Digital Security Program Domains

#	DSP Domain	Domain Identifier	Cybersecurity & Data Privacy by Design (CLP) 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 class, ication methodology to objectively determine the sensitivity and criticality of all data and technology assets so that proper bandling and disposal requirements can be
13	Embedded Technology	EMB	Provide additional scrutiny to record the risks associated with embedded technology, based on the
14	Endpoint Security	END	Harden endpoint devices o protect against reasonable threats to those devices and the data those
15	Human Resources Security	HRS	devices store, trace sands occesso Execute sound uring policices of ongoing personnel management to cultivate a cybersecurity & data
16	Identification & Authentication	IAC	Enforce to proce, if "least privilege" consistently across all systems, applications and services for individual, trop and service accounts through a documented and standardized Identity and Access Management (IA-M capability
17	Incident Response	IRO	contain a value incident response capability that trains personnel on how to recognize and report susticious differentiation of the second second incidency in accordance with a documented Incident Response Plan (IRP).
18	Information Assurance	IAO	vecute impartial assessment process to validate the existence and functionality of appropriate
19	Maintenance	мт	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	MD 1	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 (SSDE) 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
32	Vulnerability & Patch Management	VPM	Leverage industry-recognized Attack Surface Management (ASM) practices to strengthen the security and resiling on systems, applications and explicit against avoiding and explicit lated attack waters
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/assuranceadvisoryservices/aicpasoc2report.html							
Universal	BSI Standard 200-1	BSI	Standard 200-1	2022	https://www.bs.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und- Zertifizierung/TT-Grundschutz/BSI-Standards/BSI-Standard-200-1-Managementsysteme-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	СОВІТ 2019	ISACA	Control Objectives for Information and Related Technologies (COBIT)	2019	http://www.isaca.ors/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)	ν4	https://cloudsecurityalliance.org/proup/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)		bings//www.kscpa.org/writable/files/AICPADocuments/10- 9 alcpa 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	150 22301 v2019	ISO	22301 - Security and resilience — Business continuity management systems — Rev. Tema.	2019	https://www.iso.org/standard/75106.html							
Universal	150 27001 v2013	ISO	27001 - Information Security Management Systems (ISMS) - Requirements	2013	https://www.iso.org/standard/54534.html							
Universal	150 27001 v2022	ISO	27001 - Information Security Management Systems . v.,	2022	https://www.iso.org/standard/27001							
Universal	150 27002 v2013	ISO	27002 - Code of Practice for Information : urity Control	2013	https://www.iso.org/standard/54533.html							
Universal	150 27002 v2022	ISO	27002 - Information security cybersecurity Information security controls	2022	https://www.iso.org/standard/75652.html							
Universal	150 27017 v2015	ISO	27017 - Information - Thrology - Security tec - Ques — Code of practice for information security controls based on ISO/IEC 27000 - cp - d services	2015	https://www.iso.org/standard/43757.html							
Universal	150 27018 v2014	ISO	27018 - Code of Practice for Plue Unit Clouds Acting as Pl Processors	2014	https://www.iso.org/standard/61498.html							
Universal	150 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	150 29100 v2011	ISO	29100 - Privacy Framework	2011	https://www.iso.org/standard/45123.html							
Universal	150 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	МРА	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	NIAC 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://mvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf							

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://m/pubs.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/finaj
Universal	NIST 800-53 rev5 [law]	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 [moerate]	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	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		https://nvipubs.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/fina
Universal	NIST 800-161 rev 1	NIST	NIST SP 800-161 - Cybersecurity Supply Chain Risk Management Practices for Syst. Is and Conjugations	rev 1	https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final
Universal	NIST 800-161 rev 1 C-SCRM Baseline	NIST	NIST SP 800-161 - Cybersecurity Supply Chain Risk Management Process for System 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 N. Lagemen. Strices for Syntems 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 C n Risk Manage ent 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 - Cybroscurity Supply Charolist Manuscrment 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 - Cyb	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 Noederal 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://mvlpubs.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	JA	https://industries.ul.com/cybersecurity/ul-2900-standards-process
Universal	UN R155	United Nations	UN Regulation No. 155 - Cyber security and cyber security management system	N/A	http://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security- active-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 (CJI - tec 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 (c MC)	1.02	https://www.acq.osd.mil/cmmc/index.html
US	US CMMC 2.0 Level 2	Federal	Cybersecurity Maturity Model Certification (Cry 5)	1.02	https://www.acq.osd.mil/cmmc/index.html
US	US CMMC 2.0 Level 3	Federal	Cybersecurity Maturity I, Vel Comparison (CMM	1.02	https://www.acq.osd.mil/cmmc/index.html
US	US CMMC 2.1 (draft) Level 1	Federal	Cybersecurity Maturity Model Certic (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 CMS 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-Q- 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?reg=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.acq.osd.mii/dpap/dars/dfars/htmi/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 RS	Federal	Federal Risk and Authorization Management Program (FedRAMP) RS	R5	https://www.fedramp.gov/
US	US FedRAMP RS (low)	Federal	Federal Risk and Authorization Management Program (FedRAMP R5) (low baseline)	R5	https://www.fedramp.gov/
US	US FedRAMP RS (moderate)	Federal	Federal Risk and Authorization Management Program (FedRAMP R5) (moderate baseline)	R5	https://www.fedramp.gov/
US	US FedRAMP RS (high)	Federal	Federal Risk and Authorization Management Program (FedRAMP RS) (high baseline)	R5	https://www.fedramp.gov/
US	US FedRAMP R5 (LI-SaaS)	Federal	Federal Risk and Authorization Management Program (FedRAM RSP) (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-subchapIII- part4-sec1232g.pdf
US	US FFIEC	Federal	Federal Financial Institutions Examination Council (FFIEC)	N/A	https://www.fflec.gov/pdf/cybersecurity/FFIEC_CAT_App_B_Map_to_NIST_CSF_June_2015_PDF4.p df
US	US FINRA	Federal	Financial Industry Regulatory Authority (FINRA)	JA	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 Billey 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 Pract	N/A	https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx
US	HIPAA - HICP Medium Practice	Federal	Health Industry Cybersecurity Practices (HICP) dium Practice	N/A	https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx
US	HIPAA - HICP Large Practice	Federal	Health Industry Cybersecurity Practic (HICP) - Lan Practic	N/A	https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx
US	US IRS 1075	Federal	Internal Revenue Service on	N/A	https://www.irs.gov/pub/irs-pdf/p1075.pdf
US	ITAR Part 120 [limited]	Federal	International Testic in Arms Regulation (1 - 3) [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 Tability poration 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.pd
US	US NNPI (unclass)	Federal	Naval Nuclear Propulsion Information (NNPI)	N/A	https://www.secnav.navy.mii/doni/Directives/09000%20General%20Ship%20Design%20and%20Sup port/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 EIESR 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/department/civil/consumer/4548.html
US	US - CA SB327	State	CA - 58327	N/A	https://leginfo.legisiature.ca.gov/faces/billTextClient.xhtml?bill_id=20172018058327

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://cppa.ca.gov/regulations/pdf/20221102_mod_text.pdf
US	US - CA SB1386	State	CA - \$81386	N/A	https://leginfo.legislature.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.iiga.gov/legislation/lics/lics3.asp?ActID=3004&ChapterID=57
US	US - IL IPA	State	Illinois identity Protection Act (IPA)	N/A	https://www.iiga.gov/legislation/lics/lics3.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/idtheft/201cmr1700reg.pdf
US	US - NV SB220	State	NV - 58220	N/A	https://www.leg.state.nv.us/App/NELIS/REL/80th2019/Bill/6365/Tex
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 SS575B	State	NY - SHIELD Act (SB 55575B)	N/A	https://legislation.nysenate.gov/pdf/bilis/2019/s5575b
US	US - OR 646A	State	OR - OR5 646A	N/z.	ntos://www.oregonlegislature.gov/bills_laws/ors/ors646a.html
US	US - SC Insurance Data Security Act	State	SC - South Carolina Insurance Data Security Act		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/tłodocs/85R/billtext/pdf/H800008F.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-RAIN	N/A	http://dir.texas.gov/texas-risk-and-authorization-management-program-tx-ramp
US	US-TX SB820	State	TX - 2019 - 58820	N/A	https://www.legiscan.com/TX/text/58820/id/2027614/Texas-2019-58820-Enrolled.html
US	US-VA CDPA 2023	State	Virginia Consumer Date of ection Act	2023	https://lis.virginia.gov/cgi-bin/legp504.exe?212+ful+CHAP0035+pdf
US	US-VT Act 171 of 2018	State	VT - Act 171 of 2018 (b	N/A	https://legislature.vermont.gov/Documents/2018/Docs/ACTS/ACT171/ACT171%20As%20Enacted.p df
EMEA	EMEA EU EBA GL/2019/04	EU	European Banking Authority (EBA) Juidelines 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 ePrivacy [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/Erv/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.datatikynet.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.cnil.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_bdsp/englisch_bdsp.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;jse ssionid=CDFE3798FF98313981E73C57CD17B025.1_cid389?nn=9866146							
EMEA	EMEA Germany CS:2020	Germany	Cloud Computing Compliance Controls Catalogue (CS)	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%2 02472-97-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/BiobFolder/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/privacy.code-en.html							
EMEA	EMEA Kenya DPA 2019	Kenya	Kenya Data Protection Act	2019	http://kenvalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct_No24of2019.p df							
EMEA	EMEA Luxembourg	Luxembourg	Protection of Personals with Regard to the Processing of Personal Data	N	http://www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi02082002_en.pdf							
EMEA	EMEA Netherlands	Netherlands	Personal Data Protection Act	N/A	as://www.akd.nl/t/Documents/17-03-2016_ENG_Wet-bescherming-persoonsgegevens.pdf							
EMEA	EMEA Nigeria DPR 2019	Nigeria	Nigeria Data Protection Regulation		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-regulations2/							
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/i/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 PDPPL	Qatar	Personal Data Privacy Protection Law (PDPPL)	N/A	https://compliance.corti.org/sites/default/files/library/2020- 11/Law/s20No.%20Ns2813%29%200f%202016%20%200n%20Protecting%20Personal%20Data%20P r/uscy%20-%20English.pdf							
