

Digital Security Program Domains

#	DSP Domain	Domain Identifier	Cybersecurity & Data Privacy by Design (C/P) Principles
1	Cybersecurity & Data Privacy 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.
2	Artificial and Autonomous Technology	AAT	Ensure trustworthy and resilient Artificial Intelligence (AI) and autonomous technologies to achieve a beneficial impact by informing, advising or simplifying tasks, while minimizing emergent properties or unintended consequences.
3	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.
4	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.
5	Capacity & Performance Planning	CAP	Govern the current and future capacities and performance of technology assets.
6	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.
7	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.
8	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
9	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,
10	Continuous Monitoring	MON	Maintain situational awareness of security-related events through the centralized collection and analysis of event logs from systems, applications and services.
11	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.
12	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
13	Embedded Technology	EMB	Provide additional scrutiny to reduce the risks associated with embedded technology, based on the potential damages posed from malicious use of the technology.
14	Endpoint Security	END	Harden endpoint devices to protect against reasonable threats to those devices and the data those devices store, transmit and process.
15	Human Resources Security	HRS	Execute sound hiring practices and ongoing personnel management to cultivate a cybersecurity & data privacy-minded workforce.
16	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.
17	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).
18	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
19	Maintenance	MAI	Proactively maintain technology assets, according to current vendor recommendations for configurations and updates, including those supported or hosted by third-parties.
20	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
21	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.
22	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.
23	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.
24	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
25	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.
26	Secure Engineering & Architecture	SEA	Utilize industry-recognized secure engineering and architecture principles to deliver secure and resilient systems, applications and services.
27	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.
28	Security Awareness & Training	SAT	Foster a cybersecurity & data privacy-minded workforce through ongoing user education about evolving threats, compliance obligations and secure workplace practices.
29	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
30	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.
31	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.
32	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.
33	Web Security	WEB	Ensure the security and resilience of Internet-facing technologies through secure configuration management practices and monitoring for anomalous activity.

Geography	Mapping Column Header	Source	Authoritative Source - Statutory / Regulatory / Contractual / Industry Framework	Version	URL - Authoritative Source
Universal	AICPA TSC 2017 (SOC 2)	AICPA	Service Organization Control - Trust Services Criteria (TSC) - SOC2	2017	https://www.aicpa.org/interestareas/frc/assuranceadvisorservices/aicpasoc2report.html
Universal	BSI Standard 200-1	BSI	Standard 200-1	2022	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standards/200-1-Managementssysteme-fuer-Informationssicherheit/bsi-standard-200-1-managementsysteme-fuer-informationssicherheit_node.html
Universal	CIS CSC v8.0	CIS	Critical Security Controls (CSC)	8.0	https://www.cisecurity.org/controls/v8/
Universal	COBIT 2019	ISACA	Control Objectives for Information and Related Technologies (COBIT)	2019	http://www.isaca.org/COBIT/Pages/COBIT-2019-Framework-Governance-and-Management-Objectives.aspx
Universal	COSO v2017	COSO	Committee of Sponsoring Organizations (COSO) 2017 Framework	2017	https://www.coso.org/Shared%20Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf
Universal	CSA CCM v4	CSA	Cloud Controls Matrix (CCM)	v4	https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview
Universal	CSA IoT SCF v2	CSA	CSA IoT Security Controls Framework v2	v2	https://cloudsecurityalliance.org/artifacts/csa-iot-security-controls-framework-v2/
Universal	ENISA v2.0	EU	European Union Agency for Network and Information Security (ENISA)	2.0	https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf
Universal	GAPP	AICPA	Generally Accepted Privacy Principles (GAPP)	1.0	https://www.kscpa.org/writable/files/AICPADocuments/10-15-13_aicpa_cica_privacy_maturity_model_finalebook.pdf
Universal	IEC 62443-4-2	IEC	IEC 62443-4-2:2019 - Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components	2019	https://webstore.iec.ch/publication/34421
Universal	ISO/SAE 21434 v2021	IEC	ISO/SAE 21434:2021 - Road vehicles — Cybersecurity engineering	2021	https://www.iso.org/standard/70918.html
Universal	ISO 22301 v2019	ISO	22301 - Security and resilience — Business continuity management systems — Requirements	2019	https://www.iso.org/standard/75106.html
Universal	ISO 27001 v2013	ISO	27001 - Information Security Management Systems (ISMS) - Requirements	2013	https://www.iso.org/standard/54534.html
Universal	ISO 27001 v2022	ISO	27001 - Information Security Management Systems - Requirements	2022	https://www.iso.org/standard/27001
Universal	ISO 27002 v2013	ISO	27002 - Code of Practice for Information Security Controls	2013	https://www.iso.org/standard/54533.html
Universal	ISO 27002 v2022	ISO	27002 - Information security, cybersecurity and privacy protection - Information security controls	2022	https://www.iso.org/standard/75652.html
Universal	ISO 27017 v2015	ISO	27017 - Information technology security techniques — Code of practice for information security controls based on ISO/IEC 27001 for cloud services	2015	https://www.iso.org/standard/43757.html
Universal	ISO 27018 v2014	ISO	27018 - Code of Practice for PI in Clouds Acting as PI Processors	2014	https://www.iso.org/standard/61498.html
Universal	ISO 27701 v2019	ISO	27701 - Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines	2019	https://www.iso.org/standard/71670.html
Universal	ISO 29100 v2011	ISO	29100 - Privacy Framework	2011	https://www.iso.org/standard/45123.html
Universal	ISO 31000 v2009	ISO	31000 - Risk Management	2009	https://www.iso.org/iso-31000-risk-management.html
Universal	ISO 31010 v2009	ISO	31010 - Risk Assessment Techniques	2009	https://www.iso.org/standard/51073.html
Universal	MITRE ATT&CK 10	MITRE	MITRE ATT&CK - NIST 800-53 mappings	N/A	https://mitre-engenuity.org/blog/2022/01/13/nist-800-53-control-mappings/
Universal	MPA Content Security Program v5.1	MPA	MPA Content Security Best Practices Common Guidelines	5.1	https://www.motionpictures.org/what-we-do/safeguarding-creativity/additional-resources/#content-protection-best-practices
