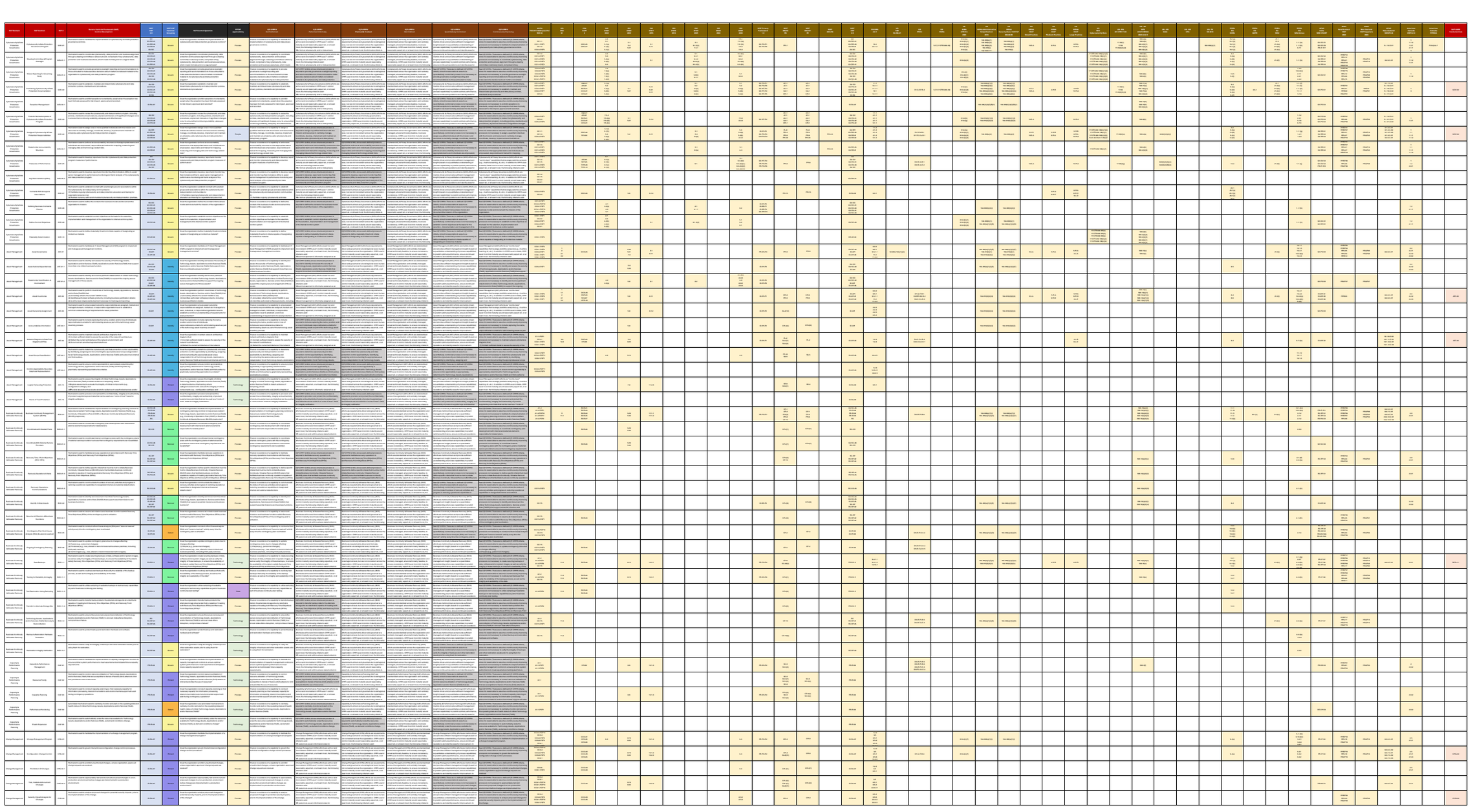
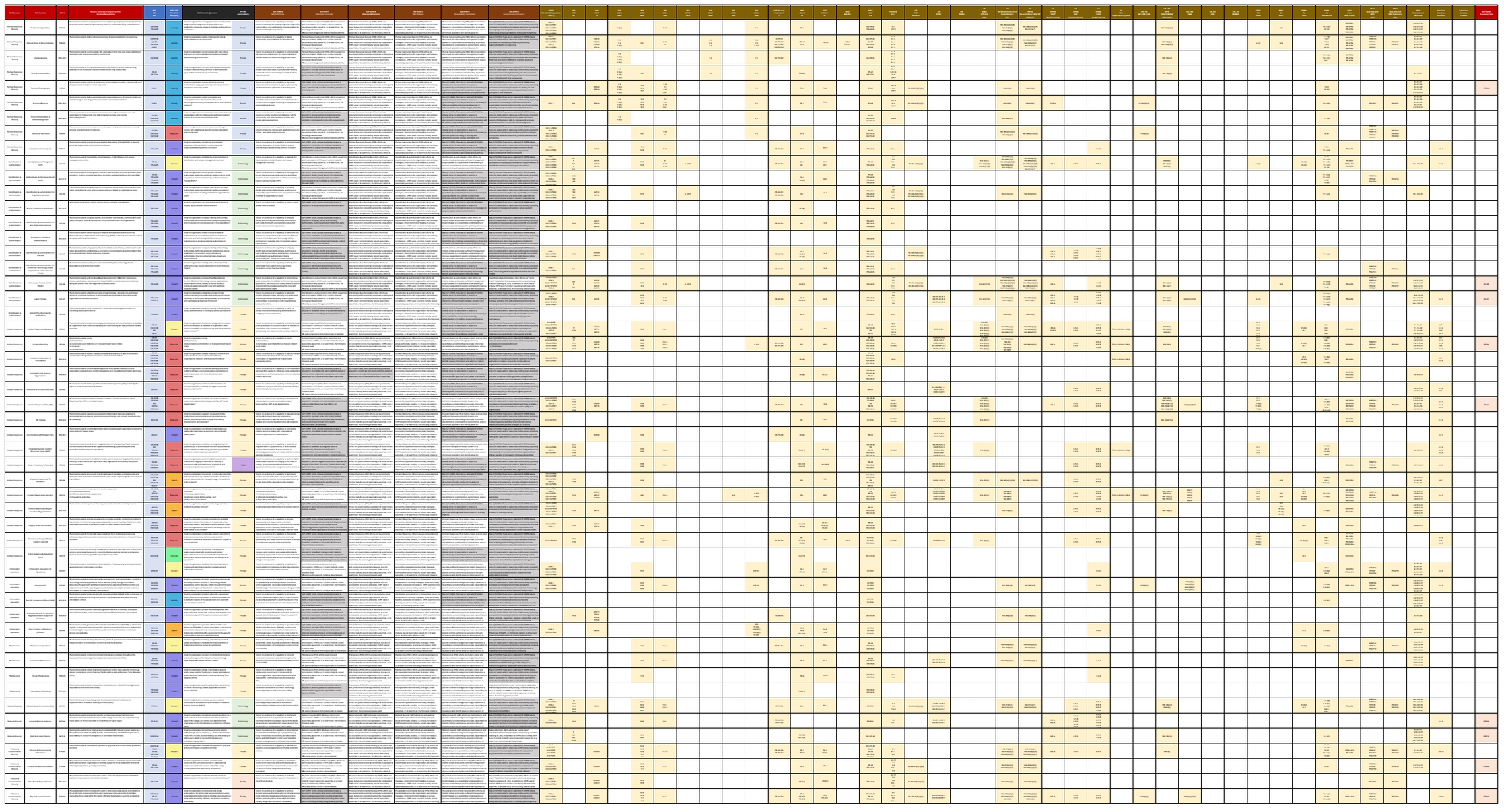
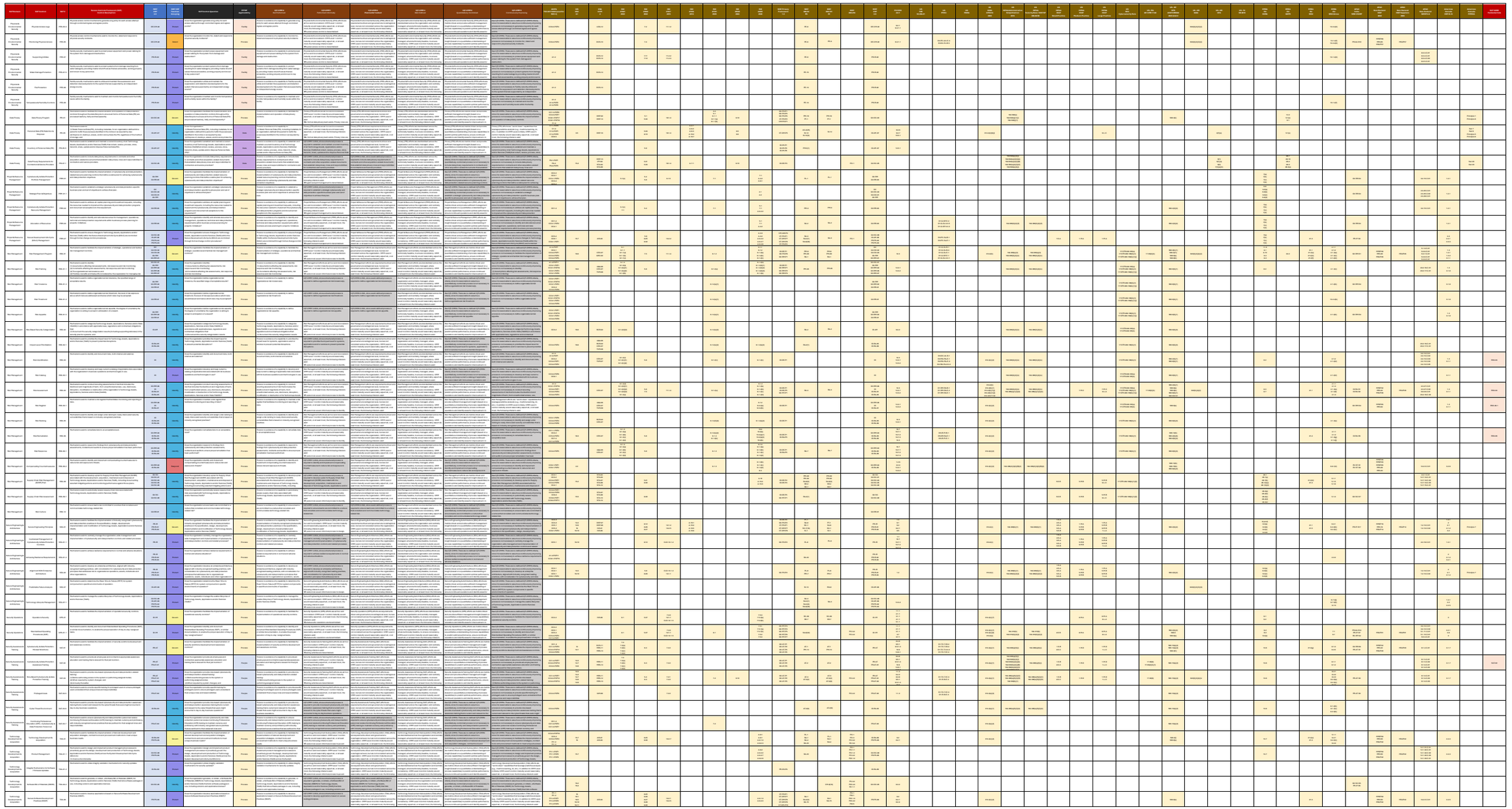


SCF Domain	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST CSF 2.0	NIST CSF Function Grouping	SCF Control Question	PPTDF Applicability
Change Management	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	ID.RA-07	Protect	Does the organization enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes?	Process
Compliance	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	GV.OC GV.OC-03 GV.SC-05 PR	Govern	Does the organization facilitate the identification and implementation of relevant statutory, regulatory and contractual controls?	Process
Compliance	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity and data protection controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	GV.SC-05	Identify	Does the organization document and validate the scope of cybersecurity and data protection controls that are determined to meet statutory, regulatory and/or contractual compliance obligations?	Process
Compliance	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership.	GV.OC-03	Detect	Does the organization provide a cybersecurity and data protection controls oversight function that reports to its executive leadership?	Process
Compliance	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity and data protection policies, standards and other applicable requirements.	ID.IM-01 ID.IM-02	Detect	Does the organization regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity and data protection policies, standards and other applicable requirements?	Process
Compliance	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's cybersecurity and data protection policies and standards.	ID.IM-01 ID.IM-02	Detect	Does the organization regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to its cybersecurity and data protection policies and standards?	Process
Configuration Management	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	PR.PS PR.PS-01 PR.PS-05	Govern	Does the organization facilitate the implementation of configuration management controls?	Process
Configuration Management	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	PR.DS-10 PR.PS PR.PS-05	Protect	Does the organization develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards?	Process
Configuration Management	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	PR.PS	Detect	Does the organization review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and	Process
Configuration Management	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	PR.PS	Protect	Does the organization configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations?	Technology
Configuration Management	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or	PR.PS	Protect	Does the organization allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment;	Technology
Configuration Management	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	PR.PS-05	Protect	Does the organization configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services?	Technology
Configuration Management	Prevent Unauthorized Software Execution	CFG-03.2	Mechanisms exist to configure systems to prevent the execution of unauthorized software programs.	PR.PS-05	Protect	Does the organization configure systems to prevent the execution of unauthorized software programs?	Technology
Configuration Management	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	PR.PS-05	Protect	Does the organization restrict the ability of non-privileged users to install unauthorized software?	Technology
Continuous Monitoring	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	DE.AE DE.CM-01 DE.CM-03 DE.CM-06 DE.CM-09	Govern	Does the organization facilitate the implementation of enterprise-wide monitoring controls?	Technology
Continuous Monitoring	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	DE.CM-01	Detect	Does the organization implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points?	Technology
Continuous Monitoring	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	DE.CM-01	Detect	Does the organization continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions?	Technology
Continuous Monitoring	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	DE.CM-01 PR.PS-04	Detect	Does the organization generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness?	Technology
Continuous Monitoring	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical Technology Assets, Applications and/or Services (TAAS) to generate alerts for unauthorized modifications.	DE.CM-09	Detect	Does the organization utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical Technology Assets, Applications and/or Services (TAAS) to generate alerts for unauthorized modifications?	Technology
Continuous Monitoring	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	DE.AE DE.AE-06 DE.CM-01	Detect	Does the organization review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures?	Process
Continuous Monitoring	Automated Alerts	MON-01.12	Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications.	DE.AE DE.AE-06	Detect	Does the organization automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications?	Technology
Continuous Monitoring	Analyze and Prioritize Monitoring Requirements	MON-01.16	Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of assets, based on asset criticality and the sensitivity of the data it stores, transmits and processes.	DE.AE DE.CM-01 DE.CM-03 DE.CM-06 DE.CM-09	Detect	Does the organization assess its needs for monitoring and prioritize the monitoring of assets, based on asset criticality and the sensitivity of the data it stores, transmits and processes?	Technology
Continuous Monitoring	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	DE.AE-03 DE.AE-06	Detect	Does the organization utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs?	Technology
Continuous Monitoring	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	DE.AE-03 DE.AE-06	Detect	Does the organization use automated mechanisms to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness?	Technology
Continuous Monitoring	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred;	PR.PS-04	Detect	Does the organization configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred;	Technology
Continuous Monitoring	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	DE.CM	Detect	Does the organization use automated mechanisms to identify and alert on Indicators of Compromise (IoC)?	Technology