EMEA	EMEA Russia	Russia	Federal Law of 27 July 2006 N 152-F2	N/A	http://www.rg.ru/2006/07/29/personalinye-dannye-dok.html							
EMEA	EMEA Saudi Arabia Critical Security Controls	Saudi Arabia	Saudi Arabian Monetary Argority - Cyber Security - mework	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 Cybersect Standard	N/A	https://www.aramco.com/-/media/downloads/working-with-us/ccc/sacs-002-third-party- cybersecurity-standard.pdf							
EMEA	EMEA Saudi Arabia SAMA CSFv1.0	Saudi Arabia	Saudi Arabian Monetary Autholity (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	Servia	Act of 9 November 2018 on Personal Data Protection (Official Gazette No. 87/18)	N/A	http://www.ilo.org/dvn/natiex/natiex4.detail?p_lange=n8p_isn=109270&p_count=55&p_classificati jon=11#::ttest=Regulates%20the%20right%20to%20protection_penalties%2C%20special%20cases%2 C%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/es/AreaTematica/DocumentacionPublicaciones/Documents/Royal_D ecree_approving the regulations relating to Constitucional Act on Personal Data Protection % 28.PDF							
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-gula-esquema-nacional-de-seguridad/2148-ccn-stic- 825-ens-national-security-framework-27001-certifications/file.html							
EMEA	EMEA Sweden	Sweden	Personal Data Act	N/A	http://www.datainspektionen.se/in-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_No1_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)	ember 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	A	tps://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/Prudentia%20Standard%20CP5%20230%20Operational%20Risk%20Management%20- %20clean.pdf_
АРАС	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
АРАС	APAC China DNSIP	China	Decision on Strengthening Network Information Protection	N/A	http://translate.google.com/translate?hi=en&si=zh-CN&u=http://www.gov.cn/irzg/2012- 12/28/content_2301231.htm&prev=search
APAC	APAC Hong Kong	Hong Kong	Personal Data Ordinance	N/A	http://www.bis.gov.hk/bils_pdf.nsf/CurAllEngDoc/B4DF8B4125C4214D482575EF000ECSFF/SFILE/C AP_486_e_b5.pdf
APAC	APAC India ITR	India	Information Technology Rules (Privacy 125)	N/A	http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf
АРАС	APAC Indonesia	Indonesia	Government Regulation No. 82 of 202	N/A	http://uk.practicailaw.com/4-583-2387
APAC	APAC Japan APPI	Japan	Act on the Protect of Person Informatio	June 2020	https://www.ppc.go.jp/files/pdf/APPI_english.pdf
APAC	APAC Japan ISMAP	Japan	Japan Information System Suchty of nagement and Assessment Program (ISMAP)	N/A	https://www.ismap.go.jp/csm/en?id=kb_article_view&sysparm_article=KB0010301&sys_kb_id=440 6b8701b4f011013a78665cc4bcbd2&spa=1
APAC	APAC Malaysia	Malaysia	Personal Data Protection Act of 2010	N/A	http://www.kkmm.gov.mv/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://orivacy.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?Compid:2f46a4ee-0962_ 49e4-8e8d-eac45eff42b2
АРАС	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
АРАС	APAC South Korea	South Korea	Personal Information Protection Act	N/A	http://koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf
АРАС	APAC Taiwan	Taiwan	Personal Data Protection Act	N/A	http://law.moj.gov.tw/Eng/LawClass/LawAlLaspx?PCode=10050021
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 132/2018	Argentina	Protection of Personal Data - MEN-2018-147-APN-PTE	N/A	https://www.argentina.gob.ar/sites/default/files/mensaje_ndeg_147-2018_datos_personales.pdf

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.pnm.adv.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 OSFI B-13	Canada	B-13	N/A	https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-id/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	http://www.secretariasenado.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.lta.doc.gov/11/titHome.nsf/9b2cb14bda0031858525cc40068ca69/11024d15acfca221 85257a78004adfdb/SfLLfCosta%20Rta%20Data%20Protection%20Leeslation%20Draft%20Protection%20Leeslation%20Draft%20Protection%20Leeslation%20Draft%20Protection%20Leeslation%20Draft%20Protection%20Leeslation%20Draft%20Protection%20Leeslation%20Draft%20Protection%20Leeslation%20Draft%20Protection%20Leeslation%20Draft%20Protection%20Leeslation%20Draft%20Protection%20Leeslation%20Draft%20Protection%20Leeslation%20Draft%20Protection%20Leeslation%20Draft%20Protection%20Leeslation%20Draft%20Protection%20Leeslation%20Draft%20Protection%20Leeslation%
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 iui/2010.pdf
Americas	Americas Peru	Peru	Personal Data Protection Law	N/A	https://www.huntonprivacyblog.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 Active Tabeas	N/A	https://legislativo.parlamento.gub.uy/temporales/leytemp3273105.htm

Pulling IF Pulling To	p Pulky Cardeni Palky Johns	Standard Standard 8 Tile	Candinal Disjustion	Nakalard Contant	Guidelines	Nigh-Gevel Target Audionia	DRP dones 6 Categorization BCP Done Applicability	in SCF Cardnel	101	Benari Cantola Fammanik (DCP) Cantol Benarphia	Abethods To Compily With LCP Controls	Reidence Requestitie (URL) #	a KY Gashad Question	Reliative Control Weighting Part	alian Erisaping Sa	CRM SCRM 1 Ser1 Ser2 1 ategic Operational T	cma le:3 ctical	NP-CMM 8 Nut Performed	3P CAMM 1 Performed Informally	SP-CMM3 Planne & Titched	3P CMM 3 Well Defined	ter cann á Quantititively Cantoláne	SP CSMM 5 Continuoudy Inspiroung
2 Cybersecurity Protection Gay	[Company/tame) shall The purpose of the implement and mantan a company based apality to reade or a statistical statistics of the ordinator of the behaviory inforcement and statistical statistics inforcement and statistics	e BEA Cybersecurity& Data Cybersecurity& Data Cybersecurity& Data Polaration Governance Polaration	The organization facilitates the implementation of cyberneountry & data privacy government controls.	[Company/Name]'s optensountly & data protection policies and databatic must be represented in a single-document, the Digital Security Property (DMP) State (p)(Must be interwell and updated at local binnually, and (b)(Documentable is the appropriate pathetics in moure all Company mounts)	The security plant for individual systems and the signalization wide DIP signifies provide complete coverage for all optensionity & data privacy related cantools employed within the organization.	Management	Broc Eyleriacum Protection Son	& Data Robertsourity & Data Protection Governance Program	609-05	Mechanisms exist to fastitute the implementation of spheroecurity & Bilds partnetise governance controls.	- Scening connotible - Digital Security Program (DSP) - Cybersecurity & DataProtection Program (CDPP)	8-629-65 8-629-62	Deer the organization facilitate the implementation of optendecurity & dataparatechne governance contract?	20	sawefy	x x	x	centence of a capability to facilitate the implementation of ing & data privacy governance controls.	Cybersecurby & Privacy Soversance (SCM) efforts are ad hoc and monoscient: CMMLevel 1 control enduring would reasonable expert3 or attract room; The following controls lowest: •Nonformatophersecurby and/or data privacy principles are identified the expensation.	Cybersourtly & Prinaly Sovenance (SDV) efforts are requirements all, drives and formally generated at alocal (regiment line), but are not consequent sources the organizations. CMM takes 1 count meansity works for meanably expectal, or at local must, the following comean to excit -typemounting and data prinally generation activities are descentiated	Operators in the standard set of the standard	Operatorship & Privag Governance (SDV) efforts are netroconver any provide orthoperatorsagement insign (paced or a quantizative enterstanding of process capatitizative) is period capation performance, encure continued aperators can identify areas for improvement, to addition to CMM Level 1 others, CMM Level 1 cannot networky would	See SF-CMIRE 3F-CMIRES (A)(A, since a continuously improved is not exclusion to facilitate the implementation of opersonality & data privacy governance controls:
2 Cybersecutity Protection Gov	(Company/Name) shall the purpose of the implementand mantan a Cybersourity & Do manny based cigability to vision of the security and observed, man and the security and observed, man and the security and observed, man and the security and observed man and security and observed	e Lika 1.a	The organization coordinates ophenocurrity, data priving and bosiness alignment through a sciencing committee in zelencoryboard, comprised of key ophenocurrity, data-privacy and autoince executives, which meets formally and or a regularibasis.	[Company/Name] mult establish a rybersacuity & data protection thereing committee, as advance basis complexited and the second state of the second of the tabletodote from (Company State) Lines of the second state technology-related executions that (pMeets Simondry and on a negative basis, and dimensional state from second states and	To achieve proper citizational answerence across the organization, key alternaturity & data private proders must faintable communication with business claim holders. This includes standating appendicuting, data	Management	Eshanced Cybertecum Protection Sor	&Data Steering Committee & Manue Program Dieright	979-011	Mochanisms exist to constraint ophenocumely, data provincies and buckness alignment through a converging simultance and anning back, manipartial of the yigher society, data prology and buckness executives, which meets formally and or a regular lasis.	- Screeing Lamatibee - Digital Security Program (DDP) - Cybersocurity & Data Probabilie Program (CDPP)	8-609-68	Desc the organization conclustor opherwoorty, attapartection and bosons alignment through a dreening sammer or advisory baseling, imported dreps phenocenty, data privacy and buciness executives, which nexts formally and on a regular factor?		samely	x x	There is non- privacy and b board, comp executives, s	cendence of a capability to coordinate ophenecumy, data a business alignment through a statesting connective or advisory spinor of of levy ophenecumy, data privacy and business c, which meets formally and on a regular basis.	Cybersecurby & Privacy Sovercance (ISCV) efforts are ad hoc and monosphere: CMM12evel 2 control industry woold reasonably superity or atteast even; the following control how exit: •thatformat cybersecurby and/ or data privacy principles are identified the expension.	Cyberseurtry & Prissoy Basemance (0074) efforts are requirements all, divers and formality generad at a locally legislant level, but are not concrete thoses the segmentation. CMM tevel to constrain marking would fill reasonably expectally, or at least must, the following otherta to exact explorison that prinsing generative activities are deservolated to an antipart of an atta prinsing generative activities are deservolated to an antipart formation of the second second second second second to an antipart of the second second second second second second to an antipart of the second second second second second second to an antipart of the second se	Cybersecurity & Privacy dowernance (EDV) efforts are standardiard across the apparation and constity enabled, where technically feasible, the energy accesses (CHBLeret Roteritarius) result reasonably expect all, or at load most, the following orders to exist. «A dowernance, Rola & Compliance (DRC) surplus, or similar feadow,	Cybersecurity & Privacy Governance (SDV) efficitizate metrics.drives any provide cultivated management magite (based on a spannttative understanding of process capabilities(1) a predict optimal performance, encore sambles dependions and skettify areas for improvement. In addition to CMM Level 3 othersa, CMM Level 6 cannot networky would	See 3P -CMBR 3P -CMRS I: R(A, Since a continuously improving process) is out increasing its countries of phonescuring, data phones, and digenment Through a treasing committee or advoory-board, comprised or by righer security, data phoney and business executives, which meets formatly and an a regular basis.
