR-03	VPM-02	WEB-14
GOV-02		AST-02	BCD-01.4	CAP-04	CHG-02.2	CLD-10	CPL-02	CFG-02.2	MON-01.3	CRY-03	DCH-01.3		END-04	HRS-03	IAC-02	IRO-02.5	IAO-02.4	MNT-03.1	MDM-04	NET-02.2	PES-03	PRI-07.1	PRM-03	RSK-01.4	SEA-02	OPS-06	SAT-03	TDA-02	TPM-03	THR-03.1	VPM-03	
GOV-02.1		AST-02.1	BCD-01.5	CAP-05	CHG-02.3		CPL-02.1	CFG-02.3	MON-01.4	CRY-04	DCH-01.4		END-04.1	HRS-03.1	IAC-02.2	IRO-03	IAO-03	MNT-04	MDM-06	NET-03	PES-03.1		PRM-04	RSK-01.5	SEA-03	OPS-07	SAT-03.2	TDA-02.3	TPM-03.1	THR-04	VPM-04	
GOV-03		AST-02.3	BCD-01.6	CAP-06	CHG-03		CPL-03	CFG-02.5	MON-01.7	CRY-05	DCH-02		END-04.3	HRS-03.2	IAC-03	IRO-04	IAO-03.1	MNT-04.1	MDM-07	NET-03.8	PES-03.3		PRM-05	RSK-02	SEA-05		SAT-03.3	TDA-02.4	TPM-03.2	THR-05	VPM-05	
GOV-04		AST-02.4	BCD-02		CHG-04		CPL-03.2	CFG-02.7	MON-01.8	CRY-05.1	DCH-03		END-04.4	HRS-04	IAC-03.5	IRO-04.2	IAO-03.2	MNT-04.3	MDM-11	NET-04	PES-03.4		PRM-07	RSK-02.1	SEA-07		SAT-03.5	TDA-03	TPM-03.3	THR-07	VPM-06	
GOV-04.1		AST-02.5	BCD-02.1		CHG-04.1			CFG-02.9	MON-01.12	CRY-07	DCH-03.1		END-04.7	HRS-04.1	IAC-04	IRO-04.3	IAO-05	MNT-05		NET-04.1	PES-04			RSK-03	SEA-07.1		SAT-03.6	TDA-04	TPM-04	THR-09	VPM-06.1	
GOV-05		AST-02.8	BCD-03		CHG-04.4			CFG-03	MON-01.15	CRY-08	DCH-04		END-06	HRS-04.2	IAC-05	IRO-05	IAO-06	MNT-05.1		NET-05	PES-04.1			RSK-03.1	SEA-11		SAT-03.7	TDA-04.2	TPM-04.1	THR-10	VPM-07	
GOV-05.2		AST-02.9	BCD-04		CHG-05			CFG-03.1	MON-02	CRY-09	DCH-06		END-07	HRS-05	IAC-05.2	IRO-05.1	IAO-07	MNT-05.2		NET-05.2	PES-05			RSK-04	SEA-18		SAT-04	TDA-05	TPM-04.3	THR-11	VPM-10	
GOV-07		AST-03	BCD-05		CHG-06			CFG-03.2	MON-02.1	CRY-09.3	DCH-06.1		END-08	HRS-05.1	IAC-06	IRO-06		MNT-05.3		NET-06	PES-05.1			RSK-04.1	SEA-18.1			TDA-06	TPM-04.4			
GOV-08		AST-03.1	BCD-06					CFG-03.3	MON-02.2	CRY-09.4	DCH-06.2		END-10	HRS-05.2	IAC-06.1	IRO-06.1		MNT-05.4		NET-06.3	PES-05.2			RSK-05	SEA-18.2			TDA-06.1	TPM-05			
GOV-09		AST-04	BCD-11					CFG-04	MON-02.3	CRY-12	DCH-06.3		END-14	HRS-05.3	IAC-06.2	IRO-07		MNT-05.5		NET-06.6	PES-06			RSK-06	SEA-20			TDA-06.2	TPM-05.1			
GOV-15		AST-04.1	BCD-11.1					CFG-04.1	MON-02.6		DCH-06.4		END-14.3	HRS-05.4	IAC-06.3	IRO-08		MNT-06		NET-07	PES-06.1			RSK-06.1	SEA-21			TDA-06.3	TPM-05.2			
GOV-15.1		AST-04.2	BCD-11.4					CFG-05	MON-02.7		DCH-07		END-14.4	HRS-05.5	IAC-07	IRO-09		MNT-06.1		NET-08	PES-06.2			RSK-06.2				TDA-09	TPM-05.3			
GOV-15.2		AST-04.3	BCD-11.5					CFG-06	MON-03		DCH-07.1		END-14.5	HRS-05.7	IAC-07.1	IRO-10		MNT-06.2		NET-08.1	PES-06.3			RSK-07				TDA-09.1	TPM-05.4			
GOV-15.3		AST-05	BCD-11.6					CFG-08	MON-03.2		DCH-07.2		END-14.6	HRS-06	IAC-07.2	IRO-10.2		MNT-07		NET-08.3	PES-06.6			RSK-09				TDA-09.5	TPM-05.5			