Universal	NAIC Insurance Data Security Model Law (MDL-668)	NAIC	Insurance Data Security Model Law (MDL-668)	N/A	https://www.naic.org/store/free/MDL-668.pdf
Universal	NIST Privacy Framework v1.0	NIST	NIST Privacy Framework	1.0	https://www.nist.gov/privacy-framework
Universal	NIST SSDF	NIST	Secure Software Development Framework (SSDF): Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)	N/A	https://nvlpubs.nist.gov/nistpubs/CSWP/NIST-CSWP-04232020.pdf
Universal	NIST 800-37 rev 2	NIST	SP 800-37 - Guide for Applying the RMF to Federal Information Systems rev2	2	https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
Universal	NIST 800-39	NIST	SP 800-39 - Managing Information Security Risk	N/A	https://csrc.nist.gov/publications/detail/sp/800-39/final
Universal	NIST 800-53 rev4	NIST	SP 800-53 - Security and Privacy Controls for Information Systems and Organizations	4	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
Universal	NIST 800-53 rev4 [low]	NIST	SP 800-53 - Security and Privacy Controls for Information Systems and Organizations (low baseline)	4	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
Universal	NIST 800-53 rev4 [moderate]	NIST	SP 800-53 - Security and Privacy Controls for Information Systems and Organizations (moderate baseline)	4	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Authoritative Sources

Geography	Mapping Column Header	Source	Authoritative Source - Statutory / Regulatory / Contractual / Industry Framework	Version	URL - Authoritative Source
Universal	NIST 800-53 rev4 [High]	NIST	SP 800-53 - Security and Privacy Controls for Information Systems and Organizations (high baseline)	4	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
Universal	NIST 800-53 rev5	NIST	SP 800-53 - Security and Privacy Controls for Information Systems and Organizations	5	https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
Universal	NIST 800-53 rev5 [Privacy]	NIST	SP 800-53 - Security and Privacy Controls for Information Systems and Organizations Privacy Baseline	5	https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
Universal	NIST 800-53 rev5 [Low]	NIST	SP 800-53 - Security and Privacy Controls for Information Systems and Organizations Low Baseline	5	https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
Universal	NIST 800-53 rev5 [Moderate]	NIST	SP 800-53 - Security and Privacy Controls for Information Systems and Organizations Moderate Baseline	5	https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
Universal	NIST 800-53 rev5 [High]	NIST	SP 800-53 - Security and Privacy Controls for Information Systems and Organizations High Baseline	5	https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
Universal	NIST 800-53 rev5 [NOC]	NIST	SP 800-53 - Security and Privacy Controls for Information Systems and Organizations Select Not Otherwise Categorized (NOC) controls	5	https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
Universal	NIST 800-63B (partial mapping)	NIST	SP 800-63B - Digital Identity Guidelines (partial mapping)	June 2017	https://pages.nist.gov/800-63-3/sp800-63b.html
Universal	NIST 800-82 rev3 LOW OT Overlay	NIST	NIST SP 800-82 - Guide to Industrial Control Systems (ICS) Security	rev 3	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf
Universal	NIST 800-82 rev3 MODERATE OT Overlay	NIST	NIST SP 800-82 - Guide to Industrial Control Systems (ICS) Security	rev 3	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf
Universal	NIST 800-82 rev3 HIGH OT Overlay	NIST	NIST SP 800-82 - Guide to Industrial Control Systems (ICS) Security	rev 3	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf
Universal	NIST 800-160	NIST	NIST SP 800-160 - Systems Security Engineering	N/A	https://csrc.nist.gov/publications/detail/sp/800-160/final
Universal	NIST 800-161 rev 1	NIST	NIST SP 800-161 - Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations	rev 1	https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final
Universal	NIST 800-161 rev 1 CSCRM Baseline	NIST	NIST SP 800-161 - Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations	rev 1	https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final
Universal	NIST 800-161 rev 1 Flow Down	NIST	NIST SP 800-161 - Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations	rev 1	https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final
Universal	NIST 800-161 rev 1 Level 1	NIST	NIST SP 800-161 - Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations	rev 1	https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final
Universal	NIST 800-161 rev 1 Level 2	NIST	NIST SP 800-161 - Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations	rev 1	https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final
Universal	NIST 800-161 rev 1 Level 3	NIST	NIST SP 800-161 - Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations	rev 1	https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final
Universal	NIST 800-171 rev 2	NIST	SP 800-171 - Protecting CUI in Non-Federal Systems and Organizations	2	https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
Universal	NIST 800-171 rev 3 FPD	NIST	NIST SP 800-171 R3 Final Public Draft (FPD)	Rev 3 FPD	https://csrc.nist.gov/pubs/sp/800/171/r3/fpd
Universal	NIST 800-171A	NIST	SP 800-171A - Assessing Security Requirements for Controlled Unclassified Information	N/A	https://csrc.nist.gov/publications/detail/sp/800-171a/final
Universal	NIST 800-171A rev 3 IPD	NIST	NIST 800-171A R3 Initial Public Draft (IPD)	Rev 3 IPD	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171Ar3.ipd.pdf
Universal	NIST 800-172	NIST	SP 800-172 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets	N/A	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172.pdf
Universal	NIST 800-218 v1.1	NIST	SP 800-218 - Secure Software Development Framework (SSDF) Version 1.1:	v1.1	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf
Universal	NIST CSF v1.1	NIST	Cybersecurity Framework (CSF)	1.1 (Apr 19)	https://www.nist.gov/cyberframework
Universal	NIST CSF v2.0 IPD	NIST	Cybersecurity Framework (CSF) 2.0 Initial Public Draft (IPD)	2.0 IPD	https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf
Universal	OWASP Top 10 v2021	OWASP	Top 10 Most Critical Web Application Security Risks	2021	https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
Universal	PCI DSS v3.2	PCI SSC	Payment Card Industry Data Security Standard (PCI DSS)	3.2	https://www.pcisecuritystandards.org/document_library
Universal	PCIDSS v4.0	PCI SSC	Payment Card Industry Data Security Standard (PCI DSS)	4.0	https://www.pcisecuritystandards.org/document_library
Universal	PCIDSS v4.0 SAQ A	PCI SSC	Payment Card Industry Data Security Standard (PCI DSS) - SAQ A	4.0	https://www.pcisecuritystandards.org/document_library
Universal	PCIDSS v4.0 SAQ A-EP	PCI SSC	Payment Card Industry Data Security Standard (PCI DSS) - SAQ A-EP	4.0	https://www.pcisecuritystandards.org/document_library
Universal	PCIDSS v4.0 SAQ B	PCI SSC	Payment Card Industry Data Security Standard (PCI DSS) - SAQ B	4.0	https://www.pcisecuritystandards.org/document_library

Geography	Mapping Column Header	Source	Authoritative Source - Statutory / Regulatory / Contractual / Industry Framework	Version	URL - Authoritative Source