Cybersecurity Protection Gav	(Company/tame) shall The purpose of the implementant and maintain a DBL maturity-based capability to visues of the security and estimated at its technology relation of its technology	e MA 100 - CE J 	The organization provides governance overcight importing and incommendations to those enrulated make executive declassion block matters (anothered material to the organization's cyberceaumy & data privacy program.	[Company/Name]'s Chief Information Security O'Hian (CRS) must be (plopente a repeatable process for reporting to [Company Name]'s based of involver, or or main covering for functions (b)(Provide detailed reporting_along with recommendations, to the descript's lody; and	None	Management	Boot Protection Son	& Data Status Reporting To Governing Roday Body	N 0074-01.3	Mochanies east to provide generation envergine expansing and recommendation con these enversions for onder executive decreases, double numbers cancelered material to the segmentation's optension by & data protection program.		1-01-03 1-01-03 1-002-03 1-002-03 1-002-03	Does the organization privile generators on-organization-paring and misioneen-Albinos torbuse entroped is non-encoder document, and matters cancelered national torbe organization's opennessity. Adda patiention program?		sawefy	x x	There is non- reporting an decision als opheriocurity	cendence of a capability to provide governance overcight and recommendations to those industrial to make executive above matters condensed material to the organization's ring & data privacy program.	3P-CMMI ION(R, since a structured protect is required to provide governance oversight repairing and economestication to those entrusted to involve neurodive discoss: about matters is cancelered material to the organization's optensecurity & data privacy program.	Cybersourtly & Privaly Devendance (0211) of floris are requirements drives and formally generated at a local inguinal meet, but are not considerations the organization. CMM tenet 2 count manufers would reasonably expectall, or at local must, the following othera to exact -Cybersourtly and data privaly generation addrets are discretizated	Operators of the opportunity the endower (SDV) efforts are standard and across the opportunity opportunity reacting 4, where technically feasible, the endower describers, Contribution for works of reasonably expect all, or at least most, the following orders take wrist. A describance, Rok & Compliance (SRC) Switchs, or circuits function,	See 3P CMRIX 3P CMMR IX (A, since a quantitatively-solution of process is not receively to provide geownance averying! reporting and recommendations in those environment of a reale exercise discussion natively considered material to the arganization's optenseumly & data physic gaugese.	See 3P -CMBR 3P -CMBT is IQA, since a continuously improving process is not increasing to possible governance averaged reparting and encommendations to those environment of since exercisive decisions de nothers considered material to the arganization's operacurity & data private program.
2 Cybersecutity Protection Gov	(Campary/Kamp) skall The purpose of the implement and maintain a Cyberiocurity & Dis mainty-based capability to visions diseased by and the second participation (SOV) readlessor of its technology indications and state should be applied as a second indication of the second participation of the second participation of the second participation of the second particip	e Ma Data Publishing Cyberteculty Data Protection - - -	The organization establishes, maintains and disamonates cybercountry & dataprotection particle standards and procedures.	The Digital Isociety Program (DIP) Joburneet represents the iso, consideration of (company taxing's operationality & data protection policies and accorders the DIP is reactioned by (company taxing's executive management and shall be: (p)Commission is the operaporte particular exercise and afficient determined to the operaporte particular exercise and afficient determined in the operaporte particular exercise and afficient determined and the operaporte particular exercise and afficient determined and determined afficient determined and afficient determined and determined afficient determined afficient determined afficient determined afficient determined determined afficient determined afficient determined determined afficient determined afficient determined determined afficient determined determined afficient determined afficient determined determined afficient determined determined afficient determined determined afficient determined determined afficient determined determined determined afficient determined determined determined afficient determined deter	An arganization's optimizerarity policies cancer brinds for inglementing cyberceuring & data privacy mesoures to protect to most valuable asserts. All personnel durule be assert af the sensitivity commentations and the sensitivity	Management	Bioc Cybertacum Protection Co	& Data Building Cyleriseurity & Data Protection Documentation	609-02	Mechanismic exit to etablish, mantain and disseminate ighest-contry & data protection palities, candidatis and procedures.	- Steering assesses - Digital Security Program (DDP) - Operationality Program (DDP) - Downmanie, Rick and Compliance Solution (DDC) food (SCCCameer), Suick and Compliance Solution (DDC) food (SCCCameer), Suick Claud, Claberdio, Zeroldic, Archev,	0-609-68 0-609-68 0-609-55	Does the organization exclution, maintain and docennoister operationality & data protection policies, clandariti, and procedures?		samely	x x	x pracedures	cendence of a capability to establish, maintain and to sphereourity & data providy policies, standards and %	Cybersonarty & Privacy Enversione (ISDV) efflats are ad locand monoscipers: CMM1zevi 2 control reading would reasonably expects or atteast room; the following control as well: •Noformal cybersocurty and/or data privacy principle care identified the expension.	Cybeneouthy & Princy Sovened at a local/organial level, but are not observed and flowards governed at a local/organial level, but are not concenter should be appreciated at a local/organial level, but are not flow reasonably expectant, or at least must, the following others to exist - cybenseurity and data princip governmene extintes are deservabled to an expected of the state of the source extintes are deservabled to be an extinct of the source of the source extintes are deservabled to be an extinct of the source of the source extintes are deservabled.	Cyberson Ty & Princey Governance (ECV) effects are standardised across the againstation and constitivy enabled, where technicality feasible, the energy accessions; Collibrative Notestinianumity would reasonably expect all, or at inset mind, the following critericate exist = 4 Generatore, Risk & Compliance (RIC) Surdice, or similar feedbox,	Cyberescurity & Privacy Sovernance (SDV) efforts are netrocodrives any product outforest management magts (Sourd on aquantizative understanding of process capabilities (1) a predict capability and encure santimum agressions and sheriffy areas for improvement, to addition to CMM server 8 others, CMM server 6 cannot networky would	ter IP-CMIRE IP-CMIRE IS (A, sone a cantinuoudy-improved process K not increasing to establish, maintain and doorminuse igher incuring & dataprinacy policies, standards and procedures.
2 Cybersecurity Protection Gav	(Company/Name) shall the purpose of the implementand mantan a patiently lated capability to water of the security and relies of all to techning inforcementand manual to the security and inforcementant manual to the security and inforcementant manual to inforcementant ma	e una 1.1 007-021 European Management	The organization prohibits exceptions to standards, except when the enception has been formally assess for mick impact, approved and encoded.	Par exception management purposes, [Company Name]: ond (plevalidation management purposes, [Company Name]: (plevanuts, limited exceptions to a standard, where the following is met: 1.Requests, for exception to a standard performing submitted to	For exception management purposes: 20. publy or defined as a high-level clatereset of management intext that exists. Is influence and guide both present and follow decision making to be influenced.	Mangement	Broc Eybertacutty Protection So	& Data Exception Management	609-623	Mechanismic exist to publicle exceptions to strandards, except when the exception has been formally assessed for each impact, approved and instance.			Door the opperation publish encyptions to conclude, except when the exception has been forman associated for each impact, approved and resistent?	289 -	Pased	x x	X approved an	oendence of a capability to prohibit exceptions to standards, on the exception has been formally assessed for nick impact, and recorded.	Cybersecurity & Privacy Sovervance (ISCV) efforts are ad hoc and massisters: CMM12evel 2 control industry woold reasonably superita or atheast most, the following control has based. •Norformal cybersecurity and/or data privacy principles are identified the organization.	Cybersourtry & Prinary Sovenanar (SDV) efforts are inquirements all, drives and formary governed at a local (regular line), but are not considerations the organization. CMM tene? Consist manufact would fill measurably expectall, or at local must, the following cities to exist expensioning and data prinary governance activities are discentiated	Operators in the standard and constraints (EON) efforts are standard and across the signaturation and constrainty managed, where technically feasible, the energy accesses (c). Constrained the standard weak reasonably expect all, or at livest most, the following orders have exist. •A deventioned, Rois & Compliance (RMC) function, or similar featible,	See SP-CMUELSP-CMMLEX(), since a quantitatively-somewind process is not recessing to provide the wayshows to standards, except when the exception has been formally assessed for eck impact, approved and recorded.	See SP-CMBR 3P-CMR51 (R(A, some a continuously improving process) Is not necessary to product encogenose to conducted, encogenation the exception has been formally assessed for risk impact, approved and recorded.