Continuous Monitoring	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	DE.CM DE.CM-03	Detect	Does the organization utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities?	Technology
Continuous Monitoring	Insider Threats	MON-16.1	Mechanisms exist to monitor internal personnel activity for potential security incidents.	DE.CM-03	Detect	Does the organization monitor internal personnel activity for potential security incidents?	Technology
Continuous Monitoring	Third-Party Threats	MON-16.2	Mechanisms exist to monitor third-party personnel activity for potential security incidents.	DE.CM-06	Detect	Does the organization monitor third-party personnel activity for potential security incidents?	Technology
Continuous Monitoring	Unauthorized Activities	MON-16.3	Mechanisms exist to monitor for unauthorized activities, accounts, connections, devices and software.	DE.CM-03	Detect	Does the organization monitor for unauthorized activities, accounts, connections, devices and software?	Technology
Continuous Monitoring	Account Creation and Modification Logging	MON-16.4	Automated mechanisms exist to generate event logs for permissions changes to privileged accounts and/or groups.	DE.CM-06	Detect	Does the organization use automated mechanisms to generate event logs for permissions changes to privileged accounts and/or groups?	Technology
Cryptographic Protections	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	PR.DS-01 PR.DS-02 PR.DS-10	Govern	Does the organization facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies?	Data
Cryptographic Protections	Alternate Physical Protection	CRY-01.1	Cryptographic mechanisms exist to prevent unauthorized disclosure of information as an alternative to physical safeguards.	PR.DS-01	Protect	Are cryptographic mechanisms utilized to prevent unauthorized disclosure of information as an alternative to physical safeguards?	Technology
Cryptographic Protections	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	PR.DS-02	Protect	Are cryptographic mechanisms utilized to protect the confidentiality of data being transmitted?	Data
Cryptographic Protections	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	PR.DS-02	Protect	Are cryptographic mechanisms utilized to protect the integrity of data being transmitted?	Data
Cryptographic Protections	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	PR.DS-01	Protect	Are cryptographic mechanisms utilized to prevent unauthorized disclosure of data at rest?	Data
Data Classification & Handling	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	ID.AM-08 PR.DS PR.DS-01 PR.DS-02 PR.DS-10	Govern	Does the organization facilitate the implementation of data protection controls?	Data
Data Classification & Handling	Data Stewardship	DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.	ID.AM-08 PR.DS	Protect	Does the organization ensure data stewardship is assigned, documented and communicated?	Data
Data Classification & Handling	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	PR.DS	Protect	Does the organization protect sensitive/regulated data wherever it is processed and/or stored?	Data
Data Classification & Handling	Sensitive / Regulated Media Records	DCH-01.3	Mechanisms exist to ensure media records for sensitive/regulated data contain sufficient information to determine the potential impact in the event of a data loss incident.	PR.DS	Protect	Does the organization ensure media records for sensitive/regulated data contain sufficient information to determine the potential impact in the event of a data loss incident?	Data
Data Classification & Handling	Defining Access Authorizations for Sensitive / Regulated Data	DCH-01.4	Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive/regulated data.	PR.DS	Protect	Does the organization explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive/regulated data?	Process
Data Classification & Handling	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	ID.AM-05 PR.DS	Identify	Does the organization ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements?	Data
Data Classification & Handling	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	PR.DS	Protect	Does the organization control and restrict access to digital and non-digital media to authorized individuals?	Data
Data Classification & Handling	Media Storage	DCH-06	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	ID.AM-07	Protect	Does the organization: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed	Data
Data Classification & Handling	Sensitive Data Inventories	DCH-06.2	Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.	ID.AM-07	Detect	Does the organization maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually?	Data
Data Classification & Handling	Periodic Scans for Sensitive / Regulated Data	DCH-06.3	Mechanisms exist to periodically scan unstructured data sources for sensitive/regulated data or data requiring special protection measures by statutory, regulatory or contractual obligations.	ID.AM-07	Detect	Does the organization periodically scan unstructured data sources for sensitive/regulated data or data requiring special protection measures by statutory, regulatory or contractual obligations?	Technology
Data Classification & Handling	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third-parties.	ID.AM-03	Identify	Does the organization inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with	Data
Endpoint Security	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	DE.CM-09	Govern	Does the organization facilitate the implementation of Endpoint Device Management (EDM) controls?	Technology
Endpoint Security	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	PR.PS-05	Protect	Does the organization use automated mechanisms to prohibit software installations without explicitly assigned privileged status?	Technology
Endpoint Security	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	DE.CM-09	Detect	Does the organization utilize antimalware technologies to detect and eradicate malicious code?	Technology
Endpoint Security	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings.	DE.CM-09	Protect	Does the organization utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings?	Technology
Human Resources Security	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	GV.RR-04 ID.AM	Govern	Does the organization facilitate the implementation of personnel security controls?	Process

copyright 2025