GOV-15.4		AST-09	BCD-12						MON-03.3		DCH-08			HRS-06.1	IAC-08	IRO-10.4		MNT-09		NET-08.4	PES-07			RSK-09.1				TDA-11	TPM-05.6			
GOV-15.5		AST-10	BCD-12.3						MON-05		DCH-09			HRS-07	IAC-09	IRO-11				NET-09	PES-07.5			RSK-12				TDA-11.1	TPM-05.7			
GOV-16		AST-12	BCD-13						MON-06		DCH-09.3			HRS-07.1	IAC-09.1	IRO-12				NET-10.2	PES-08							TDA-14	TPM-05.8			
		AST-13	BCD-13.1						MON-07		DCH-10			HRS-08	IAC-09.2	IRO-13				NET-10.4	PES-09							TDA-14.1	TPM-06			
		AST-14							MON-07.1		DCH-10.2			HRS-09	IAC-09.5	IRO-14				NET-12	PES-10							TDA-14.2	TPM-08			
		AST-15							MON-08		DCH-12			HRS-09.1	IAC-10	IRO-15				NET-14	PES-11							TDA-17	TPM-09			
		AST-15.1							MON-08.1		DCH-13			HRS-09.2	IAC-10.1	IRO-16				NET-14.1	PES-12							TDA-17.1	TPM-10			
		AST-16							MON-08.2		DCH-13.1			HRS-09.4	IAC-10.3					NET-14.2	PES-12.1							TDA-18	TPM-11			
		AST-17							MON-08.3		DCH-13.2			HRS-10	IAC-10.4					NET-14.3	PES-12.2											
		AST-18							MON-10		DCH-13.3			HRS-11	IAC-10.5					NET-14.4												
		AST-24							MON-11		DCH-13.4			HRS-12	IAC-10.6					NET-14.5												
		AST-25							MON-11.3		DCH-14				IAC-10.8					NET-14.6												
		AST-27							MON-16		DCH-14.2				IAC-10.11					NET-15												
		AST-31							MON-16.1		DCH-14.3				IAC-11					NET-15.1												
									MON-16.2		DCH-15				IAC-13					NET-15.2												
									MON-16.3		DCH-17				IAC-13.3					NET-15.3												
									MON-16.4		DCH-18				IAC-14					NET-17												
											DCH-19				IAC-15					NET-18												
											DCH-21				IAC-15.1					NET-18.2												
											DCH-22.2				IAC-15.3					NET-18.4												
															IAC-15.5					NET-18.5												
															IAC-15.6					NET-18.6												
															IAC-15.7					NET-18.7												
															IAC-16					NET-18.8												
															IAC-16.1					NET-18.9												
															IAC-17					NET-19												
															IAC-20					NET-20												
															IAC-20.1					NET-20.1												
															IAC-21					NET-20.2												
															IAC-21.2					NET-20.3												
															IAC-21.3					NET-20.4												
															IAC-21.4					NET-20.5												
															IAC-21.5					NET-20.6												
															IAC-22					NET-20.7												
															IAC-24					NET-20.8												
															IAC-24.1					NET-20.9												
															IAC-25																	
															IAC-28																	
															IAC-28.1																	