2 Cybernoutly Protection Gav	(Company/Name) shall The purpose of the implement and maintain a Cyberiocurity & Dis mainty-based capability to visited on the security and ordered on the security and policy is to govern.	e UEA Periodic Review & Option 1.3 0070-08 Cyberkeounty & Data PoliteZion Program	The organization reviews the opherocarity & data set protection program, including policies, standards and procedures, all planed intervals or if organizati changes occurs researe their continuing suitability, adequacy and effectiveneos.	To encore (company Name) is construining alignment with its sociality of coalegy, site appendix, with characteristic and a adhering on a subjectable adatatory, regulatory weight constantial compliance califigations, (company Name)'s executive in-aderiting to other accountable humanist role or function) much review the Digital incommunity.	Updates to the DDP will be annanced to employees up management updates or employees up management updates or employees up and the second of changes will be content in the Record of Changes to highlight. It the personent changes from the provides and the second of the second of the second of the second of the second of the second of the second of the second of the second of the second of the second of the second of the second of the second of the second of the second of the second of the	Mangement	Broc Eyleriacum Protection Son	& Data Roberts Cybersecutty & Data Protection Program	601-01	Mechanisms exects an inview the optionscorely & Extra privacy program, including periods, catalitatis and proceedings, inglamentationna and or figurificant changes easier to insure their continuing suitability, Mequaly and effectiveness.	- Governance, Kick and Compliance Solution (URC) Soul (ICPCanned), SameClaud, OStendio, Zeiddler, Acklew, RSMA, Meelostana, etc.) - Steering cammilitee	0-609-52	Does the expension on the second	7	samely	x x	X planed ste cardming c	e-nations of a capability to review the syberiescurp & data again, including pations, candudor and procedure, at networks or if operfaced, changes court to ensure their guardability, adequate and effectiveness.	Cybersonarty & Privacy Enversione (ISDV) efflats are ad bacand monoscipers: CMM1zevi 2 control reading would reasonably expects or atteast room; the following control as wells: •No format cybersocurty and/or data privacy principle care identified the expension.	Cybeneouthy & Princy Sovened at a local/organia feed, but are not observe and feedal governed at a local/organia feed, but are not concentrations the segmentation. CMM tested control instantly would fair instandably repectant, or at least must, the following citteria to exist - cybenseurity and data princip governmene extintes are deservabled in the segmentation of the second principal control and principal concentration of the second principal control and principal contents of the second principal content of the second principal	Cyberson Ty & Princey Governance (ECV) effects are standardised across the againstation and constitivy enabled, where technicality feasible, the energy accessions; Collibrative Notestinianumity would reasonably expect all, or at inset mind, the following critericate exist = 4 Generatore, Risk & Compliance (RIC) Surdice, or similar feedbox,	Cyberescurity & Privacy Sovernance (SDV) efforts are netrocodrives any product outforest management magts (Sourd on aquantizative understanding of process capabilities (1) a predict capability and encure santimum agressions and sheriffy areas for improvement, to addition to CMM server 8 others, CMM server 6 cannot networky would	he HP-CMIME 3P-CMMIN N(A), since a cantinuously imprinning process is not necessary to review the opheroscomy & data privacy program, including policies, canonication proceedings of policy programs including policy, canonication proceedings of policy and ophicaet changes occur to ensure their continuing suitability, adequa- and effectiveness.
2 Cybersecutity Protection Gov	(Company/Name) shall the purpose of the implementand mantan a Cybersourity & Do manny based cigability to vision of the security and observed, man and the security and observed, man and the security and observed, man and the security and observed man and security and observed	e Ma GOV-06 Assgmed Cyberseamly 8 ha - -	The organization accigins a qualified individual with the encount and resources to encodify manage, 2018 Coordinate, develop, inplement and manatism an extensional, develop, inplement and manatism an extension evaluation of the content of the second s	The Executive and line management must take formal action to support operatorizing through locating documented direction and commitment and must ensure the action to because using the overall authority and responsibility for managing the operatorizing program are designed to [company term] clinic functions	Central management refers to the experiation-wide management and implementation of selected cyberosculty and data protection controls and related protection. Central management includes	Management	Bioc Cybertecutty Protection Co	& Data Accepted Cybersecurity & Data Instance Protection Responsibilities	60V-01	Mochanisms exist to solga new or new polifield individuals with the mission and incourses to controlly-manage, and and an	- NSTNEX Flamewalk - Chief Information Security Officer (DSD)	1-965-05 1-965-05 1-965-05 1-965-07 1-965-08	Does the expension many and or more qualified individually with the environment of constaily-many, conditable, develop, implement and maintain an entreprise-wate cybersecurity in data-potentian program?	4 - 10	samely	x x	x pragram.	cendence of a capability to accept acquaithed individual with in and resources to centrality-manage, coordinate, develop, it and maintain air enterprise-wide cybersecurity & data privacy	SP-CMMI (LTR)16, EXCe a structured protect is required to policy a qualified instructural with the mixture and resource the protectify manage construince, develop, implements and exact an an extension wide cyber security & data privacy program.	Cyberseurtry & Prissly Barenaux (00%) efforts are requirements (e), diver and formality general at a local/vigitual level, but are not concrete thoses the organization. CMM tevel to constant mustify would reasonably regestrall, or at least must, the following otherta to exat explorison by and data privacy generative activities are deservabled by the second private second private activities are deservabled.	Cybersecurity & Privacy dowernance (EDV) efforts are standardiard across the apparation and constity enabled, where technically feasible, the energy accesses (CHBLeret Roteritarius) result reasonably expect all, or at load most, the following orders to exist. «A dowernance, Rola & Compliance (DRC) surplus, or similar feadow,	See 3P-CMER.3P-CMMEIX[/k, since a quantitatively-sonarising process is not recordary to assign a qualified individual with the mount and resources its constrainmentation of the sonarise of the sonaria and maintain an extension-wide spherocarity & data privacy program.	See SP-CMBR 3P-CMBS H (A, Sine a continuously improving process is not increasing to acquire qualified individual with the motion and increasing to control processing, increasing, implement and increasing and extend processing of the second state of the second matrix is an enterproce-web cyber security & Cata privacy program.
Cybersecurity Protection Gav	(Company/tame) shall The purpose of the implementant and maintain a DBL maturity-based capability to visues of the security and estimated at its technology relation of its technology	e BEA 1.3 009-06.5 53-00-e	The organization enforces an accountability shorthow octobe appropriate trainic and individuals are empowered, increase the and based for enormapping, measuring and managing data and technology-relate make.	[Company/Name] requires conclution and line management ta: (plecomment rule: and requires) these states are admitted to make decisions as testical and (company states) within that individual's area of requires) that (plenome decision) and (plenome decision) are admitted on a state management practices that	None	Management	Boot Protection Son	& Data Stakeholder Assurtability Intanie Studium	609-041	Mochanows exist to enforce an accountability divolute to that appropriate tranes and indeeduals are exponented, responsible and tototed for mapping, measuring and managing data and technolog- rotated colar.	Documented roles and responsibilities	1-985-25	Doot the opperation enforce as accurately for under a soft appropriate traver and induced of an empression (responsible and trained for mapping, measuring and managing data and technology initial encode	i br	sawefy	x x	X related roks	centence of a capability to enforce an accountability structure proprior teams and individuals are responsed in expension of in capping, measuring and managing data and technology- dis.	3P-CMMI (cR)(A, since a chrachured protect is required to enforce an accounted by structure to that appropriate search and individuals; are responsived, reproductible and Status of far mapping, measuring and managing data and technology-related exist.	SP-CMR21X R(b), since a well-defined protectic required to enforce an accombibility clusters with appropriate trans. Such underdanks are empowered, responsible and Specific and an appropriate transport, messaring and managing data and technology-related miss.	Operators of the opportunity the endower (SDV) efforts are standard and across the opportunity opportunity reacting 4, where technically feasible, the endower descriptions; Conflictment for endower reasonably expect all, or at lineat most, the following orders take entit. A description, field & Campiance (SDR) function, or similar function,	See 3P CMER 3P CMME IX/A, since a quantitatively-sonarised process is not receivery to enforce a assumption of Vacchare so that appropriate transmission and vaccharise responsives, a question that trained for mapping, measuring and managing data and technology- related roles.	See 3P -CMBR 3P -CMB1 is R(A, since a cantinuously improving process) K in all excitance particular an accountibility clusture outbut appropriate taxes and involvable are improvement, explorately and trained for mapping, mesouring and managing data and technology- related index.