SCF Domain	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST CSF 2.0	NIST CSF Function Grouping	SCF Control Question	PPTDF Applicability
Technology Development & Acquisition	Criticality Analysis	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	PR.PS-06	Protect	Does the organization require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC)?	Process
Technology Development & Acquisition	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	GV.OC-01 PR.PS-06	Identify	Does the organization perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for?	Process
Technology Development & Acquisition	Software Assurance Maturity Model (SAMM)	TDA-06.3	Mechanisms exist to utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the development of Technology Assets, Applications and/or Services (TAAS).	PR.PS-06	Identify	Does the organization utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the development of Technology Assets, Applications and/or Services (TAAS)?	Process
Technology Development & Acquisition	Cybersecurity & Data Protection Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity and data protection personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and	ID.IM-01 ID.IM-02 ID.RA-01 PR.PS-06	Protect	Does the organization require system developers/integrators consult with cybersecurity and data protection personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;	Process
Technology Development & Acquisition	Continuous Monitoring Plan	TDA-09.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a plan for the continuous monitoring of cybersecurity and data protection control effectiveness.	ID.IM-01 ID.IM-02	Detect	Does the organization require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a plan for the continuous monitoring of cybersecurity and data protection control effectiveness?	Process
Technology Development & Acquisition	Developer Configuration Management	TDA-14	Mechanisms exist to require system developers and integrators to perform configuration management during system design, development, implementation and operation.	ID.RA-09	Protect	Does the organization require system developers and integrators to perform configuration management during system design, development, implementation and operation?	Process
Technology Development & Acquisition	Software / Firmware Integrity Verification	TDA-14.1	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of software and firmware components.	ID.RA-09	Protect	Does the organization require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of software and firmware components?	Process
Technology Development & Acquisition	Hardware Integrity Verification	TDA-14.2	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of hardware components.	ID.RA-09	Protect	Does the organization require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of hardware components?	Process
Technology Development & Acquisition	Unsupported Technology Assets, Applications and/or Services (TAAS)	TDA-17	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of	PR.PS-02 PR.PS-03	Protect	Does the organization prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and	Process
Third-Party Management	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	GV.SC-04 GV.SC-06 GV.SC-07 GV.SC-08 GV.SC-10	Govern	Does the organization facilitate the implementation of third-party management controls?	Process
Third-Party Management	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	GV.SC-04 GV.SC-07 GV.SC-08 ID.AM ID.AM-01	Identify	Does the organization maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of its Technology Assets, Applications, Services and/or Data (TAASD)?	Process
Third-Party Management	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	GV.OC-04 GV.OC-05 GV.SC-04 GV.SC-06 GV.SC-07	Identify	Does the organization identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value	Process
Third-Party Management	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	GV.SC GV.SC-06 GV.SC-07	Identify	Does the organization: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the	Process
Third-Party Management	Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	GV.SC-06 GV.SC-07	Identify	Does the organization utilize security safeguards to limit harm from potential adversaries who identify and target its supply chain?	Process
Third-Party Management	Processes To Address Weaknesses or Deficiencies	TPM-03.3	Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain	GV.SC-06 GV.SC-07	Identify	Does the organization address identified weaknesses or deficiencies in the security of the supply chain	Process
Third-Party Management	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	GV.SC-06 GV.SC-07	Identify	Does the organization mitigate the risks associated with third-party access to its Technology Assets, Applications, Services and/or Data (TAASD)?	Process
Third-Party Management	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	GV.SC-06 GV.SC-07 ID.IM-01 ID.IM-02 ID.RA-10	Identify	Does the organization conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS)?	Process
Third-Party Management	Conflict of Interests	TPM-04.3	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.	GV.SC-06	Identify	Does the organization ensure that the interests of external service providers are consistent with and reflect organizational interests?	Process
Third-Party Management	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	GV.SC-06	Identify	Does the organization restrict the location of information processing/storage based on business requirements?	Process
Third-Party Management	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	GV.OC-02 GV.OC-03 GV.SC-02 GV.SC-05 GV.SC-06	Identify	Does the organization require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting its needs to protect its Technology Assets, Applications, Services and/or Data (TAASD)?	Process
Third-Party Management	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	GV.OC-03 GV.SC-02 GV.SC-05 GV.SC-06 GV.SC-10	Protect	Does the organization ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers?	Process
Third-Party Management	Third-Party Authentication Practices	TPM-05.3	Mechanisms exist to ensure External Service Providers (ESPs) use unique authentication factors for each of its customers.	GV.SC-06 GV.SC-10	Protect	Does the organization ensure External Service Providers (ESPs) use unique authentication factors for each of its customers?	Process
Third-Party Management	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).	GV.OC GV.OC-02 GV.RM-05 GV.RR GV.RR-02	Identify	Does the organization document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and	Process
