Security, Compliance & Resilience (SCR) Principles

The Secure Controls Framework (SCF) established 34 common-sense principles to guide the development and oversight of a modern cybersecurity & data privacy program. The focus is for organizations to be secure, compliant and resilient. The SCF's comprehensive listing of over 1,500 cybersecurity & data protection controls is categorized into 34 domains and are mapped to over 200 authoritative sources (e.g., laws, regulations and frameworks). Those applicable SCF controls can operationalize the SCR principles to help an organization ensure that secure, compliant and resilient practices are implemented by design and by default. Those principles are listed below:

1. Security, Compliance & Resilience Governance (GOV)
Govern the organization's Security, Compliance & Resilience Program (SCRP) through accountable oversight, evidence-based decision-making and defensible evidence that the organization is secure, compliant and resilient.

2. Artificial Intelligence and Autonomous Technology (AAT)
Govern Artificial Intelligence & Autonomous Technologies (AAT) through trustworthy, secure and resilient lifecycle practices that manage intended and unintended outcomes.

3. Asset Management (AST)
Manage Technology Assets, Applications and Services (TAAS) throughout their lifecycle to maintain visibility, accountability, authorization and protection.

4. Business Continuity & Disaster Recovery (BCD)
Maintain resilient capabilities to sustain business-critical functions and recover from disruptions through documented, tested and maintained continuity and recovery processes.

5. Capacity & Performance Planning (CAP)
Govern current and future capacity and performance requirements for Technology Assets, Applications, Services and Data (TAASD) to sustain reliable operations.

6. Change Management (CHG)
Manage changes to Technology Assets, Applications, Services and Data (TAASD) through an authorized, risk-based process that evaluates, implements and validates changes before and after deployment.

7. Cloud Security (CLD)
Govern cloud services and environments through risk-based, cloud-native security, compliance and resilience practices aligned with shared responsibility obligations.

8. Compliance (CPL)
Govern security, compliance and data protection obligations to maintain defensible evidence of conformity with applicable internal and external requirements.

9. Configuration Management (CFG)
Establish and enforce secure configuration baselines that implement least privilege and least functionality for Technology Assets, Applications and Services (TAAS) to support a defensible secure configuration posture.

10. Continuous Monitoring (MON)
Maintain situational awareness through centralized collection, correlation and analysis of security-relevant telemetry from Technology Assets, Applications and Services (TAAS).

11. Cryptographic Protections (CRY)
Use appropriate cryptographic mechanisms and industry-recognized key management practices to protect sensitive and regulated data at rest and in transit.

12. Data Classification & Handling (DCH)
Enforce a standardized classification methodology to determine data sensitivity and support Technology Assets, Applications and Services (TAAS) criticality decisions, enabling appropriate data handling, protection, retention and disposal requirements.

13. Embedded Technology (EMB)
Apply risk-based security, compliance and resilience practices to embedded technologies where compromise or misuse could create operational, safety and/or data protection impacts.

14. Endpoint Security (END)
Harden and centrally manage endpoint devices to protect Technology Assets, Applications, Services and Data (TAASD) from unauthorized access, compromise and disruption.

15. Human Resources Security (HRS)
Execute security-informed personnel management practices that address screening, onboarding, acceptable behavior, role-based risk, competence and offboarding requirements.

16. Identification & Authentication (IAC)
Implement secure, compliant and resilient Identity and Access Management (IAM) capabilities that enforce least privilege across human users, devices, service accounts and other Non-Person Entities (NPEs).

17. Incident Response (IRO)
Maintain a tested incident response capability that enables trained responders to identify, analyze, contain, eradicate and recover from incidents according to documented Incident Response Plans (IRPs).

18. Information Assurance (IAO)
Execute Information Assurance (IA) practices to validate that expected security, compliance and resilience controls are appropriately designed and operating as intended for Technology Assets, Applications and Services (TAAS).

19. Maintenance (MNT)
Proactively maintain Technology Assets, Applications and Services (TAAS) through authorized maintenance practices that preserve performance, security, compliance, resilience and supportability.

20. Mobile Device Management (MDM)
Govern mobile device access to Technology Assets, Applications, Services and Data (TAASD) to reduce attack surface and data exposure.

21. Network Security (NET)
Architect and implement defense-in-depth network protections that segment, restrict and monitor access to Technology Assets, Applications, Services and Data (TAASD).

22. Physical & Environmental Security (PES)
Protect physical environments through layered physical security and environmental controls that safeguard physical and digital assets from unauthorized access, theft, damage and disruption.

23. Data Privacy (PRI)
Execute risk-based and legally defensible data privacy practices that conform with applicable statutory, regulatory and contractual obligations to protect sensitive Personal Data (sPD) throughout its lifecycle.

24. Project & Resource Management (PRM)
Operationalize security, compliance and resilience objectives by integrating cybersecurity and data privacy requirements into project, program and resource management practices.

SECURE CONTROLS FRAMEWORK

SCR 2026.2

25. Risk Management (RSK)
Proactively identify, assess, prioritize and treat risks to align Technology Assets, Applications, Services and Data (TAASD)-related decisions with the organization's defined risk appetite and risk tolerance.

26. Quantum Security (QTS)
Mitigate quantum-enabled cryptographic risks through governance structures that operationalize Post-Quantum Cryptography (PQC) risk management practices.

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

28. Security Operations (OPS)
Deliver secure, compliant and resilient operations through defined processes, skilled personnel, monitoring, escalation and continuous improvement that effectively detect, isolate, and remediate cyber threats while ensuring business resilience.

29. Security Awareness & Training (SAT)
Foster a security, compliance and resilience-minded workforce through ongoing, role-based education on evolving threats, obligations and secure workplace practices.

30. Technology Development & Acquisition (TDA)
Develop and acquire Technology Assets, Applications and Services (TAAS) through secure-by-design, risk-informed and resilient lifecycle practices.

31. Third-Party Management (TPM)
Execute Supply Chain Risk Management (SCRM) practices to assess, select, contract, monitor and manage trustworthy third parties for product and service delivery.

32. Threat Management (THR)
Proactively identify, assess and manage threats to Technology Assets, Applications, Services and Data (TAASD) and business processes to inform risk decisions and corrective actions.

33. Vulnerability & Patch Management (VPM)
Reduce exploitable weaknesses in Technology Assets, Applications and Services (TAAS) through coordinated vulnerability identification, prioritization, remediation and validation practices.

34. Web Security (WEB)
Protect Internet-facing Technology Assets, Applications and Services (TAAS) by minimizing attack surfaces and monitoring for anomalous activity.