2 Cybersecurity Protection Day	[Company/tame) shall The purpose of the implement and mantain a country based apality to readless of its technology without and the sharing and opticity and apality to public to a first technology without and a sharing and the technology and the sharing and technology and technology and technology and technology an	e BEA 609-66.2 Authoritative Chain of Command	The organization establishes an authorizative channo command with draw time of communication to even and apply from individual can be manned that the managing data and technology related risks.	of [Company/Name] requires conclusion and line management ta: (p)(Chardy-document) an organizational chart to define ater 1. Down), and 2. Down (w) and 2. Sindnet chains of cammand, and (b)(Recognize the authority of designated individuals to make more and other	None	Management	Broc Cybertecum Protection Go	& Data Authoritative Chan of Innana Command	609-663	Mochanies east to instability and instantiation of animate with dearlines of communication to immune analgoing from individuals and teams related to managing data and technology-initiated roles.	- Digenzeron diert	1-985-25	Dest the opproximation establish-as authoritative chain of cammand with the original cammanitation to menuse analoguity from individuals and teams related to menopy or an exchanicipy-initiated mixit?	7	sawefy	x x	X Individuals a roba.	centence of a capability to establish an surfacilitative chain of with client tree; of communication to remove ambiguity from is and teams related to managing data and technology-related	3P-CMMI (cR)(3), since a chruchwed protect is required to establish an authorithme chain of command with close times of communication to renove antibuying from individuals and teams related to managing da and technology-related exist.	3P-CMM2 is R(b), since a well-defined protectic required to establish a autostratave data of assessand with dearthest of dominanciation to an ensous analyphythesis students and teams critized to managing data and technology-related role.	Operators of the operators of the second sec	See 3P-CMEE 3P-CMME IX[/s, since a quantitatively-instanting process is not receiving to establish as authoritative channol inseminal with dear these of communications to more availability from individuality and teams instand to managing data and technology-initiated max.	See 3P -CMBR 3P -CMB1 is R(A, since a continuously improving process is not necessary to establish an authoritizate elsas of commany with destribute of communications to more a malegaler from mithed act and teams initiated to managing data and technology initiated risks.
2 Cybersecurity Protection Day	[CompanyName] shall The purpose of the implement and manchain a matching based logalities to Numerical states and the state of the states of the security and restlence of the technology addictionan and data. A how and the states of the states of the security and addictionan and data.	e GGA La GOV-OS Mesourecol Performance 	The organization develops, reports and monitors cyberoscultry & data privacy program measures of performance.	[Company/Name]'s Chief Information Security Officer [CH2], or the CH2's designated appendix develop(), multi-develop and implement. [(Measures of performance or autome-based metrics to measure the efficience out efficiency of the optimization of performance of the efficience of the optimization of the optimization of the exercise output & data princip candidic employed in coopert of the	Measures of performance are outcome- based restricts used by [Company trained to measure the effectiveness or efficiency of the spheresourity program and objectionality 8 data privacy contacts employed in support actions and	Management	Broc Cybertecum Protection Go	\$08a thesaws of Performance	601-05	Mechanismi exit to éverligi, ingoit and mantar ighesteoarthy & étito privacy program measures of performance.	MeSixx Governance, Nok and Compliance Islantices (SRC) cool (ICPCanced, TurneClaud, Oblembia, ZeroSRC, Archev, RSMM, Moledativana, etc.) Independe Rick Management (IRM) solution	8-629-58	Der the operation develop, epoil and nantiv operatories in a support of a performance?		Poted	x x	There is non opheniscum	cendence of a capability to develop, report and monitor rity & data private program messanes of performance.	Cybersecurby & Privacy Diversion (ODV) efforts are ad hoc and monoscients CMM/level is control enduring would reasonably expect a or attract most, the following citteria to exist: with control ybersecurity and, or data privacy principles are identified the organization.	Cybertacuitty & Privacy Sovernance (SDV) efforts are inquirements- all, drives and formally generated at alocal (regiment lines), but are not consider along the organization. CMM lines? 2 control maturity would for instanding expectal, or at load musit, the following others to exact expension music privacy powervance activities are docentrative constructions and and a privacy powervance activities are docentrative	Eybersacumty & Princey Governance (ISDP) efforts are standardized associate organizzation and constatily managed, where technically fractable, to ensure concentency. Childravel Toortrainstantity would reasonable spectral at or at load music, the following contention exerci- ence of the second contention of the following contention exerci- ence of the second contention of the following contention exerci- ence of the second contention of the following contention exercise and contention of the second contention of the second contention.	Eglensecurity & Privaly Governance (SDV) efflattate netrottednes and provide calibrated examplement insight (based or a squarettatue understanding of process capabilities(1) predict optimal performance, encours and many operations and letterity areas for improvement. In addition to CMM Level 1 Context, CMM Level 1 control resource models.	Experiseculty & Privacy Governance (GDV) efflats are "world-class" Opplithes (Intell-winege productive analysis) (e.g., machine steaming, AJ, etc.) is addition to Chiff Level & Contexia, Chiff Level 5 satisfies and machine would machinely expect 201, or at host many, the 500 weing uttents 55 excit.
Cybersecutity Protection Gov	[Campany/tame] shall The purpose of the implement and mantan a mattern a mattern based capability to vision of the searchy and observed the searchy and estimated with the searchy and understand mattern based of the understand mattern based of the based of the bas	e BEA 5.3 SETV-OS.5 Key Performance Inducts (IPTN)	The organization develops, reports and maintain Rey Performance indication (CPR) to a least organizational management is performance monitoring and trend analysis of the cyberoscurity & data private program.	y [Company/Kame] multiidentify Key Performance Indicators (OTK) ii that measure the performance of [Company Kame]'s optensecumy program's measure, vision and strategic direction.	A EPI mesoures of how well samething is being down. EPIs are metrics that help clarify performance expectations.	Management	Broc Cybertecum Protection Co	8.785 ExyPediamance Industors Innanze (DPIs)	609-01.1	Mechanisms exist to develop, respect and monitor they Preformance Indicators (1971) to 2008 organizational management in performance monitoring and trend analysis of the opheroscump & data penalographics.	- Key Performance Inductors (KPN)		Beet the expension events of the events of the events of the expension of the events of the event of the e		Pulled	×	There is non Performance performance privaty progr	centence of a capability to develop, report and monitor Key normalization (Princ) to accur degenerational management in normanizing and trend analysis of the sybersecurity & data again.	3P-CMMI (c0)(3), since a structured protect is required to develop, rep and manifest Key Performance Subclassin (KMS) to autoct organizational management is performance manifesting and trend analysis of the systemetarity & data privacy program.	port SP-CMR21X R(A, since a well-defined protection required to develop, in report and monitor Key Performance solutions (CPR) to accost organizationalizational protection and monitoring and trend analysis of the optimisection generation protection.	Operators of the operators of the standard set of the standard set process the operators of constant y managed, where technically fractions is overcare concentency. Constances the following constant would reasonable spectral at our kinetic mean, the following constants would near standard program and the standard program and the standard program and the standard program and the standard program and the standard program and standard program and stand	Cybersecurity & Privag Governance (SDV) efflattaine netrocolineer and provide outbranet management imagit (blood or aquantizative understanding of process capabilities) for product optimal performance, encoure authorized operations and encourt parts for improvement. In addition to CMM served to therea, CMM served is annot on encourt provide	Cybersecurity & Privacy Governance (SCV) efflints are "wolfd-staot" Capabilities that investige predictive analysis (e.g., machine learning, AJ etc.) Is addition to Child Level Cortexia, Child Level's cantol insuring would machanize prediate, or at least mart, the following attents to excit
S Cybersecurity Protection Gov	[Company/Kame] shall The purpose of the implement and mantain a statement and mantain a statement of the second part of the manuel statement of the statement of the second part of the second part is technology with the second part is technology bacament of the second second secon	e 1623 1533 1534 1537 1557 1557 1557 1557 1557 1557 1557	The organization develops, reports and monitors tary Risk Indicators (DRII) to address on our management in performance monitoring and trend analysis of the cyberse-outry & data privacy program.	y (Company/Name) must identify Key Nok talkation (KNA) through international key mitchebiles in (Company Name) business units that identify a collocert new of insting and ingoing indication for effective nok management.	A EX II is a massure used in management to indicate how risky an activity is XPCs are metrics used by organizations to provide an early organisation company risk experiance in various areas of the enterprise. It differs	Management	Bioc Cyberlecum Protection Go	80aa maace teytok nekaters(0%)	60V-81.2	Mechanisms exist to develop, region and monthin they thin technologies (form) to avoid sensor management in performance maintening and trend analysis of the sphereourity & data privacy program.	- Key Nokindicators (KN)		Deet the equation is a sport and manufacture (the transmission) is a sport and manufacture (the transmission) is a sport and manufacture (the expension) i	•	Pulled	×	There is non- tick subcito monitoring a pragram.	cendence of a capability to develop, report and monitor Key does (KRO) to accus center nanagement is performance g and trend analysis of the spheric curity & data privacy	3P CMMI IST(I), Since a distalated protect is required to develop, reg and monitor Key Hill Indicators (DER) to addit sensor management is performance monitoring and trend analysis of the sphereourity & dat privacy program.	pot 3P-CMRD is R(R), since a well-defined process is required to develop, report and monitor tray this indicates (DKS) to assist sense? a managementic performance monitoring and trend analysis of the operaciently & dRa privacy program.	Eybersacumty & Prinacy downnance (BCP) efforts are standardized anosci the organization and constativy managed, where technically feadable, to encare concentency. Climitative El bostnain maturity would enabled by expect all, or at load musit, the following others to encir. A downnance, Rola & Compliance (BIC) function, or constant function,	Eglensecurity & Privacy Governance (SDV) efflattate national de pools cultures en pools cultures en augustation () to product our squartitative understanding of process capabilities() to product optimal performance, encore satismus operations and usefully area (or improvement. In addition to CMM served) otherwa, CMM served is cannot encortly would	Cybersecurity & Prince, Governmente (DDV) efficiel ser "solida class" Capabilities inschieverage predictive analysis (e.g., machine beaming, M, etc.) In addition to Child Level & Cortexia, Child Level 5 cantool instanting would reasonably expect all, or at least mart, the following united is to excit
Cybersecutity Protection Gov	[Company/Kane] shall the purpose of the implement and mantain a manual planed application (SCV) manuel direction (SCV) policy is a govern estimated in the security and orderes all its technicity documented, risk-	e Sta 1.3 021-06 Centads With Authoritie	The organization identifies and documents appropria contacts with releases law enforcement and regulate balles.	ate (Company/Rume)'s Chief Information Security Officer (CRD), or the ory CRD's decignated representative), much develop and maintain formal contact with relevant authorities (in g, two enforcement, regulatory bodies and oupervisory authorities).	Cantack with other authorities include, but are not limited to: Elaw enforcement; Phylic utilities; and Thelecommunication providers.	Management	Eroc Cyberiecum Protection Go	& Data enance Cantack With Authorities	601-08	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	Thread Intelligence personnel Integrated Security Incident Response Team (DIRT)		equation shells a very appropriate contact a face enforcement		blentify	x	There is non- appropriate a bodies.	centerior of a capability to identify and document to contacts with relevant law enforcement and regulatory	Cyberosourby & Privacy Sovervance (ISDV) efforts are ad hoc and monocourses: CMMTavel I control ensuring would reasonably expect or attract most, the following citteria to exist: "Automaticyberological and," or data privacy principle care identified the organization.	Cybersourty & Prisay Savenaka (IOTV) of Sorta ar requirements It, divers and Sontally generated at a local/vigonal liver, bottare not considerations the arganisation. CBM Level 2 control maturity would for reasonably repectal, or at least must, the Soltawing others to exist. • Cybersourthy and data prisay governance activities are develoalized	Eybersacumty & Prinacy-Governance (ISDP) efforts are standardized across the organization and constally managed, where technically feadable, to ensure concentency. Climitizenet Doctorshimatority would reasonable yeapert all, or at load musit, the following optimization exist: •N dovernance, Rock & Campiliance (ISRE) function, or cumtar function,	Eglensecurity & Privacy Governance (SDV) efflutture institutiones and provide collisient management insight (based on aquantitative understanding of process capabilities) to predict optimal performance, encore statistical operations and usefully area for improvement. In addition to CDM lawel's othersa, CDM Level 4 control naturity would	Cybersecurity & Princey Governance (DDV) efficient are "world class" Opporting on the twenge predictive analysis (c.g., watchine beaming, AJ etc.). In addition to Child Level & Criteria, Child Level 5 canton in watching would reasonably expect all, or at least must, the Softwarg unterlass excit.