Third-Party Management	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity and data protection control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.	GV.SC-06	Identify	Does the organization perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity and data protection control assignments accurately reflect current business	Process
Third-Party Management	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity and data protection controls, including any flow-down requirements to subcontractors.	GV.SC-06	Identify	Does the organization obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity and data protection controls, including	Process
Third-Party Management	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or data protection controls.	GV.SC-06	Protect	Does the organization include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or data protection controls?	Process
Third-Party Management	Third-Party Personnel Security	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	GV.SC-06 ID.AM	Identify	Does the organization control personnel security requirements including security roles and responsibilities for third-party providers?	Process
Third-Party Management	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.	GV.SC-07 ID.IM-01 ID.IM-02	Identify	Does the organization monitor, regularly review and audit External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls?	Process
Third-Party Management	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	GV.SC-06 GV.SC-07 GV.SC-08	Identify	Does the organization address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements?	Process
Third-Party Management	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	GV.SC-08	Identify	Does the organization control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party?	Process
Third-Party Management	Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	GV.SC-08	Identify	Does the organization ensure response/recovery planning and testing are conducted with critical suppliers/providers?	Process
Threat Management	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	DE DE.AE-07 ID.RA-03 ID.RA-08	Govern	Does the organization implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response	Process
Threat Management	Indicators of Exposure (IOE)	THR-02	Mechanisms exist to develop Indicators of Exposure (IOE) to understand the potential attack vectors that attackers could use to attack the organization.	DE DE.CM ID.RA-03 ID.RA-05 ID.RA-08	Identify	Does the organization develop Indicators of Exposure (IOE) to understand the potential attack vectors that attackers could use to attack the organization?	Process
Threat Management	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	DE DE.AE-07 ID.RA-02 ID.RA-03 ID.RA-08	Identify	Does the organization maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls?	Process
Threat Management	Insider Threat Program	THR-04	Mechanisms exist to implement an insider threat program that includes a cross-discipline insider threat incident handling team.	ID.RA-03	Identify	Does the organization implement an insider threat program that includes a cross-discipline insider threat incident handling team?	Process
Threat Management	Insider Threat Awareness	THR-05	Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.	ID.RA-03	Identify	Does the organization utilize security awareness training on recognizing and reporting potential indicators of insider threat?	Process
Threat Management	Threat Hunting	THR-07	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	DE ID.RA-03	Detect	Does the organization perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls?	Process
Threat Management	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	DE ID.RA-03 ID.RA-04 ID.RA-05 PR.IR-02	Protect	Does the organization develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade?	Process
Threat Management	Threat Analysis	THR-10	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	DE DE.AE-07 ID.RA-04 ID.RA-05	Protect	Does the organization identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats?	Process
Vulnerability & Patch Management	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	ID.RA-01 ID.RA-08 PR.PS-02	Govern	Does the organization facilitate the implementation and monitoring of vulnerability management controls?	Process
Vulnerability & Patch Management	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	PR.PS-02	Protect	Does the organization define and manage the scope for its attack surface management activities?	Process
Vulnerability & Patch Management	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	ID.RA-08 PR.PS-02	Protect	Does the organization ensure that vulnerabilities are properly identified, tracked and remediated?	Process
Vulnerability & Patch Management	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	ID.RA-08	Identify	Does the organization identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information?	Process
Vulnerability & Patch Management	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	PR.PS-02	Protect	Does the organization conduct software patching for all deployed systems, applications and firmware?	Technology
Vulnerability & Patch Management	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	ID.RA-01	Detect	Does the organization detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications?	Process

SCF #	C|P-CMM 0 Not Performed	C|P-CMM 1 Performed Informally	C|P-CMM 2 Planned & Tracked	C|P-CMM 3 Well Defined	C|P-CMM 4 Quantitatively Controlled	C|P-CMM 5 Continuously Improving
TDA-06.1	There is no evidence of a capability to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	C|P-CMM1 is N/A, since a structured process is required to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	Technology Development & Acquisition (TDA) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following	Technology Development & Acquisition (TDA) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Technology Development & Acquisition (TDA) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined
TDA-06.2	There is no evidence of a capability to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	C|P-CMM1 is N/A, since a structured process is required to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	Technology Development & Acquisition (TDA) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following	Technology Development & Acquisition (TDA) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	See C|P-CMM3. There are no defined C|P-CMM4 criteria, since it is reasonable to assume a quantitatively-controlled process is not necessary to perform threat modelling and other secure design techniques, to ensure that threats to software and	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.
TDA-06.3	There is no evidence of a capability to utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the development of Technology Assets, Applications and/or Services (TAAS).	C|P-CMM1 is N/A, since a structured process is required to utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the development of Technology Assets, Applications and/or Services (TAAS).	C|P-CMM2 is N/A, since a well-defined process is required to utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the development of Technology Assets, Applications and/or Services (TAAS).	Technology Development & Acquisition (TDA) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	See C|P-CMM3. There are no defined C|P-CMM4 criteria, since it is reasonable to assume a quantitatively-controlled process is not necessary to utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the development of Technology Assets,
TDA-09	There is no evidence of a capability to require system developers/integrators consult with cybersecurity and data protection personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;	Technology Development & Acquisition (TDA) efforts are ad hoc and inconsistent. CMM Level 1 control maturity would reasonably expect all, or at least most, the following criteria to exist: •IT personnel use an informal process to govern	Technology Development & Acquisition (TDA) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following	Technology Development & Acquisition (TDA) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Technology Development & Acquisition (TDA) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to require system developers/integrators consult with cybersecurity and data protection personnel to:
TDA-09.1	There is no evidence of a capability to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a plan for the continuous monitoring of cybersecurity and data protection control effectiveness.	Technology Development & Acquisition (TDA) efforts are ad hoc and inconsistent. CMM Level 1 control maturity would reasonably expect all, or at least most, the following criteria to exist: •IT personnel use an informal process to govern	Technology Development & Acquisition (TDA) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following	Technology Development & Acquisition (TDA) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Technology Development & Acquisition (TDA) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a plan for the continuous monitoring of
TDA-14	There is no evidence of a capability to require system developers and integrators to perform configuration management during system design, development, implementation and operation.	C|P-CMM1 is N/A, since a structured process is required to require system developers and integrators to perform configuration management during system design, development, implementation and operation.	Technology Development & Acquisition (TDA) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following	Technology Development & Acquisition (TDA) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Technology Development & Acquisition (TDA) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to require system developers and integrators to perform configuration management during system design, development, implementation and
TDA-14.1	There is no evidence of a capability to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of software and firmware components.	C|P-CMM1 is N/A, since a structured process is required to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of software and firmware components.	Technology Development & Acquisition (TDA) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following	Technology Development & Acquisition (TDA) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Technology Development & Acquisition (TDA) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	Technology Development & Acquisition (TDA) efforts are "world-class" capabilities that leverage predictive analysis (e.g., machine learning, AI, etc.). In addition to CMM Level 4 criteria, CMM Level 5 control maturity would reasonably expect all, or at least most, the following criteria to exist:
TDA-14.2	There is no evidence of a capability to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of hardware components.	C|P-CMM1 is N/A, since a structured process is required to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of hardware components.	C|P-CMM2 is N/A, since a well-defined process is required to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of hardware components.	Technology Development & Acquisition (TDA) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	See C|P-CMM3. There are no defined C|P-CMM4 criteria, since it is reasonable to assume a quantitatively-controlled process is not necessary to require developers of Technology Assets, Applications and/or Services (TAAS) to enable	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of hardware components.
TDA-17	There is no evidence of a capability to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the	C|P-CMM1 is N/A, since a structured process is required to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the	Technology Development & Acquisition (TDA) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following	Technology Development & Acquisition (TDA) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Technology Development & Acquisition (TDA) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by:
TPM-01	There is no evidence of a capability to facilitate the implementation of third-party management controls.	Third-Party Management (TPM) efforts are ad hoc and inconsistent. CMM Level 1 control maturity would reasonably expect all, or at least most, the following criteria to exist: •Third-party management is decentralized.	Third-Party Management (TPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Third-Party Management (TPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Third-Party Management (TPM) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to facilitate the implementation of third-party management controls.