Universal	PCIDSS v4.0 SAQ B-IP	PCI SSC	Payment Card Industry Data Security Standard (PCI DSS) - SAQ B-IP	4.0	https://www.pcisecuritystandards.org/document_library
Universal	PCIDSS v4.0 SAQ C	PCI SSC	Payment Card Industry Data Security Standard (PCI DSS) - SAQ C	4.0	https://www.pcisecuritystandards.org/document_library
Universal	PCIDSS v4.0 SAQ C-VT	PCI SSC	Payment Card Industry Data Security Standard (PCI DSS) - SAQ C-VT	4.0	https://www.pcisecuritystandards.org/document_library
Universal	PCIDSS v4.0 SAQ D Merchant	PCI SSC	Payment Card Industry Data Security Standard (PCI DSS) - SAQ D Merchant	4.0	https://www.pcisecuritystandards.org/document_library
Universal	PCIDSS v4.0 SAQ D Service Provider	PCI SSC	Payment Card Industry Data Security Standard (PCI DSS) - SAQ D Service Provider	4.0	https://www.pcisecuritystandards.org/document_library
Universal	PCIDSS v4.0 SAQ P2PE	PCI SSC	Payment Card Industry Data Security Standard (PCI DSS) - SAQ P2PE	4.0	https://www.pcisecuritystandards.org/document_library
Universal	Shared Assessments SIG 2023	Shared Assessments	Shared Assessments Standard Information Gathering Questionnaire (SIG)	2023	https://sharedassessments.org/sig/
Universal	SWIFT CSF v2023	SWIFT	SWIFT Customer Security Controls Framework	2021	https://www.swift.com/myswift/customer-security-programme-csp/security-controls
Universal	TISAX ISA v5.1.0	TISAX	TISAX ISA	5.1.0	https://portal.enx.com/en-us/TISAX/downloads/
Universal	UL 2900-1	UL	2900-1 - Software Cybersecurity for Network-Connectable Products	N/A	https://industries.ul.com/cybersecurity/ul-2900-standards-process
Universal	UN RISS	United Nations	UN Regulation No. 155 - Cyber security and cyber security management system	N/A	https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-cyber-security
Universal	UN ECE WP.29	United Nations	UNECE WP.29	N/A	https://unece.org/fileadmin/DAM/trans/doc/2020/wp29/ECE-TRANS-WP29-2020-079e.pdf
US	US C2M2 v2.1	Federal	Cybersecurity Capability Maturity Model v2.1	2.1	https://c2m2.doe.gov/
US	US CERT RMM v1.2	Federal	CERT Resilience Management Model	1.2	https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084
US	US CISA CPG v2022	Federal	CISA Cross-Sector Cybersecurity Performance Goals (CPG)	2022	https://www.cisa.gov/cpg
US	US CJIS Security Policy 5.9	Federal	US DOJ / FBI - Criminal Justice Information Services (CJIS) Security Policy	5.9	https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view
US	US CMMC 2.0 Level 1	Federal	Cybersecurity Maturity Model Certification (CMMC)	1.02	https://www.aco.osd.mil/cmmc/index.html
US	US CMMC 2.0 Level 2	Federal	Cybersecurity Maturity Model Certification (CMMC)	1.02	https://www.aco.osd.mil/cmmc/index.html
US	US CMMC 2.0 Level 3	Federal	Cybersecurity Maturity Model Certification (CMMC)	1.02	https://www.aco.osd.mil/cmmc/index.html
US	US CMMC 2.1 (draft) Level 1	Federal	Cybersecurity Maturity Model Certification (CMMC)	2.1 draft	https://www.reginfo.gov/public/do/PRAICList?ref_nbr=202211-0704-001
US	US CMMC 2.1 (draft) Level 2	Federal	Cybersecurity Maturity Model Certification (CMMC)	2.1 draft	https://www.reginfo.gov/public/do/PRAICList?ref_nbr=202211-0704-001
US	US CMMC 2.1 (draft) Level 3	Federal	Cybersecurity Maturity Model Certification (CMMC)	2.1 draft	https://www.reginfo.gov/public/do/PRAICList?ref_nbr=202211-0704-001
US	US OMS MARS-E v2.0	Federal	US Centers for Medicare & Medicaid Services MARS-E Document Suite, Version 2.0	2.0	https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/3-MARS-E-v2-0-Catalog-of-Security-and-Privacy-Controls-11102015.pdf
US	US COPPA	Federal	Children's Online Privacy Protection Act (COPPA)	N/A	http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim
US	US DFARS Cybersecurity 252.204-70xx	Federal	Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7008 - 7012	252.204-7008	https://www.aco.osd.mil/dpap/dars/dfars/html/current/252204.htm
US	US FACTA	Federal	Fair & Accurate Credit Transactions Act (FACTA) / Fair Credit Reporting Act (FCRA)	N/A	http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0111-fair-credit-reporting-act.pdf
US	US FAR 52.204-21	Federal	Federal Acquisition Regulation (FAR)	52.204-21	https://www.acquisition.gov/far/52.204-21
US	US FAR 52.204-27	Federal	52.204-27 Prohibition on a ByteDance Covered Application	52.204-27	https://www.acquisition.gov/far/52.204-27
US	US FAR Section 889	Federal	Federal Acquisition Regulation (FAR) - Section 889	889	https://www.federalregister.gov/documents/2020/07/14/2020-15293/federal-acquisition-regulation-prohibition-on-contracting-with-entities-using-certain
US	US FDA 21 CFR Part 11	Federal	Food & Drug Administration (FDA)	21 CFR Part 11	https://www.gpo.gov/fdsys/pkg/CFR-2012-title21-vol1/pdf/CFR-2012-title21-vol1-part11.pdf
US	US FedRAMP	Federal	Federal Risk and Authorization Management Program (FedRAMP)	R4	https://www.fedramp.gov/
US	US FedRAMP [low]	Federal	Federal Risk and Authorization Management Program (FedRAMP) (low baseline)	R4	https://www.fedramp.gov/

Geography	Mapping Column Header	Source	Authoritative Source - Statutory / Regulatory / Contractual / Industry Framework	Version	URL - Authoritative Source
US	US FedRAMP (moderate)	Federal	Federal Risk and Authorization Management Program (FedRAMP) (moderate baseline)	R4	https://www.fedramp.gov/
US	US FedRAMP (high)	Federal	Federal Risk and Authorization Management Program (FedRAMP) (high baseline)	R4	https://www.fedramp.gov/
US	US FedRAMP (LI-SaaS)	Federal	Federal Risk and Authorization Management Program (FedRAMP) (LI-SaaS) baseline)	R4	https://www.fedramp.gov/
US	US FedRAMP R5	Federal	Federal Risk and Authorization Management Program (FedRAMP) R5	R5	https://www.fedramp.gov/
US	US FedRAMP R5 (low)	Federal	Federal Risk and Authorization Management Program (FedRAMP R5) (low baseline)	R5	https://www.fedramp.gov/
US	US FedRAMP R5 (moderate)	Federal	Federal Risk and Authorization Management Program (FedRAMP R5) (moderate baseline)	R5	https://www.fedramp.gov/
US	US FedRAMP R5 (high)	Federal	Federal Risk and Authorization Management Program (FedRAMP R5) (high baseline)	R5	https://www.fedramp.gov/
US	US FedRAMP R5 (LI-SaaS)	Federal	Federal Risk and Authorization Management Program (FedRAM R5P) (LI-SaaS) baseline)	R5	https://www.fedramp.gov/
US	US FERPA	Federal	Family Educational Rights and Privacy Act (FERPA)	N/A	https://www.gpo.gov/fdsys/pkg/USCODE-2010-title20/pdf/USCODE-2010-title20-chap31-subchap11-part4-sec1232g.pdf
US	US FFIEC	Federal	Federal Financial Institutions Examination Council (FFIEC)	N/A	https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_B_Map_to_NIST_CSF_June_2015_PDF.pdf
US	US FINRA	Federal	Financial Industry Regulatory Authority (FINRA)	N/A	http://www.finra.org/industry/cybersecurity
US	US FTC Act	Federal	Federal Trade Commission (FTC) Act	N/A	https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act
US	US GLBA CFR 314	Federal	Gramm Leach Bliley Act (GLBA)	CFR 314	https://www.federalregister.gov/documents/2021/12/09/2021-25736/standards-for-safeguarding-customer-information
US	US HIPAA	Federal	Health Insurance Portability and Accountability Act (HIPAA)	N/A	https://www.hhs.gov/hipaa/for-professionals/security/index.html
US	HIPAA - HICP Small Practice	Federal	Health Industry Cybersecurity Practices (HICP) - Small Practice	N/A	https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx
US	HIPAA - HICP Medium Practice	Federal	Health Industry Cybersecurity Practices (HICP) - Medium Practice	N/A	https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx
US	HIPAA - HICP Large Practice	Federal	Health Industry Cybersecurity Practices (HICP) - Large Practice	N/A	https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx
US	US IRS 1075	Federal	Internal Revenue Service (IRS) Section 1075	N/A	https://www.irs.gov/pub/irs-pdf/p1075.pdf
US	ITAR Part 120 (limited)	Federal	International Traffic in Arms Regulation (ITAR) (limited to Part 120)	N/A	https://www.ecfr.gov/cgi-bin/text-idx?SID=70e390c181ea17f847fa696c47e3140a&mc=true&node=pt22.1.120&rgn=div
US	US NERC CIP	Federal	North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)	N/A	http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
US	US NISPOM	Federal	National Industrial Security Program Operating Manual (NISPOM)	N/A	http://www.dss.mil/documents/odaa/nispom2006-5220.pdf
US	US NNPI (unclass)	Federal	Naval Nuclear Propulsion Information (NNPI)	N/A	https://www.secnv.navy.mil/doni/Directives/09000%20General%20Ship%20Design%20and%20Support/09-200%20Propulsion%20Plants%20Support/N9210.3%20(Unclas%20Portion).pdf
US	US NSTC NSPM-33	Federal	National Science & Technology Council (NSTC) NSPM-33	N/A	https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf
US	US Privacy Shield	Federal	Privacy Shield	N/A	https://www.privacyshield.gov/article?id=Requirements-of-Participation
US	US SEC Cybersecurity Rule	Federal	Cybersecurity Final Rule (Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure) - 17 CFR Parts 229, 232, 239, 240, and 249	N/A	https://www.sec.gov/files/rules/final/2023/33-11216.pdf
US	US SOX	Federal	Sarbanes Oxley Act (SOX)	N/A	http://www.sec.gov/about/laws/soa2002.pdf
US	US SSA EISR v8.0	Federal	Social Security Administration (SSA) Electronic Information Exchange Security Requirements	8.0	https://www.ssa.gov/dataexchange/security.html
US	StateRAMP Low Category 1	State	StateRAMP Low (Category 1)	N/A	https://stateramp.org/documents/
US	StateRAMP Low+ Category 2	State	StateRAMP Low+ (Category 2)	N/A	https://stateramp.org/documents/
US	StateRAMP Moderate Category 3	State	StateRAMP Moderate (Category 3)	N/A	https://stateramp.org/documents/
US	US - AK PIPA	State	AK - Alaska Personal Information Protection Act (PIPA)	N/A	http://law.alaska.gov/departments/civil/consumer/4548.html
US	US - CA SB327	State	CA - SB327	N/A	https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=2017201805B327

Geography	Mapping Column Header	Source	Authoritative Source - Statutory / Regulatory / Contractual / Industry Framework	Version	URL - Authoritative Source
US	US-CA CPRA (Nov 2022)	State	California Privacy Rights Act (CPRA) - November 2022 version	November 2022	https://cnpa.ca.gov/regulations/pdf/20221102_mod_text.pdf
US	US - CA SB1386	State	CA - SB1386	N/A	https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=2001200205B1386
US	US - CO Colorado Privacy Act	State	CO - Colorado Privacy Act	N/A	https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf
US	US - IL BIPA	State	Illinois Biometric Information Privacy Act (PIPA)	N/A	https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57
US	US - IL IPA	State	Illinois Identity Protection Act (IPA)	N/A	https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3174&ChapterID=2
US	US - IL PIPA	State	IL - Illinois Personal Information Protection Act (PIPA)	N/A	https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapterID=67
US	US - MA 201 CMR 17.00	State	MA - 201 CMR 17.00	N/A	http://www.mass.gov/ocabr/docs/dtheft/201cmr1700reg.pdf
US	US - NV SB220	State	NV - SB220	N/A	https://www.leg.state.nv.us/App/NEUS/REL/80th2019/Bill/6365/Text
US	US - NY DFS 23 NYCRR500	State	NY - NY DFS 23NYCRR500	N/A	http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf
US	US - NY SHIELD Act S575B	State	NY - SHIELD Act (SB 5575B)	N/A	https://legislation.nysenate.gov/pdf/bills/2019/s575b
US	US - OR 646A	State	OR - ORS 646A	N/A	https://www.oregonlegislature.gov/bills_laws/ors/646a.html
US	US - SC Insurance Data Security Act	State	SC - South Carolina Insurance Data Security Act	N/A	https://www.scstatehouse.gov/sess122_2017-2018/bills/4655.htm
US	US - TX BC521	State	TX - BC521	N/A	http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC_521.htm
US	US-TX Cybersecurity Act	State	TX - Cybersecurity Act	N/A	http://www.legis.state.tx.us/tlodocs/85B/billtext/pdf/HB0008F.pdf#navpanes=0
US	US-TX DIR Control Standards 2.0	State	TX - DIR Security Control Standards Catalog	2.0	https://dir.texas.gov/resource-library/item/security-controls-standards-catalog
US	US-TX TX-RAMP	State	TX - Texas Risk & Authorization Management Program (TX-RAMP)	N/A	http://dir.texas.gov/texas-risk-and-authorization-management-program-tx-ramp
US	US-TX SB820	State	TX - 2019 - SB820	N/A	https://www.legiscan.com/TX/text/SB820/id/2027614/Texas-2019-SB820-Enrolled.html
US	US-VA CPA 2023	State	Virginia Consumer Data Protection Act	2023	https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+CHAP0035+pdf
US	US-VT Act 171 of 2018	State	VT - Act 171 of 2018 (Liquor Registration Act)	N/A	https://legislature.vermont.gov/Documents/2018/Docs/ACTS/ACT171/ACT171%20As%20Enacted.pdf
EMEA	EMEA EU EBA GL/2019/04	EU	European Banking Authority (EBA) Guidelines on ICT and security risk management	N/A	https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management
EMEA	EMEA EU DORA	EU	EU Digital Operational Resilience Act (DORA)	2023	https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554&from=EN
EMEA	EMEA EU Privacy [draft]	EU	ePrivacy Directive	draft	http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241
EMEA	EMEA EU GDPR	EU	General Data Protection Regulation (GDPR)	N/A	http://ec.europa.eu/justice/data-protection/reform/index_en.htm
EMEA	EMEA EU NIS2	EU	ENISA NIS2 (Directive (EU) 2022/2555)	N/A	https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new
EMEA	EMEA EU PSD2	EU	Second Payment Services Directive (PSD2)	N/A	https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf
EMEA	EMEA EU EU-US Data Privacy Framework	EU	EU-US Data Privacy Framework	N/A	https://www.dataprivacyframework.gov/s/
EMEA	EMEA Austria	Austria	Federal Act concerning the Protection of Personal Data (DSG 2000)	N/A	https://www.ris.bka.gv.at/Dokumente/Erw/ERV_1999_1_165/ERV_1999_1_165.pdf
EMEA	EMEA Belgium	Belgium	Act of 8 December 1992	N/A	http://www.privacycommission.be/sites/privacycommission/files/documents/Privacy_Act_1992.pdf
EMEA	EMEA Czech Republic	Czech Republic	Act No. 101/2000 on the Protection of Personal Data	N/A	https://www.uoou.cz/en/vismo/zobraz_dok.asp?id_ktg=1107&p1=1107
EMEA	EMEA Denmark	Denmark	Act on Processing of Personal Data (Act No. 429 of May 31, 2000)	N/A	http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/
EMEA	EMEA Finland	Finland	Personal Data Act (986/2000)	N/A	http://www.finlex.fi/en/laki/kaannokset/1999/en19990523.pdf
EMEA	EMEA France	France	78 17 / 2004 8021 - Information Technology, Data Files & Civil Liberty	N/A	http://www.cnll.fr/fileadmin/documents/en/Act78-17VA.pdf

Geography	Mapping Column Header	Source	Authoritative Source - Statutory / Regulatory / Contractual / Industry Framework	Version	URL - Authoritative Source