5 Cybersecurity Protection Gav	[Company/Kame] skall the purpose of the implement and mantain a statement and mantain a manuary based capability to Protection (9079) mance designees the security and policy is to govern estimated with the sharing understood of its technology bacamented, man- based covers the bacamented of the bacamented of bacamented of the bacamented of th	a SEA GOV-ET Associations Associations	The organization establishes contact with selected groups and sconzolations within the cyberocurrity Bate privacy communities to: = statistics angoing spherocurrity Bates privacy educations and training for organizational personnel.	[Company/Name]'s Chief Information Security Officer [CH2], or the ASS CH2's decignized representative(3), much develop and maintain formal contact with selected groups and/or associations within the occurity community.	Disgoing cantact with security groups and accounts or is of patientoust importance in an environment of capitaly changing Individuality and threads. Security groups and acausations include, but are not invited in environment environment.	Management	Bloc Cybernecum Protection Go	& Tata Cantacts With Streeps & Accelotions	601-07	Mechanisms eard to enabled a cancerate with oriented groups and associated within the spheresearchy dealers provide consolites this: • "paintime auguing optimication of a faith privaty relationate and training for approximated generations • Self-statistic automotive the enabled optimication of a faith privately position, techniques and the bioinding occurring the enabled optimication or antice sphere position of the techniques of and the bioinding occurring the enabled optimication or antice sphere position of the techniques and the bioinding occurring the enabled optimication or antice sphere position of the techniques and the bioinding occurring the enabled optimication of the techniques of the techniques and the sphere position of the techniques of techn	- SANS - CRDEtectulare Network - ISACA chapters - ISACA chapters - ISACA chapters	ıα	Description with our provide the second seco	el 7	salentafy	х х	There is non- groups and a communities +Facilitate o for organizat	cendence of a capability to establish contact with selected a associations within the sylectrocytity & data privacy testion origining cybertscurity & data privacy education and training cational personnel;	Cybersecurity & Privacy Diversion (IDDV) efforts are ad hoc and monocourses: CMMTevel 1 control endurity would reasonably expect or atleast most, the following cities to exist "addomicitybecourse and, or data privacy principle care identified the organization.	Cybersourty & Privacy Sovernance (GDV) efforts are requirements- ity, drives and formally governed at a local (regular) trees, but are not consider a concern the argumentation. Admit sevel 2 control maturity would for reasonable expectad, of all boots music, the following contexts to exact -cybersourty and data privacy governance activities are docentrative	Eybersacunty & Prinacy-dosenance (ISDP) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure an extension, Child Level Solutionin standard material and a series of the standard protocols and ensure and expect all, or at load must, the following/ortholia on entiti- ed dovernance, Rola & Compliance (ISDE) secretion, or constant function, and dovernance.	Eglensecurity & Privacy Governance (SDV) efflattate metrocodrises and provide collisient management insign (Socied on aquantitative understanding of process capabilities) for predict optimal performance, encore and mean approximation and instructing areas for improvement. In addition to CMM served is otherway, CMM served is cannot encoring would	Cybersteadty & Kristey Governine (DOV) efficient and "and a Class" Copatities of Indianess generative analysis (e.g., machine Issuering, AJ etc.). In addition to Child Level Cortexia, Child Level 5 cancel and underly would reasonably expect 20, or at least mart, the following attends to encode
2 Cybersecurity Protection Day	[CompanyName] shall The purpose of the implement and manchain a matching based logalities to Numerical states and the state of the states of the security and restlence of the technology addictionan and data. A how and the states of the states of the security and addictionan and data.	e GED La La Mission Mission	The organization defines the instead of its business, model and document the microon of the organization is	[Company/Name]'s executive insiderable beam is required to: . (c)[cether the signalization's business model; (b)[cether the mission of the organization so that othersecurity- mitated algestive can be under stand; (c)[cether ensured and instrument issues that are relevant and that efficients.	Toone	Management	Broc Cybertecum Protection Go	& Data Defining Buciness Cantest & Inforce Strates	601-08	Mechanisms exist to define the contract of its buciness model and document the mission of the organization.		1-95	Some paration define the data of its bosiness model and document the ressons of the organization of the second sec		sawefy	x	There is no e model and d	cendence of a capability to define the context of trobucteoc document the mission of the organization.	3P CMMI IS/L(1), SINCE a structured process is required to define the context of its business model and document the mission of the organization.	Cybertacuity & Privacy Sovernance (SDV) efforts are requirements drives and formally governed at a local inguard inset, but are not considered account of the organization. SUMI lawel 2 control maturity would reasonable expectad, or at local musit, the following cortex to evalu- e complementary and data privacy governance schedules are docentrative	Eybersacumty & Princey Governance (ISDP) efforts are standardized associate organizzation and constatily managed, where technically fractable, to ensure concentency. Childravel Toortrainstantity would reasonable spectral at or at load music, the following contention exercit extension (ISD) and ISD and ISD and ISD and ISD and ISD and ISD and A downnance, Rola & Compliance (ISDE) function, or constant function, and the second second second second second second second association and the second second second second second association and the second sec	See 3P-CMIR.3P-CMIR.IX() is since a quantizatively-instantial process is not encourage to define the compact of its houses model and document the massion of the organization.	See 3P-CMIRL 3P-CMIRLIN (A, Give a cashwoody improving process is not excessing to define the context of its bostness model and document the instance of the arganization.
Cybersecutity Protection Gov	[Campany/tame] shall The purpose of the implement and mantan a mattern a mattern based capability to vision of the searchy and observed the searchy and estimated with the searchy and understand mattern based of the understand mattern based of the based of the bas	e usa na ozv.ce Define Control Objective	The organization establishes control objectives as the back for the ordestion, implementation and management of the organization's internal control optimis.	 [Company/Name]'s Digital Security Program (DIP) contanc cannot depeties that save as the back for the selection, implementation and management of [Company Name]'s interval ophenecurity & dat privacy control system. 	The appropriate resc of [company Name]'s interval cantool system is defined by the Ea applicable standord, regulatory and/for compactual obligations that [company Name]'s cyber security personnel must	Management	Broc Cybertecum Protection Co	& Data Innanze Define Control Objectives	601-09	Mechanisms exist to establish control algorithms as the basis for the ordering, implementation and management of the organization's internal isotopi (spines.			Does the expension — excellent-nonexist algebraics at the lases for the celection, anglementations an management of the organization's intensist control system?	5 E	stantify	x x	There is no- basis for the organisation	cendence of a capability to establish control objectives as the te ordination, implementation and management of the on "cinternal control system.	3P CMMI (c/t)/s, since a chruchwed process is required to establish control algoritows as the basis for the orientias, implementations and management of the organization's internal control system.	Cyberseurity & Prisaly Bavenance (IDTV) efforts are reparements drives and formally generated at a local (regional lines), but are not considered associes the arganizations. CBM taxel 2 control maturity would reasonable repectable, or at least mult, the following attenta to wait: • Cyberseurity and data prisally generate activities are discensibled to extend the priority generative discense activities are discensibled.	Operators of the operators of the second sec	See 3F-CMER.3F-CMMELTR/A, since a quantitatively-something process is not encourse to establish control objectures in the basis for the calention, implementation and management of the organization's interval calendal system.	See SP-CMIRE 3P-CMIRE IN (A, Since a continuously improving produce is not excessing to establish control objectives as the basis for the oriention, implementation and management of the organization's internal control system.