ESP Level 1
ESP Level 2
ESP Level 3

Copyright © 2025 by Secure Controls Framework Council, LLC (SCF Council). All rights reserved.

All text, images, logos, trademarks and information contained in this document are the intellectual property of SCF Council, unless otherwise indicated. Modification of any content, including text and images, requires the prior written permission of SCF Council. Requests may be sent to support@securecontrolsframework.com.

SCF CORE EXTERNAL SERVICE PROVIDER (ESP) LEVEL 3 - ADVANCED THREATS

The Secure Controls Framework (SCF) Cybersecurity Oversight, Resilience & Enablement (CORE) External Service Provider (ESP) Level 3 control set is a comprehensive set of cybersecurity and data protection controls that are designed for Managed Service Providers (MSP) and Managed Security Services Providers (MSSP) that are reasonable targets for advanced threats. The SCF CORE ESP initiative is a tiered approach to establish ESP-focused baselines that are based on common, reasonably-expected frameworks to address client needs for secure, compliant and resilient service providers.

The SCF CORE ESP Level 3 addresses thirty-one (31) of the SCF's Cybersecurity & Data Protection Principles:

Cybersecurity & Data Protection Governance (GOV)
Execute a documented, risk-based program that supports business objectives while encompassing appropriate cybersecurity & data protection principles that addresses applicable statutory, regulatory and contractual obligations.

Asset Management (AST)
Manage all technology assets from purchase through disposition, both physical and virtual, to ensure secured use, regardless of the asset's location.

Business Continuity & Disaster Recovery (BCD)
Maintain a resilient capability to sustain business-critical functions while successfully responding to and recovering from incidents through well-documented and exercised processes.

Capacity & Performance Planning (CAP)
Govern the current and future capacities and performance of technology assets.

Change Management (CHG)
Manage change in a sustainable and ongoing manner that involves active participation from both technology and business stakeholders to ensure that only authorized changes occur.

Cloud Security (CLD)
Govern cloud instances as an extension of on-premise technologies with equal or greater security protections than the organization's own internal cybersecurity & data privacy controls.

Compliance (CPL)
Oversee the execution of cybersecurity & data privacy controls to ensure appropriate evidence required due care and due diligence exists to meet compliance with applicable statutory, regulatory and contractual obligations.

Configuration Management (CFG)
Enforce secure configurations according to vendor-recommended and industry-recognized secure practices that enforce the concepts of "least privilege" and "least functionality" for all systems, applications and services.

Continuous Monitoring (MON)
Maintain situational awareness of security-related events through the centralized collection and analysis of event logs from systems, applications and services.

Cryptographic Protections (CRY)
Utilize appropriate cryptographic solutions and industry-recognized key management practices to protect the confidentiality and integrity of sensitive/regulated data both at rest and in transit.

Data Classification & Handling (DCH)
Enforce a standardized data classification methodology to objectively determine the sensitivity and criticality of all data and technology assets so that proper handling and disposal requirements can be followed.

Endpoint Security (END)
Harden endpoint devices to protect against reasonable threats to those devices and the data those devices store, transmit and process.

Human Resources Security (HRS)
Execute sound hiring practices and ongoing personnel management to cultivate a cybersecurity & data privacy-minded workforce.

Identification & Authentication (IAC)
Enforce the concept of "least privilege" consistently across all systems, applications and services for individual, group and service accounts through a documented and standardized Identity and Access Management (IAM) capability.

Incident Response (IRO)
Maintain a viable incident response capability that trains personnel on how to recognize and report suspicious activities so that trained incident responders can take the appropriate steps to handle incidents, in accordance with a documented Incident Response Plan (IRP).

Information Assurance (IAO)
Execute an impartial assessment process to validate the existence and functionality of appropriate cybersecurity & data privacy controls, prior to a system, application or service being used in a production environment.

Maintenance (MNT)
Proactively maintain technology assets, according to current vendor recommendations for configurations and updates, including those supported or hosted by third-parties.

Mobile Device Management (MDM)
Implement measures to restrict mobile device connectivity with critical infrastructure and sensitive/regulated data that limit the attack surface and potential data exposure from mobile device usage.

Network Security (NET)
Architect and implement a secure and resilient defense-in-depth methodology that enforces the concept of "least functionality" through restricting network access to systems, applications and services.

Physical & Environmental Security (PES)
Protect physical environments through layers of physical security and environmental controls that work together to protect both physical and digital assets from theft and damage.

Data Privacy (PRI)
Align data privacy practices with industry-recognized data privacy principles to implement appropriate administrative, technical and physical controls to protect regulated personal data throughout the lifecycle of systems, applications and services.

