Framework, Standard or Model (FSM)

Program Area	Value Add	Security Controls Area	Best Practice FSM Selection
Cyber Technical Safeguards	Technology - Resource focused controls to minimize common attack vectors.	• Implementation Groups (Control Levels) • Asset Inventory, Hardware & Software. • Vulnerability & Configuration Mgmt. • Malicious Code • Response and Readiness	**CIS Controls v8.1**

Zero Trust (ZT) Roadmap	Allows for mapping ZT principles via planned roadmapping exercises across all security domains.	• Five pillars and three cross-cutting capabilities. Each pillar of the maturity model provides specific examples of ZT Architectures:
		  • Traditional
		  • Initial
		  • Advanced
		  • Optimal
			CISA Zero Trust Maturity Model

Cloud Security Assurance	Cloud based security controls and responsibilities for all cloud providers, customers and shared services.	• Cloud Governance & Shared Responsibilities (Provider, Customer & Service)	**CSA Cloud Controls v4.1**
Cyber Security Risk	If done properly a balance of people, process and technology. Often for complete technology aspects combining with CIS can be very effective. Generally better for SMBs or medium sized companies.	• Govern - Govern Risk, Compliance (GRC) & Security Strategy • Identify - Assessment, Scanning, Knowing your Environment • Protect - Defensive Capabilities • Detect - Monitoring • Respond - Incident Responce • Recover - BCP/DR & Resilience	**NIST CSF 2.0**
Security & Privacy Controls	A much more thorough framework than NIST CSF but also harder to implement and geared for more larger enterprises.	• Access Control & Auditing • Contingency and Incident Response (IR) • Supply Chain (TPRM) • Privacy	**NIST SP 800-53**
Zero Trust Architecture	Continuous verification around users, assets and resources.	• Identity and Asset Posture • Policy Decision and Enforcement • Telemetry • Segmentation • Least Privilege	**NIST SP 800-160 v1**
SDLC - Secure Development Lifecycle	Catch security and even code quality issues earlier in the development cycle.	• Code security flaw detection • Protect code Integrity • Reduce production flaws • Lifecycle of more security software	**NIST SSDF SP 800-218**
OT/IACS/IOT/PLC Cybersecurity	Securing of industrial and operational technologies via baseline and security requirements.	• Zones & Conduits • Security Levels • Lifecycle Controls • Asset Owner • Integration • Supplier Duties • Segmentation & VM MGMT.	**ISA/IEC 62443**
Credit Card Payment Security	Meet strict PCI payment processing technical and operational requirements.	• Network Security Controls • System Security Controls • Cardholder Data Protection • Access Control • Monitoring • Testing	**PCI DS v4.0.1**
General Information Security Management	A complete system and process of certifying a management system based in information, security, risk and continual improvement. Generally geared towards larger organizations.	• ISMS Scope & Objectives • Risk Assessment, Reduction and Remediation • Policies • Roles • Overall General Security Controls • Improvement	**ISO/IEC 27001**
Security Control Guidance	Complete program for applying practical safeguards for information security, cybersecurity and privacy protection. Generally geared towards larger organizations.	• Organizational Controls • People Related Controls • Physical Controls • Technology Controls • Monitoring	**ISO/IEC 27002**

Program Area	Value Add	Security Controls Area	Best Practice FSM Selection

Application Security	The standard provides a basis for testing application technical security controls, as well as any technical security controls in the environment, that are relied on to protect against vulnerabilities.	• Controls focus on the reduction of technology vulnerabilities, such as:
		  • Cross-Site Scripting (XSS)
		  • SQL injection.
		• This standard can be used to establish a level of confidence in the security of Web applications.
			OWASP ASVS 5.0.0

GenAI Application Security	identifying, mitigating, and documenting security and safety risks associated with generative AI technologies, including large language models (LLMs), agentic AI systems, and AI-driven applications.	• Goal is for secure development, deployment, and governance of generative AI systems.	**OWASP Top 10 for LLM**

Threat Behaviors & Knowledge (Threat Intelligence)	Methodology for connecting the complexity of threat actor tactics, detection engineering, threat hunting and validation of applicable controls and mitigating controls.	• Threat Intelligence
		  • Tactics and Techniques
		  • Adversary
		  • Detection Logic
		  • Defense Testing
			MITRE ATT&CK v19

Resource
https://learn.cisecurity.org/cis-controls-download
https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf
https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4-1
https://www.nist.gov/cyberframework
https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final
https://csrc.nist.gov/pubs/sp/800/218/final
https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
https://blog.pcisecuritystandards.org/just-published-pci-dss-v4-0-1
https://www.iso.org/standard/27001
https://www.iso.org/standard/75652.html

Resource
https://owasp.org/www-project-application-security-verification-standard/
https://owasp.org/www-project-top-10-for-large-language-model-applications/
https://attack.mitre.org/resources/updates/updates-april-2026/