2 Cybersecutity Protection Gov	(Company/Name) shall the purpose of the implementand mantan a Cybersourity & Do manny based cigability to vision of the security and observed, man and the security and observed, man and the security and observed, man and the security and observed man and security and observed	e Lia Lia - -	The organization facilitate-cata governance to every the arganization's particle, classifiation and procedures cathol constructive (legislated data is effectively manag- and maintained in accordance with applicable classifiary, regulatory and contractual obligations.	Gompany/Rame)'s Chief Esta-Officer (EDG) must develop and simplement a Esta-Sourceanara Cammative (EDG) annothing of enginestation defined with each defined responsibilities for data governance-related activities.	A data Sovemance Body can below ensure that the apparcation has coherent patients and the ability to obtain the two calify of data with cyberonaumy & data privacy requirements. The data Governance Body establishes	Management	Eshanced Cybertecum Protection Sor	\$085 mana	609-13	Mochanismo e exist to balitate ada governance to evenise the argunostari's palence, (standardicua) procedures at the transmission of the standard standard and standard standard procession of the standard standard standard standard standard standard standard with applicable statutory, regulatory and constant at adaptions.			or the expension failures and generates to server the expension's place, marked and providences that entropy-hypothesis datas of the entropy manager and maintained in anomania with applicable standary, regulatory and contractual subgetuno?	•	Pased	×	There is non- overtae the constitue/reg accordance w obligations.	cendence of a capability to facilitate data governance to e organization's policies, candidate and procedures or that hegitated data is effectively inanged and maintained in e with applicable catalutory, regulatory and contractual 6.	Cybersecurby & Privacy Sovercance (ISCV) efforts are ad hoc and monosphere: CMM12evel 2 control industry woold reasonably superity or atteast even; the following control how exit: •thatformat cybersecurby and/ or data privacy principles are identified the expension.	Cyberseurtry & Prissoy Basemance (0074) efforts are requirements all, divers and formality generad at a locally legislatil level, but are not concrete thoses the segmentation. CMM tevel to constrain marking would fill reasonably segectail, or at least must, the following otherta to exact explorison that prinsing generative activities are deservolated to an another formation of the second excitition are deservolated to an another formation of the second excitition are deservolated	Cybersecurity & Privacy dowernance (EDV) efforts are standardiard across the apparation and constity enabled, where technically feasible, the energy accesses (CHBLeret Roteritarius) result reasonably expect all, or at load most, the following orders to exist. «A dowernance, Rola & Compliance (DRC) Surples, or similar feaders,	Cybersecurity & Privacy Governance (SDV) efficitizate metrics.drives any provide cultivated management magite (based on a spannttative understanding of process capabilities(1) a predict optimal performance, encore sambles dependions and skettify areas for improvement. In addition to CMM Level 3 othersa, CMM Level 6 cannot networky would	See 3P -CMBR 3P -CMR11 R (A), Since a continuously improving process K out increasing its facilities data governance to service the organization's granteet, standard componenties is that ownortine/implotted data/c effectively managed and maintained in accordance with applicable data/acay, regulatory and compactual
Cybersecutity Protection Gov	[Campany/tame] shall The purpose of the implement and mantan a matrix a matrix based apality to visites of the searchy and resilies of its technicity documented, rol-	e Ma ha GOV-11 Purpose Validation	The organization monitors mozion/bucheos ortificat constance of functions to ensure those resources are being used consistent with their intended purpose.	[Company/Name]'s Chief Information Security Officer (CRD), or the CRD's designated apprecisation(s), multi-develop and implement mechanism to analyse massion critical (CR2) induces or untra- (IRC2) technology assets to ensure that those technology resources are being used consistent with their intended purpose.	See Annex & Roseline Security Categoristics Guidelines for Safety & Consoling USC categoroutions. Systems are designed to support a specific microan or Businessfunction. However, over time,	Management	Estanced Exploration for	808a Manage Purpose Validation	009-13	Mochanisms exist to monitor instance/business critical dovotes of functionals because those restancies are being used cancelerer with their intended purpose.			Deet the approximation monitor instance, but near other invaries or function to ensure the resources are being used considered with their intended purpose?		stientify	x	x With their ist	centence of a capability to monitor motion/business-ortical r functions to ensure those resources are being used conditions intended purpose.	Cybersecurby & Privacy Soversance (ISCV) efforts are ad hoc and monoscient: CMM1evel 1 control industry would inscended engents or atteast event, the following oriented beexts: •Radiomatophersecurby and/or data privacy principles are identified the organisation.	Cybersecurty & Prisaly Bavemance (IDTV) efforts are requirements and chorea and formality governed at a locally regulated liver, but are not concentent sources the organization. CMM tasks of control insufting would find instantiably expectatil, or at least must, the following otherta losi source -tybersecurity and data prisaly governance activities are deservabled	Operators of the operators of the second sec	Operators in the Privacy Governance (ISDV) efflats are metrics driver any provide sufficient management insign based or a sparsticiture understanding of process capabilities (1) a predict optimal performance, encore summary dependence and selectify area for improvement, in addition to CMM server3 others, CMM server 4 control maturity would	See 3P -CMBR 3P -CMB1 is R(A, since a continuously improving process is not necessary to monitor resource/bacteria ortification/concor functions to necessary those resourcectare being used consistent with their interedied purpose.
2 Cybersecurity Protection Day	[Company/tame) shall The purpose of the implement and mantain a country based apality to readless of its technology without and the sharing and opticity and apality to public to a first technology without and a sharing and the technology and the sharing and technology and technology and technology and technology an	e BEA 6070-12 Parced Technology Trand (PTT)	The organization accels and/or constrains the formed edification of devoltine / regulated information (e.g. table)inclust Property (P)/to the host government for purposes of market access remarket management pactors.	E [Company/Name]'s executive leadership team mult: (p) (developpmices of to indextfy and saves risks to [Company Name]'s based or planning specific to instruct data requires protectally require Funced technology transfer (PTT) that includes, but is card timeted to: neurosciences	Porsed Technology Transfer (PTT) is a practice in which a government function foreign in Durinescentismes to divising technology secrets in exchange for market access. Secrets we data and nethnology technologies	Management	Estanced Cyberlander Protection Go	&data Insteil Technology Transfer Instalar (FTT)	609-12	Mechanisms exist to avoid a high constraint the fourier exhibition of serior particular distinguishing of the series of the seri	- Rand		Does the organization another analysis and can the functeendinational devotions / regulated information (a), posterbitured response (PT) (b) the back government for purposes of madet access o madet introgeneet practices?	а 20	Pilled	x x	There is non- exclutation of Property (P) market mana	oendence of a capability to avoid and/ or contrain the forced of Generatory / regulated information (e.g., interfectual regulate the data provident for purposes of market access or integrment produces.	SP-CMMI (cN)15, since a structured process is required to avoid and/is constant the found estimation of sensitive / regulated information (e.g., interferctual respects; (b?)) is the local government for purposes o matter bacters or name in management processes.	IF SMEDIATIS (R)A, since a well-defined protectic required to avoid and/ economisms the found editionism of senatory / regulated information of (n.g., instead integrity (in the backgrowennest for purposes of makeet assess or market runggement practices.	Operators of the operators of the second sec	See 3P-CMEE.3P-CMMEE.X[/k, since a quantitatively-solution of cost exercises you have a long or constants the found of distance of encounter / programs information (e.g., solution) and property (PI) (so the host government for purposes of market scores or maket management pactors.	See 3P -CMBR 3P -CMB1 is R(A, since a continuously improved process is not exercising to avoid and/or constrains the forced extitution of monthew / populated information (i.g., instellectual property)(P) [13 the forct government for purposes of market access or market management practices.
2 Cybersecutity Protection Gov	(Company Name) shall the purpose of the implementant mantana a control of the purpose of the maturity & Extend applicitly & DX Protection (DXP) pathog & DX pathog	e Ma La 029-13 350e-tijoncored Bijnona -	The organization constrains the hold government's addity to hveroage the organization's technology acce for concourse or pathtical exponence and/or cyberoantee activation.	[Company/Rame]'s executive inader/hip team mult: etc. ((Developpmicesco) to identify and source roles to [Company Rame]'s functioner practices from cate-sponsored expensage adjustes. (((Developppopuls) calculate in the secondariation strateger that expension and company and calculate in the secondariation strateger that	Itale-consumd espresage factors of discovering and exploiting (Company Name)/comparise source and technologies fair the benefit of the husble actor's country. This includes, but is not thered to:	Mangement	Eshanced Cybertecum Protection Sor	\$285 Star-Sponared Equivage	609-18	Mochanismic exist to associate the local generation of the control	y - Baad of Down		Does the opposition constants the hold government's ability to leverage the exponentias's technology assets for economic or political exponency and for syleeworkse activities?	2	Potest	x x	There is non- ability to leve political expr	cendence of a capability to constrain the host government's needige the argumization's technology assets for economic or capanage and/or cyberwarfare activities.	3P-OMM (LO()), since a christianed process is required to constrain the food powersenic's addity to leverage the argumentatic's technology assets for economic or political expanage and/or opervisitize activities.	 SP-CMR21x R(h, since a well-defined prosecus required to contrain the host government's addity to inversage the organization's technology assets for economic or political expanage and/ or systemicalize addition. 	Cybersecurity & Privacy dosenance (EDV) efforts are standardized across the againstaton and constity managad, where technically feasible, the neuron accessions; Chillbaret Roteritariusantly evaluation reasonably expect all, or at load most, the following/orders to exist a A dosenance, Rola & Campiance (IDC) function, or consta function, and accessions; Child & Campiance (IDC) function, or consta function, and accessions; Child & Campiance (IDC) function, or consta function, and accessions; Child & Campiance (IDC) function, or consta function, and accession accession accession accession function, accession function, accession accession accession accession accession accession function, accession acc	See 3P CMUELSP CMML IX()4, since a quantitatively-somewined process is east excessing to constrain the host government's ability to beyonge the argumatomic thermology assets for examines or partitual exprimage and/or cyberwarfare activities.	See 3P -CMBR 3P -CMB1 is R(A, since a continuously improving process is out increasing its contrained the bud government's Addity to overlape the argumentary stochastic passes for economic or patitical esponage and/or optimization activities.