EMEA	EMEA Germany	Germany	Federal Data Protection Act	N/A	https://www.gesetze-im-internet.de/englisch_bdsge/englisch_bdsge.pdf
EMEA	EMEA Germany Banking Supervisory Requirements for IT (BAIT)	Germany	Banking Supervisory Requirements for IT (BAIT)	N/A	https://www.bafin.de/SharedDocs/Downloads/EN/Rundschreiben/dl_rs_1710_ba_BAIT_en.html?__blob=publicationFile&cid=3798FF98313981E73C57CD178025_1_cid3897nn=9866146
EMEA	EMEA Germany CS-2020	Germany	Cloud Computing Compliance Controls Catalogue (C5)	2020	https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Criteria_Catalogue/Compliance_Criteria_Catalogue_node.html
EMEA	EMEA Greece	Greece	Protection of Individuals with Regard to the Processing of Personal Data (2472/1997)	N/A	http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW%202472-97-NOV2013-EN.PDF
EMEA	EMEA Hungary	Hungary	Informational Self-Determination and Freedom of Information (Act CXII of 2011)	N/A	http://www.naih.hu/files/Privacy_Act-CXII-of-2011_EN_201310.pdf
EMEA	EMEA Ireland	Ireland	Data Protection Act (2003)	N/A	http://www.irishstatutebook.ie/2003/en/act/pub/0006/print.html
EMEA	EMEA Israel CDMO v1.0	Israel	Cybersecurity Methodology for an Organization	1.0	https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/he/Cyber1.0_english_617_A4.pdf
EMEA	EMEA Israel	Israel	Protection of Privacy Law, 5741 – 1981	N/A	http://unpan1.un.org/intradoc/groups/public/documents/UN-DPADM/UNPAN041914.pdf
EMEA	EMEA Italy	Italy	Personal Data Protection Code	N/A	http://www.privacy.it/privacode-en.html
EMEA	EMEA Kenya DPA 2019	Kenya	Kenya Data Protection Act	2019	http://kenyalaw.org/ki/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct_No24of2019.pdf
EMEA	EMEA Luxembourg	Luxembourg	Protection of Personals with Regard to the Processing of Personal Data	N/A	http://www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi02082002_en.pdf
EMEA	EMEA Netherlands	Netherlands	Personal Data Protection Act	N/A	https://www.akd.nl/t/Documents/17-03-2016_ENG_Wet-bescherming-persoonsgegevens.pdf
EMEA	EMEA Nigeria DPR 2019	Nigeria	Nigeria Data Protection Regulation	N/A	https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf
EMEA	EMEA Norway	Norway	Personal Data Act	N/A	https://www.datatilsynet.no/en/regulations-and-tools/regulations-and-decisions/norwegian-privacy-law/personal-data-regulations/
EMEA	EMEA Poland	Poland	Act of 29 August 1997 on the Protection of Personal Data	N/A	http://www.giodo.gov.pl/144/id_art/171/li/en/
EMEA	EMEA Portugal	Portugal	Act on the Protection of Personal Data	N/A	https://www.cnpd.pt/english/bin/legislation/Law6798EN.HTM
EMEA	EMEA Qatar PDPL	Qatar	Personal Data Privacy Protection Law (PDPL)	N/A	https://compliance.ncert.org/sites/default/files/library/2020-11/Law%20No.%20%2813%29%20of%20the%202016%20%20Protecting%20Personal%20Data%20Privacy%20-%20English.pdf
EMEA	EMEA Russia	Russia	Federal Law of 27 July 2006 N 152-FZ	N/A	http://www.rg.ru/2006/07/29/personalnye-dannye-dok.html
EMEA	EMEA Saudi Arabia Critical Security Controls	Saudi Arabia	Saudi Arabian Monetary Authority - Cyber Security Framework	Version 1.0 (May 2017)	https://www.sama.gov.sa/en-US/Laws/FinanceRules/SAMA%20Cyber%20Security%20Framework%20v1.0%20final_updated.pdf
EMEA	EMEA Saudi Arabia SACS-002	Saudi Arabia	SACS-002 - Third Party Cybersecurity Standard	N/A	https://www.aramco.com/-/media/downloads/working-with-us/cc/sacs-002-third-party-cybersecurity-standard.pdf
EMEA	EMEA Saudi Arabia SAMA CSv1.0	Saudi Arabia	Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework (CSF)	2017 v1	https://www.sama.gov.sa/en-US/Laws/FinanceRules/SAMA%20Cyber%20Security%20Framework%20v1.0%20final_updated.pdf
EMEA	EMEA Saudi Arabia ECC-1 2018	Saudi Arabia	Essential Cybersecurity Controls (ECC – 1 : 2018)	2018	https://nca.gov.sa/files/ecc-en.pdf
EMEA	EMEA Saudi Arabia OTCC-1 2022	Saudi Arabia	Operational Technology Cybersecurity Controls (OTCC -1: 2022)	2022	https://nca.gov.sa/otcc_en.pdf
EMEA	EMEA Serbia 87/2018	Serbia	Act of 9 November 2018 on Personal Data Protection (Official Gazette No. 87/18)	N/A	http://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=109270&p_count=5&p_classification=018--text=Regulates%20the%20right%20to%20protection.penalties%2C%20special%20cases%2C%20prevention%20and
EMEA	EMEA Slovak Republic	Slovak Republic	Protection of Personal Data (122/2013)	N/A	https://www.dataprotection.gov.sk/uoou/sites/default/files/kcfinder/files/Act_122-2013_84-2014_en.pdf
EMEA	EMEA South Africa	South Africa	Protection of Personal Information Act (POPIA)	N/A	http://www.justice.gov.za/legislation/acts/2013-004.pdf
EMEA	EMEA Spain	Spain	Royal Decree 1720/2007 (protection of personal data)	N/A	https://www.mjusticia.gob.es/AreaTematica/DocumentacionPublicaciones/Documents/Royal_Decree_approving_the_regulations_relating_to_Constitutional_Act_on_Personal_Data_Protection_%28PDF
EMEA	EMEA Spain CCN-STIC 825	Spain	ICT Security Guide CCN-STIC 825	N/A	https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2148-ccn-stic-825-ens-nacional-security-framework-27001-certifications/file.html
EMEA	EMEA Sweden	Sweden	Personal Data Act	N/A	http://www.datainspektionen.se/en-english/legislation/the-personal-data-act/
EMEA	EMEA Switzerland	Switzerland	Federal Act on Data Protection (FADP)	N/A	https://www.admin.ch/opc/en/classified-compilation/19920153/index.html
EMEA	EMEA Turkey	Turkey	Regulation on Protection of Personal Data in Electronic Communications Sector	N/A	https://global.tbmm.gov.tr/docs/constitution_en.pdf
EMEA	EMEA UAE	UAE	Data Protection Law No. 1 of 2007	N/A	https://www.difc.ae/files/5814/5448/9177/Data_Protection_Law_DIFC_Law_No._1_of_2007.pdf

Geography	Mapping Column Header	Source	Authoritative Source - Statutory / Regulatory / Contractual / Industry Framework	Version	URL - Authoritative Source
EMEA	EMEA UK CAF v3-1	United Kingdom	Cyber Assessment Framework	3.1	https://www.ncsc.gov.uk/files/Cyber-Assessment-Framework-v3-1.pdf
EMEA	EMEA UK CAP 1850	United Kingdom	Cyber Assessment Framework (CAF) for Aviation Guidance (CAP1850)	N/A	https://publicapps.caa.co.uk/modalapplication.aspx?appid=11&mode=detail&id=9295
EMEA	EMEA UK Cyber Essentials	United Kingdom	Cyber Essentials	N/A	https://www.cyberessentials.ncsc.gov.uk
EMEA	EMEA UK DPA	United Kingdom	Data Protection Act	N/A	http://www.legislation.gov.uk/ukpga/1998/29/contents
EMEA	EMEA UK GDPR	United Kingdom	UK General Data Protection Regulation	N/A	https://www.legislation.gov.uk/eur/2016/679/data.pdf
APAC	APAC Australia Essential 8 ML 1	Australia	Australia Essential Eight	N/A	https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
APAC	APAC Australia Essential 8 ML 2	Australia	Australia Essential Eight	N/A	https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
APAC	APAC Australia Essential 8 ML 3	Australia	Australia Essential Eight	N/A	https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
APAC	APAC Australia Privacy Act	Australia	Privacy Act of 1998	N/A	https://www.comlaw.gov.au/Details/C2015C00089
APAC	APAC Australia ISM 2022	Australia	Australian Government Information Security Manual (ISM)	September 2022	https://www.cyber.gov.au/acsc/view-all-content/ism