Project & Resource Management (PRM)
Operationalize a viable strategy to achieve cybersecurity & data privacy objectives that establishes cybersecurity as a key stakeholder within project management practices to ensure the delivery of resilient and secure solutions.

Risk Management (RSK)
Proactively identify, assess, prioritize and remediate risk through alignment with industry-recognized risk management principles to ensure risk decisions adhere to the organization's risk threshold.

Secure Engineering & Architecture (SEA)
Utilize industry-recognized secure engineering and architecture principles to deliver secure and resilient systems, applications and services.

Security Operations (OPS)
Execute the delivery of cybersecurity & data privacy operations to provide quality services and secure systems, applications and services that meet the organization's business needs.

Security Awareness & Training (SAT)
Foster a cybersecurity & data privacy-minded workforce through ongoing user education about evolving threats, compliance obligations and secure workplace practices.

Technology Development & Acquisition (TDA)
Develop and/or acquire systems, applications and services according to a Secure Software Development Framework (SSDF) to reduce the potential impact of
undetected or unaddressed vulnerabilities and design flaws.

Third-Party Management (TPM)
Execute Supply Chain Risk Management (SCRM) practices so that only trustworthy third-parties are used for products and/or service delivery.

Threat Management (THR)
Proactively identify and assess technology-related threats, to both assets and business processes, to determine the applicable risk and necessary corrective action.

Vulnerability & Patch Management (VPM)
Leverage industry-recognized Attack Surface Management (ASM) practices to strengthen the security and resilience systems, applications and services against evolving and sophisticated attack vectors.

Web Security (WEB)
Ensure the security and resilience of Internet-facing technologies through secure configuration management practices and monitoring for anomalous activity.

The SCF CORE ESP Level 3 includes mapping to requirements found in SCF CORE Fundamentals, NIST CSF 2.0, FAR 52.204-25 (NDAA Section 889), NIST SP 800-161 R1 C-SCRM Baseline, NIST SP 800-171 R3, DHS CISA TIC 3.0 and NIST SP 800-172:

GOV	AAT	AST	BCD	CAP	CHG	CLD	CPL	CFG	MON	CRY	DCH	EMB	END	HRS	IAC	IRO	IAO	MNT	MDM	NET	PES	PRI	PRM	RSK	SEA	OPS	SAT	TDA	TPM	THR	VPM	WEB
GOV-01		AST-01	BCD-01	CAP-01	CHG-01	CLD-01	CPL-01	CFG-01	MON-01	CRY-01	DCH-01		END-01	HRS-01	IAC-01	IRO-01	IAO-01	MNT-01	MDM-01	NET-01	PES-01	PRI-01	PRM-01	RSK-01	SEA-01	OPS-01	SAT-01	TDA-01	TPM-01	THR-01	VPM-01	WEB-01
GOV-01.1		AST-01.1	BCD-01.1	CAP-02	CHG-02	CLD-02	CPL-01.1	CFG-02	MON-01.1	CRY-01.1	DCH-01.1		END-03	HRS-02	IAC-01.2	IRO-02	IAO-01.1	MNT-02	MDM-02	NET-02	PES-02	PRI-05	PRM-01.1	RSK-01.1	SEA-01.1	OPS-01.1	SAT-02	TDA-01.1	TPM-01.1	THR-02	VPM-01.1	WEB-06
GOV-01.2		AST-01.2	BCD-01.2	CAP-03	CHG-02.1	CLD-06	CPL-01.2	CFG-02.1	MON-01.2	CRY-01.5	DCH-01.2		END-03.2	HRS-02.1	IAC-01.3	IRO-02.4	IAO-02	MNT-03	MDM-03	NET-02.1	PES-02.1	PRI-05.5	PRM-02	RSK-01.3	SEA-01.2	OPS-03	SAT-02.2	TDA-01.2	TPM-02	THR-03	VPM-02	WEB-14
GOV-02		AST-02	BCD-01.4	CAP-04	CHG-02.2	CLD-10	CPL-02	CFG-02.2	MON-01.3	CRY-03	DCH-01.3		END-04	HRS-03	IAC-02	IRO-02.5	IAO-02.4	MNT-03.1	MDM-04	NET-02.2	PES-03	PRI-07.1	PRM-03	RSK-01.4	SEA-02	OPS-04	SAT-03	TDA-02	TPM-03	THR-03.1	VPM-03	
GOV-02.1		AST-02.1	BCD-01.5	CAP-05	CHG-02.3		CPL-02.1	CFG-02.3	MON-01.4	CRY-04	DCH-01.4		END-04.1	HRS-03.1	IAC-02.2	IRO-03	IAO-03	MNT-04	MDM-06	NET-02.3	PES-03.1		PRM-04	RSK-01.5	SEA-03	OPS-06	SAT-03.1	TDA-02.3	TPM-03.1	THR-04	VPM-04	
GOV-03		AST-02.3	BCD-01.6	CAP-06	CHG-03		CPL-03	CFG-02.5	MON-01.7	CRY-05	DCH-02		END-04.3	HRS-03.2	IAC-03	IRO-04	IAO-03.1	MNT-04.1	MDM-07	NET-03	PES-03.3		PRM-05	RSK-02	SEA-05	OPS-07	SAT-03.2	TDA-02.4	TPM-03.2	THR-05	VPM-05	
GOV-04		AST-02.4	BCD-02		CHG-04		CPL-03.2	CFG-02.7	MON-01.8	CRY-05.1	DCH-03		END-04.4	HRS-04	IAC-03.5	IRO-04.2	IAO-03.2	MNT-04.3	MDM-11	NET-03.7	PES-03.4		PRM-07	RSK-02.1	SEA-07		SAT-03.3	TDA-03	TPM-03.3	THR-07	VPM-06	
GOV-04.1		AST-02.5	BCD-02.1		CHG-04.1			CFG-02.8	MON-01.12	CRY-07	DCH-03.1		END-04.7	HRS-04.1	IAC-04	IRO-04.3	IAO-05	MNT-05		NET-03.8	PES-04			RSK-03	SEA-07.1		SAT-03.5	TDA-04	TPM-04	THR-09	VPM-06.1	
GOV-05		AST-02.8	BCD-02.4		CHG-04.4			CFG-02.9	MON-01.15	CRY-08	DCH-04		END-06	HRS-04.2	IAC-05	IRO-05	IAO-06	MNT-05.1		NET-04	PES-04.1			RSK-03.1	SEA-08.1		SAT-03.6	TDA-04.2	TPM-04.1	THR-10	VPM-07	
GOV-05.2		AST-02.9	BCD-03		CHG-05			CFG-03	MON-02	CRY-09	DCH-06		END-07	HRS-05	IAC-05.2	IRO-05.1	IAO-07	MNT-05.2		NET-04.1	PES-05			RSK-04	SEA-11		SAT-03.7	TDA-05	TPM-04.3	THR-11	VPM-10	
GOV-07		AST-03	BCD-04		CHG-06			CFG-03.1	MON-02.1	CRY-09.3	DCH-06.1		END-08	HRS-05.1	IAC-06	IRO-06		MNT-05.3		NET-05	PES-05.1			RSK-04.1	SEA-13		SAT-04	TDA-06	TPM-04.4			
GOV-08		AST-03.1	BCD-05					CFG-03.2	MON-02.2	CRY-09.4	DCH-06.2		END-10	HRS-05.2	IAC-06.1	IRO-06.1		MNT-05.4		NET-05.2	PES-05.2			RSK-04.2	SEA-14			TDA-06.1	TPM-05			
GOV-09		AST-04	BCD-06					CFG-03.3	MON-02.3	CRY-12	DCH-06.3		END-14	HRS-05.3	IAC-06.2	IRO-07		MNT-05.5		NET-06	PES-06			RSK-05	SEA-15			TDA-06.2	TPM-05.1			
GOV-15		AST-04.1	BCD-11					CFG-04	MON-02.6	CRY-13	DCH-06.4		END-14.3	HRS-05.4	IAC-06.3	IRO-08		MNT-06		NET-06.3	PES-06.1			RSK-06	SEA-18			TDA-06.3	TPM-05.2			
GOV-15.1		AST-04.2	BCD-11.1					CFG-04.1	MON-02.7		DCH-07		END-14.4	HRS-05.5	IAC-07	IRO-09		MNT-06.1		NET-06.4	PES-06.2			RSK-06.1	SEA-18.1			TDA-09	TPM-05.3			
GOV-15.2		AST-04.3	BCD-11.4					CFG-05	MON-03		DCH-07.1		END-14.5	HRS-05.7	IAC-07.1	IRO-10		MNT-06.2		NET-06.6	PES-06.3			RSK-06.2	SEA-18.2			TDA-09.1	TPM-05.4			