TPM-01.1	There is no evidence of a capability to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of its Technology Assets, Applications,	C|P-CMM1 is N/A, since a structured process is required to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of its Technology	Third-Party Management (TPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Third-Party Management (TPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	See C|P-CMM3. There are no defined C|P-CMM4 criteria, since it is reasonable to assume a quantitatively-controlled process is not necessary to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity,
TPM-02	There is no evidence of a capability to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery	C|P-CMM1 is N/A, since a structured process is required to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery	Third-Party Management (TPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Third-Party Management (TPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Third-Party Management (TPM) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain
TPM-03	There is no evidence of a capability to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the	C|P-CMM1 is N/A, since a structured process is required to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and	Third-Party Management (TPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Third-Party Management (TPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Third-Party Management (TPM) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the
TPM-03.2	There is no evidence of a capability to utilize security safeguards to limit harm from potential adversaries who identify and target its supply chain.	C|P-CMM1 is N/A, since a structured process is required to utilize security safeguards to limit harm from potential adversaries who identify and target its supply chain.	Third-Party Management (TPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Third-Party Management (TPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Third-Party Management (TPM) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to utilize security safeguards to limit harm from potential adversaries who identify and target its supply chain.
TPM-03.3	There is no evidence of a capability to address identified weaknesses or deficiencies in the security of the supply chain	C|P-CMM1 is N/A, since a structured process is required to address identified weaknesses or deficiencies in the security of the supply chain	Third-Party Management (TPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Third-Party Management (TPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Third-Party Management (TPM) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to address identified weaknesses or deficiencies in the security of the supply chain
TPM-04	There is no evidence of a capability to mitigate the risks associated with third-party access to its Technology Assets, Applications, Services and/or Data (TAASD).	C|P-CMM1 is N/A, since a structured process is required to mitigate the risks associated with third-party access to its Technology Assets, Applications, Services and/or Data (TAASD).	Third-Party Management (TPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Third-Party Management (TPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Third-Party Management (TPM) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to mitigate the risks associated with third-party access to its Technology Assets, Applications, Services and/or Data (TAASD).
TPM-04.1	There is no evidence of a capability to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	C|P-CMM1 is N/A, since a structured process is required to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	Third-Party Management (TPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Third-Party Management (TPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Third-Party Management (TPM) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services
TPM-04.3	There is no evidence of a capability to ensure that the interests of third-party service providers are consistent with and reflect organizational interests.	Third-Party Management (TPM) efforts are ad hoc and inconsistent. CMM Level 1 control maturity would reasonably expect all, or at least most, the following criteria to exist: •Third-party management is decentralized.	Third-Party Management (TPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Third-Party Management (TPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Third-Party Management (TPM) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to ensure that the interests of third-party service providers are consistent with and reflect organizational interests.
TPM-04.4	There is no evidence of a capability to restrict the location of information processing/storage based on business requirements.	C|P-CMM1 is N/A, since a structured process is required to restrict the location of information processing/storage based on business requirements.	Third-Party Management (TPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Third-Party Management (TPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Third-Party Management (TPM) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to restrict the location of information processing/storage based on business requirements.
TPM-05	There is no evidence of a capability to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting its needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	Third-Party Management (TPM) efforts are ad hoc and inconsistent. CMM Level 1 control maturity would reasonably expect all, or at least most, the following criteria to exist: •Third-party management is decentralized.	Third-Party Management (TPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Third-Party Management (TPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Third-Party Management (TPM) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting its needs to
TPM-05.2	There is no evidence of a capability to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	C|P-CMM1 is N/A, since a structured process is required to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	Third-Party Management (TPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Third-Party Management (TPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	See C|P-CMM3. There are no defined C|P-CMM4 criteria, since it is reasonable to assume a quantitatively-controlled process is not necessary to ensure cybersecurity and data protection requirements are included in contracts that flow-	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.
TPM-05.3	There is no evidence of a capability to ensure External Service Providers (ESPs) use unique authentication factors for each of its customers.	C|P-CMM1 is N/A, since a structured process is required to ensure External Service Providers (ESPs) use unique authentication factors for each of its customers.	Third-Party Management (TPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Third-Party Management (TPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	See C|P-CMM3. There are no defined C|P-CMM4 criteria, since it is reasonable to assume a quantitatively-controlled process is not necessary to ensure External Service Providers (ESPs) use unique authentication factors for each of its customers.	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to ensure External Service Providers (ESPs) use unique authentication factors for each of its customers.
TPM-05.4	There is no evidence of a capability to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between	C|P-CMM1 is N/A, since a structured process is required to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data	Third-Party Management (TPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Third-Party Management (TPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	See C|P-CMM3. There are no defined C|P-CMM4 criteria, since it is reasonable to assume a quantitatively-controlled process is not necessary to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to
TPM-05.5	There is no evidence of a capability to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity and data protection control	C|P-CMM1 is N/A, since a structured process is required to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity and data protection control	Third-Party Management (TPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Third-Party Management (TPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	See C|P-CMM3. There are no defined C|P-CMM4 criteria, since it is reasonable to assume a quantitatively-controlled process is not necessary to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to
TPM-05.6	There is no evidence of a capability to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for	C|P-CMM1 is N/A, since a structured process is required to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for	Third-Party Management (TPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Third-Party Management (TPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	See C|P-CMM3. There are no defined C|P-CMM4 criteria, since it is reasonable to assume a quantitatively-controlled process is not necessary to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPs) that provides	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified
TPM-05.7	There is no evidence of a capability to include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or data protection controls.	C|P-CMM1 is N/A, since a structured process is required to include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or data protection controls.	Third-Party Management (TPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Third-Party Management (TPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	See C|P-CMM3. There are no defined C|P-CMM4 criteria, since it is reasonable to assume a quantitatively-controlled process is not necessary to include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or data	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or data protection controls.
TPM-06	There is no evidence of a capability to control personnel security requirements including security roles and responsibilities for third-party providers.	Third-Party Management (TPM) efforts are ad hoc and inconsistent. CMM Level 1 control maturity would reasonably expect all, or at least most, the following criteria to exist: •Third-party management is decentralized.	Third-Party Management (TPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Third-Party Management (TPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Third-Party Management (TPM) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to control personnel security requirements including security roles and responsibilities for third-party providers.