APAC	APAC Australia IoT Code of Practice	Australia	Australia - Code of Practice - Securing the Internet of Things for Consumers	N/A	https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf
APAC	APAC Australia Prudential Standard CPS230	Australia	Prudential Standard CPS 230 - Operational Risk Management	N/A	https://www.apra.gov.au/sites/default/files/2023-07/Prudential%20Standard%20CPS%20230%20Operational%20Risk%20Management%20-%20Clean.pdf
APAC	APAC Australia Prudential Standard CPS 234	Australia	Prudential Standard CPS 234 Information Security	N/A	https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf
APAC	APAC Australia Privacy Principles	Australia	Australia Privacy Principles	N/A	https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf
APAC	APAC China DNSIP	China	Decision on Strengthening Network Information Protection	N/A	http://translate.google.com/translate?hl=en&sl=zh-CN&u=http://www.gov.cn/jrzq/2012-12/28/content_2301231.htm&prev=search
APAC	APAC Hong Kong	Hong Kong	Personal Data Ordinance	N/A	http://www.blis.gov.hk/blis_pdf.nsf/CurAllEngDoc/B4DF8B4125C4214D482575EF000ECSFF/\$FILE/CAP_486_e_b5.pdf
APAC	APAC India ITR	India	Information Technology Rules (Privacy Rules)	N/A	http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf
APAC	APAC Indonesia	Indonesia	Government Regulation No. 82 of 2012	N/A	http://uk.practicallaw.com/4-583-2387
APAC	APAC Japan APPI	Japan	Act on the Protection of Personal Information	June 2020	https://www.ppc.go.jp/files/pdf/APPI_english.pdf
APAC	APAC Japan ISMAP	Japan	Japan Information System Security Management and Assessment Program (ISMAP)	N/A	https://www.ismap.go.jp/csm/en?id=kb_article_view&sysparm_article=K80010301&sys_kb_id=4d06b8701b4f011013a78665cc4bcdb2&spa=1
APAC	APAC Malaysia	Malaysia	Personal Data Protection Act of 2010	N/A	http://www.kkmm.gov.my/pdf/Personal%20Data%20Protection%20Act%202010.pdf
APAC	APAC New Zealand Health ISF	New Zealand	NZ Health Information Security Framework	N/A	https://www.health.govt.nz/system/files/documents/publications/health-information-security-framework-dec2015.pdf
APAC	APAC New Zealand NZISM 3.6	New Zealand	New Zealand Information Security Manual (NZISM)	3.6	https://www.nzism.gcsb.govt.nz/ism-document/
APAC	APAC New Zealand Privacy Act of 2020	New Zealand	Privacy Act of 2020	2020	https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html
APAC	APAC Philippines	Philippines	Data Privacy Act of 2012	N/A	https://privacy.gov.ph/implementing-rules-and-regulations-of-republic-act-no-10173-known-as-the-data-privacy-act-of-2012/
APAC	APAC Singapore	Singapore	Personal Data Protection Act of 2012	N/A	http://statutes.agc.gov.sg/aol/download/0/0/pdf/binaryFile/pdfFile.pdf?Compld:2f46a4ee-0962-49e4-8e8d-eac45eff42b2
APAC	APAC Singapore Cyber Hygiene Practice	Singapore	Cyber Hygiene Practice	N/A	https://www.mas.gov.sg/-/media/MAS/Notices/PDF/MAS-Notice-132.pdf
APAC	APAC Singapore MAS TRM 2021	Singapore	Monitory Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines	2021	https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf
APAC	APAC South Korea	South Korea	Personal Information Protection Act	N/A	http://koreanlii.or.kr/w/images/0/0e/KoreanDPAAct2011.pdf
APAC	APAC Taiwan	Taiwan	Personal Data Protection Act	N/A	http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021
Americas	Americas Argentina	Argentina	Protection of Personal Law No. 25,326	N/A	http://www.infoleg.gov.ar/infoleginternet/anexos/60000-64999/64790/norma.htm
Americas	Americas Argentina Reg 152/2018	Argentina	Protection of Personal Data - MEN-2018-147-APN-PTE	N/A	https://www.argentina.gob.ar/sites/default/files/mensaie_ndeg_147-2018_datos_personales.pdf

Authoritative Sources

Geography	Mapping Column Header	Source	Authoritative Source - Statutory / Regulatory / Contractual / Industry Framework	Version	URL - Authoritative Source
Americas	Americas Bahamas	Bahamas	Data Protection Act	N/A	http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0003/DataProtectionPrivacyofPersonalInformationAct_1.pdf
Americas	Americas Bermuda BMA CCC	Bermuda	Bermuda Monetary Authority Cyber Code of Conduct	N/A	https://www.bma.bm/viewPDF/documents/2020-10-06-09-27-29-Insurance-Sector-Cyber-Risk-Management-Code-of-Conduct.pdf
Americas	Americas Brazil	Brazil	General Data Protection Law (LGPD)	N/A	https://www.onm.adb.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf
Americas	Americas Canada CSAG	Canada	Office of the Superintendent of Financial Institutions Canada (OSFI) - Cyber Security Self-Assessment Guidance	N/A	https://www.osfi-bsif.gc.ca/Eng/Docs/cbrsk.pdf
Americas	Americas Canada OSH B-13	Canada	B-13	N/A	https://www.osfi-bsif.gc.ca/Eng/If/rr-ro/pdn-ort/pl-lt/Pages/b13-jul-let.aspx
Americas	Americas Canada PIPEDA	Canada	Personal Information Protection and Electronic Documents Act (PIPEDA)	N/A	http://laws-lois.justice.gc.ca/eng/acts/p-8.6/FullText.html
Americas	Americas Chile	Chile	Act 19628 - Protection of Personal Data	N/A	http://www.leychile.cl/Navegar?idNorma=141599
Americas	Americas Colombia	Colombia	Law 1581 of 2012	N/A	http://www.secretariassenado.gov.co/senado/basedoc/ley_1581_2012.html
Americas	Americas Costa Rica	Costa Rica	Protection of the Person in the Processing of His Personal Data	N/A	http://web.ita.doc.gov/ITI/itiHome.nsf/9b2cb14bda00318585256cc40068ca69/11024d15acfa22185257a78004adfdb/\$FILE/Costa%20Rica%20Data%20Protection%20Legislation%20Draft%20June%202011_EN%20translation%20by%20ITA.pdf
Americas	Americas Mexico	Mexico	Federal Law on Protection of Personal Data held by Private Parties	N/A	https://privacyassociation.org/media/pdf/knowledge_center/Mexico_Federal_Data_Protection_Act_July2010.pdf
Americas	Americas Peru	Peru	Personal Data Protection Law	N/A	https://www.huntonprivacblog.com/wp-content/uploads/sites/18/migrated/Peru%20Data%20Protection%20Law%20July%2028_EN%20_2.pdf
Americas	Americas Uruguay	Uruguay	Law No. 18,331 - Protection of Personal Data and Actio Habeas	N/A	https://legislativo.parlamento.gub.uy/temporales/leytemp3273105.htm

EXAMPLE

Policy ID	Policy Title	Policy Content	Program Area	Strategic Intent	Business Case	Stakeholders	Key Objectives	Enabling Context	Key Enabler	Key Performance Indicator (KPI)	Key Performance Indicator (KPI) Definition	Key Performance Indicator (KPI) Metric	Key Performance Indicator (KPI) Weight	Key Performance Indicator (KPI) Unit	Key Performance Indicator (KPI) Frequency	Key Performance Indicator (KPI) Target	Key Performance Indicator (KPI) Status	Key Performance Indicator (KPI) Risk	Key Performance Indicator (KPI) Status	Key Performance Indicator (KPI) Risk	Key Performance Indicator (KPI) Status	Key Performance Indicator (KPI) Risk	Key Performance Indicator (KPI) Status	Key Performance Indicator (KPI) Risk