GOV-15.3		AST-05	BCD-11.5					CFG-06	MON-03.2		DCH-07.2		END-14.6	HRS-06	IAC-07.2	IRO-10.2		MNT-07		NET-07	PES-06.6			RSK-07	SEA-20			TDA-09.5	TPM-05.5			
GOV-15.4		AST-09	BCD-11.6					CFG-06.1	MON-03.3		DCH-08			HRS-06.1	IAC-08	IRO-10.4		MNT-09		NET-08	PES-07			RSK-09	SEA-21			TDA-11	TPM-05.6			
GOV-15.5		AST-10	BCD-12					CFG-08	MON-05		DCH-09			HRS-07	IAC-09	IRO-11				NET-08.1	PES-07.5			RSK-09.1				TDA-11.1	TPM-05.7			
GOV-16		AST-12	BCD-12.3						MON-06		DCH-09.3			HRS-07.1	IAC-09.1	IRO-12				NET-08.3	PES-08			RSK-12				TDA-14	TPM-05.8			
		AST-13	BCD-13						MON-07		DCH-10			HRS-07.3	IAC-09.2	IRO-13				NET-08.4	PES-09							TDA-14.1	TPM-06			
		AST-14	BCD-13.1						MON-07.1		DCH-10.2			HRS-08	IAC-09.5	IRO-14				NET-09	PES-10							TDA-14.2	TPM-08			
		AST-15							MON-08		DCH-12			HRS-09	IAC-10	IRO-15				NET-10.2	PES-11							TDA-17	TPM-09			
		AST-15.1							MON-08.1		DCH-13			HRS-09.1	IAC-10.1	IRO-16				NET-10.4	PES-12							TDA-17.1	TPM-10			
		AST-16							MON-08.2		DCH-13.1			HRS-09.2	IAC-10.3					NET-12	PES-12.1							TDA-18	TPM-11			
		AST-17							MON-08.3		DCH-13.2			HRS-09.4	IAC-10.4					NET-14	PES-12.2											
		AST-18							MON-10		DCH-13.3			HRS-10	IAC-10.5					NET-14.1	PES-18											
		AST-24							MON-11		DCH-13.4			HRS-11	IAC-10.6					NET-14.2												
		AST-25							MON-11.3		DCH-14			HRS-12	IAC-10.8					NET-14.3												
		AST-27							MON-16		DCH-14.2				IAC-10.11					NET-14.4												
		AST-31							MON-16.1		DCH-14.3				IAC-11					NET-14.5												
									MON-16.2		DCH-15				IAC-13					NET-14.6												
									MON-16.3		DCH-17				IAC-13.3					NET-15												
									MON-16.4		DCH-18				IAC-14					NET-15.1												
											DCH-19				IAC-15					NET-15.2												
											DCH-21				IAC-15.1					NET-15.3												
											DCH-22.2				IAC-15.3					NET-17												
															IAC-15.5					NET-18												
															IAC-15.6					NET-18.2												
															IAC-15.7					NET-18.4												
															IAC-16					NET-18.5												
															IAC-16.1					NET-18.6												
															IAC-17					NET-18.7												
															IAC-20					NET-18.8												
															IAC-20.1					NET-18.9												
															IAC-20.5					NET-19												
															IAC-21					NET-20												
															IAC-21.2					NET-20.1												
															IAC-21.3					NET-20.2												
															IAC-21.4					NET-20.3												
															IAC-21.5					NET-20.4												
															IAC-22					NET-20.5												
															IAC-24					NET-20.6												
															IAC-24.1					NET-20.7												
															IAC-25					NET-20.8												
															IAC-28					NET-20.9												
															IAC-28.1																	

ESP Level 1
ESP Level 2
ESP Level 3

Copyright © 2025 by Secure Controls Framework Council, LLC (SCF Council). All rights reserved.

All text, images, logos, trademarks and information contained in this document are the intellectual property of SCF Council, unless otherwise indicated. Modification of any content, including text and images, requires the prior written permission of SCF Council. Requests may be sent to support@securecontrolsframework.com.