TPM-08	There is no evidence of a capability to monitor, regularly review and audit Third-Party Service Providers (TSP) for compliance with established contractual requirements for cybersecurity and data protection controls.	C|P-CMM1 is N/A, since a structured process is required to monitor, regularly review and audit Third-Party Service Providers (TSP) for compliance with established contractual requirements for cybersecurity and data protection controls.	Third-Party Management (TPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Third-Party Management (TPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Third-Party Management (TPM) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to monitor, regularly review and audit Third-Party Service Providers (TSP) for compliance with established contractual requirements for
TPM-09	There is no evidence of a capability to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	C|P-CMM1 is N/A, since a structured process is required to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	Third-Party Management (TPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Third-Party Management (TPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Third-Party Management (TPM) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such
TPM-10	There is no evidence of a capability to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	C|P-CMM1 is N/A, since a structured process is required to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	Third-Party Management (TPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Third-Party Management (TPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Third-Party Management (TPM) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data
TPM-11	There is no evidence of a capability to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	C|P-CMM1 is N/A, since a structured process is required to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	Third-Party Management (TPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Third-Party Management (TPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Third-Party Management (TPM) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to ensure response/recovery planning and testing are conducted with critical suppliers/providers.
THR-01	There is no evidence of a capability to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions,	Threat Management (THR) efforts are ad hoc and inconsistent. CMM Level 1 control maturity would reasonably expect all, or at least most, the following criteria to exist: •Threat management is decentralized.	Threat Management (THR) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to exist:	Threat Management (THR) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following criteria to	Threat Management (THR) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for improvement. In	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of
THR-02	There is no evidence of a capability to develop Indicators of Exposure (IOE) to understand the potential attack vectors that attackers could use to attack the organization.	C|P-CMM1 is N/A, since a structured process is required to develop Indicators of Exposure (IOE) to understand the potential attack vectors that attackers could use to attack the organization.	Threat Management (THR) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to exist:	Threat Management (THR) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following criteria to	Threat Management (THR) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for improvement. In	Threat Management (THR) efforts are "world-class" capabilities that leverage predictive analysis (e.g., machine learning, AI, etc.). In addition to CMM Level 4 criteria, CMM Level 5 control maturity would reasonably expect all, or at least most, the following criteria to exist:
THR-03	There is no evidence of a capability to maintain situational awareness of evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating	Threat Management (THR) efforts are ad hoc and inconsistent. CMM Level 1 control maturity would reasonably expect all, or at least most, the following criteria to exist: •Threat management is decentralized.	Threat Management (THR) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to exist:	Threat Management (THR) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following criteria to	Threat Management (THR) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for improvement. In	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to maintain situational awareness of evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the
THR-04	There is no evidence of a capability to implement an insider threat program that includes a cross-discipline insider threat incident handling team.	Threat Management (THR) efforts are ad hoc and inconsistent. CMM Level 1 control maturity would reasonably expect all, or at least most, the following criteria to exist: •Threat management is decentralized.	Threat Management (THR) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to exist:	Threat Management (THR) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following criteria to	Threat Management (THR) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for improvement. In	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to implement an insider threat program that includes a cross-discipline insider threat incident handling team.
THR-05	There is no evidence of a capability to utilize security awareness training on recognizing and reporting potential indicators of insider threat.	Threat Management (THR) efforts are ad hoc and inconsistent. CMM Level 1 control maturity would reasonably expect all, or at least most, the following criteria to exist: •Threat management is decentralized.	Threat Management (THR) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to exist:	Threat Management (THR) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following criteria to	Threat Management (THR) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for improvement. In	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to utilize security awareness training on recognizing and reporting potential indicators of insider threat.
THR-07	There is no evidence of a capability to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	C|P-CMM1 is N/A, since a structured process is required to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	Threat Management (THR) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to exist:	Threat Management (THR) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following criteria to	See C|P-CMM3. There are no defined C|P-CMM4 criteria, since it is reasonable to assume a quantitatively-controlled process is not necessary to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.
THR-09	There is no evidence of a capability to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	C|P-CMM1 is N/A, since a structured process is required to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	Threat Management (THR) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to exist:	Threat Management (THR) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following criteria to	See C|P-CMM3. There are no defined C|P-CMM4 criteria, since it is reasonable to assume a quantitatively-controlled process is not necessary to develop and keep current a catalog of applicable internal and external threats to the organization, both	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.
THR-10	There is no evidence of a capability to embed false data or steganographic data in files to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	C|P-CMM1 is N/A, since a structured process is required to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	Threat Management (THR) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to exist:	Threat Management (THR) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following criteria to	See C|P-CMM3. There are no defined C|P-CMM4 criteria, since it is reasonable to assume a quantitatively-controlled process is not necessary to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.
VPM-01	There is no evidence of a capability to facilitate the implementation and monitoring of vulnerability management controls.	Vulnerability & Patch Management (VPM) efforts are ad hoc and inconsistent. CMM Level 1 control maturity would reasonably expect all, or at least most, the following criteria to exist: •Attack Surface Management (ASM) is decentralized.	Vulnerability & Patch Management (VPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Vulnerability & Patch Management (VPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Vulnerability & Patch Management (VPM) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to facilitate the implementation and monitoring of vulnerability management controls.
VPM-01.1	There is no evidence of a capability to define and manage the scope for its attack surface management activities.	Vulnerability & Patch Management (VPM) efforts are ad hoc and inconsistent. CMM Level 1 control maturity would reasonably expect all, or at least most, the following criteria to exist: •Attack Surface Management (ASM) is decentralized.	Vulnerability & Patch Management (VPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Vulnerability & Patch Management (VPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	See C|P-CMM3. There are no defined C|P-CMM4 criteria, since it is reasonable to assume a quantitatively-controlled process is not necessary to define and manage the scope for its attack surface management activities.	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to define and manage the scope for its attack surface management activities.