CSP-001	Information Security Policy	The Information Security Policy (ISP) defines the organization's approach to the protection of information. It outlines the principles and objectives for the protection of information and provides a framework for the implementation of information security measures. The ISP is a key document for the organization and provides a clear and concise statement of the organization's information security goals and objectives. It is the foundation upon which all other information security policies and procedures are based.	Information Security	Protect and preserve the confidentiality, integrity, and availability of information. The ISP is a key document for the organization and provides a clear and concise statement of the organization's information security goals and objectives. It is the foundation upon which all other information security policies and procedures are based.	Confidentiality, Integrity, Availability	Information Security	Protect and preserve the confidentiality, integrity, and availability of information. The ISP is a key document for the organization and provides a clear and concise statement of the organization's information security goals and objectives. It is the foundation upon which all other information security policies and procedures are based.	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security
CSP-002	Acceptable Use Policy	The Acceptable Use Policy (AUP) defines the acceptable use of the organization's information technology resources. It outlines the rules and regulations that govern the use of information technology resources and provides a framework for the implementation of acceptable use measures. The AUP is a key document for the organization and provides a clear and concise statement of the organization's acceptable use goals and objectives. It is the foundation upon which all other acceptable use policies and procedures are based.	Information Security	Ensure that information technology resources are used in a responsible and secure manner. The AUP is a key document for the organization and provides a clear and concise statement of the organization's acceptable use goals and objectives. It is the foundation upon which all other acceptable use policies and procedures are based.	Confidentiality, Integrity, Availability	Information Security	Ensure that information technology resources are used in a responsible and secure manner. The AUP is a key document for the organization and provides a clear and concise statement of the organization's acceptable use goals and objectives. It is the foundation upon which all other acceptable use policies and procedures are based.	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security
CSP-003	Security Incident Response Policy	The Security Incident Response Policy (SIRP) defines the organization's approach to the detection, response, and recovery from security incidents. It outlines the procedures and processes for the detection, response, and recovery from security incidents and provides a framework for the implementation of security incident response measures. The SIRP is a key document for the organization and provides a clear and concise statement of the organization's security incident response goals and objectives. It is the foundation upon which all other security incident response policies and procedures are based.	Information Security	Detect, respond to, and recover from security incidents. The SIRP is a key document for the organization and provides a clear and concise statement of the organization's security incident response goals and objectives. It is the foundation upon which all other security incident response policies and procedures are based.	Confidentiality, Integrity, Availability	Information Security	Detect, respond to, and recover from security incidents. The SIRP is a key document for the organization and provides a clear and concise statement of the organization's security incident response goals and objectives. It is the foundation upon which all other security incident response policies and procedures are based.	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security
CSP-004	Business Continuity Policy	The Business Continuity Policy (BCP) defines the organization's approach to the maintenance and recovery of critical business operations in the event of a disaster. It outlines the procedures and processes for the maintenance and recovery of critical business operations and provides a framework for the implementation of business continuity measures. The BCP is a key document for the organization and provides a clear and concise statement of the organization's business continuity goals and objectives. It is the foundation upon which all other business continuity policies and procedures are based.	Information Security	Ensure the continuity of critical business operations in the event of a disaster. The BCP is a key document for the organization and provides a clear and concise statement of the organization's business continuity goals and objectives. It is the foundation upon which all other business continuity policies and procedures are based.	Confidentiality, Integrity, Availability	Information Security	Ensure the continuity of critical business operations in the event of a disaster. The BCP is a key document for the organization and provides a clear and concise statement of the organization's business continuity goals and objectives. It is the foundation upon which all other business continuity policies and procedures are based.	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security
CSP-005	Information Security Governance Policy	The Information Security Governance Policy (ISGP) defines the organization's approach to the management of information security. It outlines the procedures and processes for the management of information security and provides a framework for the implementation of information security governance measures. The ISGP is a key document for the organization and provides a clear and concise statement of the organization's information security governance goals and objectives. It is the foundation upon which all other information security governance policies and procedures are based.	Information Security	Manage information security in a consistent and effective manner. The ISGP is a key document for the organization and provides a clear and concise statement of the organization's information security governance goals and objectives. It is the foundation upon which all other information security governance policies and procedures are based.	Confidentiality, Integrity, Availability	Information Security	Manage information security in a consistent and effective manner. The ISGP is a key document for the organization and provides a clear and concise statement of the organization's information security governance goals and objectives. It is the foundation upon which all other information security governance policies and procedures are based.	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security	Information Security



SCF Domain	CMRM KPI #	Key Performance Index (KPI) Name	%	Description	Method of Calculation	Key Risk Indicator (KRI)	Key Performance Indicator (KPI)	Domain	Domain Rollup	Analytics Weighting	Domain Score	Weighted Analytics Score	NIST CSF Function	Function Score	Function Rollup	Domain Weighting	Weighted Domain Score
Asset Management	AST-A-01	Unknown Devices	5.7%	% of unknown devices on the network	AST-M-087 divided by (AST-M-001 + AST-M-087)	KRI		Asset Management	100%	30%	80.7	28.30	IDENTIFY	63.0	100%	20%	16.1
Asset Management	AST-A-02	Known Server Functions	73.0%	% server-class systems with a documentation function/purpose	AST-M-088 divided by AST-M-001	KRI				20%		14.60					