1 Cybersecurity Probection Gen	[Company/Kame] shall The purpose of the implement and manches a many based capability to readers of the security and entregettes the security and publy is to govern indicators of its Sechndargy biological and tax.	e BES 5.3 GOV-34 BACKER FLADAR (BAD) SeCure FLADAR M	The organization incorporates syleeneavity & data privale principles into humanissi. As zoual (MAI) plastices through executive feadership involvement.	[Company Name]'s executive inadership beam must develop processes to scorpacize a glenno-unity & data privacy principles into musiness in stuard (Mol) practices across [Company Name]'s busines operations.	Poine 6	Management	Bios Cybershouth Protection Son	& Data Buranesi Astocal (BA3) Incare Produces	609-14	Mochanismic exist to insight and presently & Addis private principle critic busines and (DKC) practices through execution and by involvement.			Date: the eigenstation incorporate righteneums, & data privacy principles into Business As total (BAU) practices through execution instaership invaluement?	•	Potest	×	x Press is non- privacy principality princip	cendence of a capability to incorporate cybercecurty & data incipies into Businesi. A Obaid (BAU) practices through leadership involvement.	1P - CMMI (c/t)/s, cince a structured process is required to incorporate sylenneumly & Exits process processing incoherence. As Obsail (MAD) practices: Unitsight executive leadership incoherence.	3P-CMR2 x IQA, since a well-defined protectic required to incorporate opteneously & alta privacy principles that Bacaneer AC Usual (BAD) practice through executive leadership inschement.	Epherancumty & Prinacy dose mance (BCP) efforts are standardized across the organization and constativy managed, where technically feasibles, the every accordings: Contributive H constraints would reasonably expect all, or at livest mind, the following criteria to exist a Gaussiance (BCR) & Compliance (BCR) function, or crimital feadings	See 3P CMML 3P CMML IX/A, since a quantitatively-controlled process is not exercisely to incorporate cyberseculty & data privacy procedure into Transver. As Usual (IMA) practices through executive leadership incoherence.	her 3P-CMBL 3P-CMB11 K(A, since a castinuous) emproving protect K exit exercising to incorporate operaneutry & data privacy principles to a busines. As Usual (BBLS) practices through executive leadership involvement.
S Cybersecurity Protection Gav	[Company/Name] shall The purpose of the implementant meantain a material based apallity to Public of the security and ordiness of the base of the security and indicators of the based of the security and indicators and security and based on the security and indicators and security and based on the security and indicators and security and based on the security and based on the security and indicators and security and based on the securit	e GDP-33 Cpercitionalizing Cpercitionalizing Cole-security & Data Productions Fractions	The organization competend and and/or process owner to operationable of phenomenology & data protection processor for each system, application and/or service under their control.	It becaute and the management mutitals competiate and/or process owners to specification be determined by determining solution process for the cash systems, applications for anyone under their control through processor for an advancement and that determine and the second statement of the se	Tuone	Management	BIOC Cyberseculty Protection Go	& Data Operationalizing Cybersecurity Innanze & Data Protection Practices	ny 001-15	Mochanismis exect to camp the providence of the separational are glownawing principleations for each space. The principleation water their control.			Date: the organization competidata and/or process connex to operationative phenocentry & data prinary practices for each system, application and/or service-under their consol?		Pased	x x	There is non- devent to op system, appl	cendence of a capability to competiaticand/ or process operationalise openeousity & data-principaticies for each photon and/ or service-under their canoni.	3P CMMI IS/U(), SINCE A STRUCTURE protect is required to competitize and/an process owners: to operationation systematicity is data privaty practices for each system, application and/ar service under their conti- cution.	3P-CMR2 x T(A), since a well-defined protect is required to competitud and/or process sweres to operationalize optimization (a factorina) processor for each system, application and/or service under their control processor for each system, application and/or service.	Eybersacumty & Princeydose nance (BCP) efflicts are standardiaed across the organization and centrality managed, where technically fiscalatin, the neuron accessions: (Childhared Rotenthistanthy would reasonably expect all, or at lineat most, the following/ordentatio entit. «A downnance, Rola & Compliance (DIC) function, or similar function, and accessions of the standard standard standard accession of the standard sta	See 3P-CMULT3P-CMMULTA/Ix, since a quantitatively-isorballed process is not necessary to compret data and/or process owners to approximation cyberonoutry & data provid pactitions for each system, application and/ or censor under their control.	her 3P-CMBR 3P-CMBS in X(A, cance a continuously improving protocol is not inclusionly to competitudia and/or process overent to operationality operationality & data privacy positions for each system, application and/or or census under their council.
Cybernecurity Protection Gav	[CompanyName] shall The purpose of the implementand matchins a Cyberoecumty & Du back of the second state of the second state of reading company of the second panel of the second panel of the second state of the second stat	e Ma 1.3 029-33.5 SelectControls	The organization competicizes and/or process owner to onless required spheroesarity & data privacy control for each system, application and/or service under the control.	Stata and/or process services are inspected to select required to coherence on the data privacy constants for each system, paginations and/or anone under their constant. Required determination of determination and/or anone and their constant. Required determination of applications into an anone and the data as a similar above of applications. Indefinitions for constants are addeted as a similar above on a page to the indefinition of constants are addeted as a similar above on a page to the indefinitions.	While MCK establish the minimal cantoxis that must be adhered to, DSK are where expansions when achieve improved ethorecy, automation and enhanced cancels	Management	Boot Cybernecurty Protection Cor	& Data senance Select Cantools	609-13.1	Machanisma veist to sampet data and for product to sensor of devocuting Britata prinacy contract for each system, application and			Boes the expensation samper data and/or process owners to select required spheroecurty & data privacy antisis for each system, application and/or service under their autour?		Pater	*	x Calena, appl	e-indexec if a opability to competitation of or process -solect impained spheroeumly & data privacy annuals for each aprilation and/or service under their cannul.	SP-CMM2 (LTL/R, since a structured process is required to competiate and/ar process reveres to adect required apheneticarity & data privaty construction each system, application and/or sensor under their contri in the sensor of the senso	 IN-CARLY IL TUD, UNLY a work defined protect required to competitize panaly or protect to select required cybersecutty. & data protect protection of a set by them, application and/or concern index their control or protection. 	Cybersacuithy & Prinacy Sovernance (SDV) efforts are standardized account on equivalent and constantly managed, where it inclusively finalizes, for earning constantly managed, where its standard reasonably watert ally or at inact many, the following orthograph and constantly watert ally or at inact many, the following orthograph is to movement which its memory that is standard or constants (which are its inact and provide the standard or constants).	See SP-CMRE SP-CMRE URUS, since a quantitatively-analysis for incent eccesary to competibility and/or process contex to salinet required operiod curring & data and/or process contex for each system, application and/or service under their carbot.	I be SP-CBBML SP-CBMERIC R(A, sour a continuously improving process is not necessary to competiate and/or process owners to stretct enquined operationality & data privacy controls if ne acti optimes, application and/or service under their cantool.

SCF Domain	CMRM KPX #	Key Performance Index (KPX) 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				30%		28.30					
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					í
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					í
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					í
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		Accel Management	100%	5%	90.7	4.44				201/	161
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			Asset Management	100%	5%	80.7	3.20				20%	10.1
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					í
Asset Management	AST-A-10	IoT/OT with Assigned Owners	74.2%	% embedded technology-class systems with an assigned system owner/custodian	1 AST-M-096 divided by AST-M-067					5%		3.71					í
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					í
Asset Management	AST-A-12	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined					0%		0.00					í
Asset Management	AST-A-13	TBD - company-defined	0.0%	TBD - company-defined	T8D - company-defined					0%		0.00					1
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				25%		8.33					
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)	BCD-M-004 divided by BCM-M-001	KRI				50%		21.88					
Business Continuity & Disaster	BCD-A-03	Incidents Related To Lack of Capacity or Denial of Service (DoS)	3.4%	% incidents related to capacity issues or Denial of Service (DoS) attacks	CAP-M-001 divided by IRO-M-003		KPI	Business Continuity & Disaster		25%		0.84					í
Business Continuity & Disaster	BCD-A-04	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined			Recovery	100%	0%	31.0	0.00				15%	4.7
Business Continuity & Disaster	BCD-A-05	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined					0%		0.00					í
Business Continuity & Disaster	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					100%		85.82					
Compliance	CPL-A-02	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined					0%		0.00	IDENTIFY	63.0	100%		í
Compliance	CPL-A-03	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined			Compliance	100%	0%	85.8	0.00				10%	8.6
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 8CD-M-001	KRI				40%		29.17					
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					1
Network Security	NET-A-03	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined			Network Security	100%	0%	62.9	0.00				15%	9.4
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					1
Risk Management	RSK-A-01	Production Migrations With Exceptions to Standards	72.7%	% projects transition into production with exceptions to standards	RSX-M-003 divided by PRM-M-004					25%		18.18					
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					í
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	Risk Management	100%	20%	67.2	10.84				20%	13.4
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-N+-001 divided by RSK-N+-002					30%		8.43					
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-078 + AST-M-079 + AST-M-008 + AST-M-012 + AST-M-012 + AST-M-014 + AST-M-019 + AST-M-019 + AST-M-028 + AST-M-028 + AST-M-028 + AST-M-028 + AST-M-038 + AST-M					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)	1 TPM-M-007 divided by (AST-M-003 + AST-M-004 + AST-M-014 +			71	40000	20%	53.5	0.14				2014	
Third-Party Management	TPM-A-04	TBD - company-defined	0.0%	TBD - company-defined	TBD - company-defined			Third-Party Management	100%	0%	53.5	0.00				20%	10.7
Third-Party Management	TPM-A-05	TBD - company-defined	0.0%	TBD - company-defined	T8D - 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					