Asset Management	AST-A-03	Servers with Assigned Owners	75.6%	% server-class systems with an assigned system owner/custodian	AST-M-089 divided by AST-M-002	KRI				10%		7.56					
Asset Management	AST-A-04	Workstations with Assigned Owners	88.0%	% workstation-class systems with an assigned system owner	AST-M-090 divided by AST-M-012					5%		4.40					
Asset Management	AST-A-05	Network Devices with Assigned Owners	91.4%	% network devices with an assigned system owner/custodian	AST-M-091 divided by AST-M-017					5%		4.57					
Asset Management	AST-A-06	Databases with Assigned Owners	83.0%	% databases with an assigned system owner/custodian	AST-M-092 divided by AST-M-027	KRI				5%		4.15					
Asset Management	AST-A-07	Major Applications with Assigned Owners	88.9%	% major applications with an assigned system owner/custodian	AST-M-093 divided by AST-M-037	KRI				5%		4.44					
Asset Management	AST-A-08	Minor Applications with Assigned Owners	64.0%	% minor applications with an assigned system owner/custodian	AST-M-094 divided by AST-M-047					5%		3.20					
Asset Management	AST-A-09	Cloud-Based Applications with Assigned Owners	86.6%	% cloud-based applications with an assigned system owner/custodian	AST-M-095 divided by AST-M-057	KRI				5%		4.33					
Asset Management	AST-A-10	IoT/OT with Assigned Owners	74.2%	% embedded technology-class systems with an assigned system owner/custodian	AST-M-096 divided by AST-M-067					5%		3.71					
Asset Management	AST-A-11	Facility Infrastructure Devices with Assigned Owners	29.5%	% facility infrastructure-class systems with an assigned system owner/custodian	AST-M-097 divided by AST-M-072					5%		1.47					
Asset Management	AST-A-12	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined					0%		0.00					
Asset Management	AST-A-13	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined					0%		0.00					
Asset Management	AST-A-14	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined					0%		0.00					
Business Continuity & Disaster Recovery	BCD-A-01	Line of Business (LOB) with a Business Impact Analysis (BIA)	33.3%	% lines of business with a Business Impact Analysis (BIA)	BCM-M-002 divided by BCM-M-001	KRI		Business Continuity & Disaster Recovery	100%	25%	31.0	8.33	IDENTIFY	63.0	100%	15%	4.7
Business Continuity & Disaster Recovery	BCD-A-02	Line of Business (LOB) with a Business Continuity Plan (BCP)	43.8%	% lines of business with a Business Continuity Plan (BCP)	BCM-M-004 divided by BCM-M-001	KRI				50%		21.88					
Business Continuity & Disaster Recovery	BCD-A-03	Incidents Related To Lack of Capacity or Denial of Service (DoS) attacks	3.4%	% incidents related to capacity issues or Denial of Service (DoS) attacks	CAP-M-001 divided by IRO-M-003		KPI			25%		0.84					
Business Continuity & Disaster Recovery	BCD-A-04	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined					0%		0.00					
Business Continuity & Disaster Recovery	BCD-A-05	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined					0%		0.00					
Business Continuity & Disaster Recovery	BCD-A-06	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined					0%		0.00					
Compliance	CPL-A-01	Security Events Impacting Compliance Efforts	14.2%	% security events with applicable statutory, regulatory and contractual compliance implications	CPL-M-002 divided by IRO-M-003			Compliance	100%	100%	85.8	85.82	IDENTIFY	63.0	100%	10%	8.6
Compliance	CPL-A-02	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined					0%		0.00					
Compliance	CPL-A-03	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined					0%		0.00					
Compliance	CPL-A-04	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined					0%		0.00					
Network Security	NET-A-01	Line of Business (LOB) with a Network Diagram	72.9%	% lines of business with network diagrams	NET-M-008 divided by BCD-M-001	KRI		Network Security	100%	40%	62.9	29.17	IDENTIFY	63.0	100%	15%	9.4
Network Security	NET-A-02	Line of Business (LOB) with a Data Flow Diagram (DFD)	56.3%	% lines of business with Data Flow Diagrams (DFD)	NET-M-009 divided by BCD-M-001	KRI				60%		33.75					
Network Security	NET-A-03	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined					0%		0.00					
Network Security	NET-A-04	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined					0%		0.00					
Network Security	NET-A-05	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined					0%		0.00					
Risk Management	RSK-A-01	Production Migrations With Exceptions to Standards	72.7%	% projects transition into production with exceptions to standards	RSK-M-003 divided by PRM-M-004			Risk Management	100%	25%	67.2	18.18	IDENTIFY	63.0	100%	20%	13.4
Risk Management	RSK-A-02	Risk Assessments Exceeding Risk Tolerance	61.6%	% risk assessments that exceed risk tolerance thresholds	RSK-M-004 divided by RSK-M-002		KPI			25%		15.40					
Risk Management	RSK-A-03	Risk Register Findings older than 90 days	91.9%	% findings on the risk register older than 90 days	RSK-M-005 divided by RSK-M-001		KPI			10%		9.19					
Risk Management	RSK-A-04	Risk Register Findings older than 180 days	68.1%	% findings on the risk register older than 180 days	RSK-M-006 divided by RSK-M-001		KPI			20%		13.62					
Risk Management	RSK-A-05	Risk Register Findings older than 365 days	54.2%	% findings on the risk register older than 365 days	RSK-M-007 divided by RSK-M-001		KPI			20%		10.84					
Risk Management	RSK-A-06	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined					0%		0.00					
Risk Management	RSK-A-07	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined					0%		0.00					
Risk Management	RSK-A-08	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined					0%		0.00					
Third-Party Management	TPM-A-01	Third-Party Risk Assessments Performed	28.1%	% third party risk assessments performed to address cybersecurity-related supply chain risk	TPM-M-001 divided by RSK-M-002			Third-Party Management	100%	30%	53.5	8.43	IDENTIFY	63.0	100%	20%	10.7
Third-Party Management	TPM-A-02	Critical Systems, Applications & Services Provided By Third-Parties	10.1%	% critical systems, processes and services provided by third parties	(AST-M-058 + AST-M-059 + AST-M-078 + AST-M-079) divided by (AST-M-003 + AST-M-004 + AST-M-013 + AST-M-014 + AST-M-018 + AST-M-019 + AST-M-023 + AST-M-024 + AST-M-028 + AST-M-029 + AST-M-038 + AST-M-039 + AST-M-048 + AST-M-049 + AST-M-058 + AST-M-059 + AST-M-068 + AST-M-069 + AST-M-073 + AST-M-074 + AST-M-078 + AST-M-079)					50%		44.95					
Third-Party Management	TPM-A-03	Critical Systems, Applications & Services Provided With SBOM	0.7%	% critical systems, processes and services with a Software Bill of Materials (SBOM)	TPM-M-007 divided by (AST-M-003 + AST-M-004 + AST-M-014 + AST-M-018 + AST-M-019 + AST-M-023 + AST-M-024 + AST-M-028 + AST-M-029 + AST-M-038 + AST-M-039 + AST-M-048 + AST-M-049 + AST-M-058 + AST-M-059 + AST-M-068 + AST-M-069 + AST-M-073 + AST-M-074 + AST-M-078 + AST-M-079)					20%		0.14					
Third-Party Management	TPM-A-04	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined					0%		0.00					
Third-Party Management	TPM-A-05	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined					0%		0.00					
Third-Party Management	TPM-A-06	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined					0%		0.00					