VPM-02	There is no evidence of a capability to ensure that vulnerabilities are properly identified, tracked and remediated.	C|P-CMM1 is N/A, since a structured process is required to ensure that vulnerabilities are properly identified, tracked and remediated.	Vulnerability & Patch Management (VPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Vulnerability & Patch Management (VPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Vulnerability & Patch Management (VPM) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	Vulnerability & Patch Management (VPM) efforts are "world-class" capabilities that leverage predictive analysis (e.g., machine learning, AI, etc.). In addition to CMM Level 4 criteria, CMM Level 5 control maturity would reasonably expect all, or at least most, the following criteria to exist:
VPM-03	There is no evidence of a capability to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	C|P-CMM1 is N/A, since a structured process is required to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	Vulnerability & Patch Management (VPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Vulnerability & Patch Management (VPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Vulnerability & Patch Management (VPM) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	See C|P-CMM4. There are no defined C|P-CMM5 criteria, since it is reasonable to assume a continuously-improving process is not necessary to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability
VPM-05	There is no evidence of a capability to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	Vulnerability & Patch Management (VPM) efforts are ad hoc and inconsistent. CMM Level 1 control maturity would reasonably expect all, or at least most, the following criteria to exist: •Attack Surface Management (ASM) is decentralized.	Vulnerability & Patch Management (VPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Vulnerability & Patch Management (VPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Vulnerability & Patch Management (VPM) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	Vulnerability & Patch Management (VPM) efforts are "world-class" capabilities that leverage predictive analysis (e.g., machine learning, AI, etc.). In addition to CMM Level 4 criteria, CMM Level 5 control maturity would reasonably expect all, or at least most, the following criteria to exist:
VPM-06	There is no evidence of a capability to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	Vulnerability & Patch Management (VPM) efforts are ad hoc and inconsistent. CMM Level 1 control maturity would reasonably expect all, or at least most, the following criteria to exist: •Attack Surface Management (ASM) is decentralized.	Vulnerability & Patch Management (VPM) efforts are requirements-driven and governed at a local/regional level, but are not consistent across the organization. CMM Level 2 control maturity would reasonably expect all, or at least most, the following criteria to	Vulnerability & Patch Management (VPM) efforts are standardized across the organization and centrally managed, where technically feasible, to ensure consistency. CMM Level 3 control maturity would reasonably expect all, or at least most, the following	Vulnerability & Patch Management (VPM) efforts are metrics driven and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for	Vulnerability & Patch Management (VPM) efforts are "world-class" capabilities that leverage predictive analysis (e.g., machine learning, AI, etc.). In addition to CMM Level 4 criteria, CMM Level 5 control maturity would reasonably expect all, or at least most, the following criteria to exist:

SCF #	AICPA TSC 2017:2022 (used for SOC 2)	CIS CSC 8.1	CSA CCM 4	ISO 27001 2022	ISO 27002 2022	ISO 27017 2015	ISO 27018 2014	ISO 27701 2025	ISO 29100 2024	ISO 42001 2023	NIST Privacy Framework 1.0	NIST 800-53 R5	NIST 800-161 R1	NIST 800-218	NIST CSF 2.0	PCI DSS 4.0.1	US FAR 52.204-21	US FFIEC	US FINRA	US GLBA CFR 314 2023
TDA-06.1	PI1.1				8.29						ID.BE-P3	PM-30(1) RA-9 SA-15(3)	RA-9 SA-15(3)	PW.1	PR.PS-06					
TDA-06.2		16.2 16.14										SA-11(2) SA-15(8)	SA-15(4) SA-15(8)	PW.1 PW.1.1 RV.2.2	GV.OC-01 PR.PS-06					
TDA-06.3		16.1 16.5 16.11												PW.1 PW.2 PW.4.2	PR.PS-06	6.2.2				
TDA-09	CC4.1-POF1	16.2 16.3 16.12	AIS-05 TVM-03		8.25 8.29 8.30	14.2.7 14.2.8 14.2.9					CT.DM-P9 CT.DM-P10	SA-11 SA-11(5) SA-11(6) SA-11(7)	SA-11	PO.4 PO.4.1 PW.5.1 PW.6 PW.7	ID.IM-01 ID.IM-02 ID.RA-01 PR.PS-06	6.2.3 6.2.3.1 6.2.4 6.5.6				
TDA-09.1		16.2										SA-4(8)	SA-4(8)	RV.1	ID.IM-01 ID.IM-02					
TDA-14		16.11			8.30 8.32	14.2.4						SA-10	SA-10		ID.RA-09					
TDA-14.1		16.5 16.11									PR.DS-P6	SA-10(1)			ID.RA-09					
TDA-14.2												SA-10(3)			ID.RA-09					
TDA-17		2.2										SA-22	SA-22		PR.PS-02 PR.PS-03					
TPM-01	CC1.1-POF5 CC1.4-POF2 CC1.4-POF3 CC2.3-POF10 CC2.3-POF12	15 15.2	IAM-11 SEF-02 STA-01 STA-02 STA-03		5.19 5.20 8.30	15.1.1		6.1.3(h)		A.10 A.10.2 A.10.3	GV.PO-P4	SA-4 SR-1	SA-4 SR-1		GV.SC-04 GV.SC-06 GV.SC-07 GV.SC-08 GV.SC-10	8.2.3 12.8 12.8.1 12.9 12.9.1	52.204-21(b)(1)(ii)			314.4(e) 314.4(a)(1) 314.4(a)(2) 314.4(a)(3) 314.4(f)
TPM-01.1	CC2.1-POF6	15.1			5.19								SR-13		GV.SC-04 GV.SC-07 GV.SC-08 ID.AM ID.AM-01	12.8 12.8.1				
TPM-02	CC3.2-POF8 CC3.2-POF9 CC9.1	15.3	STA-07		5.19						ID.BE-P3	PM-30(1) RA-9 SA-9(3)	RA-9		GV.OC-04 GV.OC-05 GV.SC-04 GV.SC-06 GV.SC-07			D1.G.SP.A.3		314.4(f)(1)
TPM-03	CC1.1-POF5 CC3.2-POF7 CC9.1 CC9.2-POF1 CC9.2-POF10		IAM-11 STA-02 STA-03 STA-13		5.19 5.21 5.22 8.30	15.1.3				A.10 A.10.2 A.10.3		SA-9(3) SR-2 SR-2(1)	SA-9(3) SR-2		GV.SC GV.SC-06 GV.SC-07					314.4(f)(1)
TPM-03.2	CC9.1 P6.4-POF2 P6.5-POF1 P6.5-POF2 P6.6-POF1	15.4	STA-13		5.19 5.20							SR-3(2)			GV.SC-06 GV.SC-07					314.4(f)(1)
TPM-03.3	CC9.1				5.19 5.22							SR-3	SR-3		GV.SC-06 GV.SC-07					
TPM-04	CC3.3	15.4 15.5	IAM-11 STA-02 UEM-14		5.19 8.30	14.2.7 15.1.1				A.10 A.10.2 A.10.3		SA-9	SA-9		GV.SC-06 GV.SC-07	8.2.3 12.8.2 12.9 12.9.1 12.9.2				314.4(f)(1) 314.4(f)(2) 314.4(f)(3)
TPM-04.1	CC3.2-POF8 CC3.2-POF9 CC3.4 CC9.2 CC9.2-POF11	15.5	STA-05 STA-13		5.19						ID.DE-P5	SA-9(1)	SA-9(1)		GV.SC-06 GV.SC-07 ID.IM-01 ID.IM-02 ID.RA-10	12.8.3				314.4(f)(1) 314.4(f)(3)
TPM-04.3	CC1.3-POF6 CC3.3				5.19							SA-9(4)	SA-9(4)		GV.SC-06					
TPM-04.4	CC2.1-POF9 CC9.1				5.21	6.1.3						PE-23 SA-9(5)	SA-9(5)		GV.SC-06	3.2.1 12.5.2				314.4(f)(1)
TPM-05	CC1.1-POF5 CC2.3-POF10 CC2.3-POF11 CC2.3-POF12 CC2.3-POF2	15.4	IPY-04 SEF-02 STA-02 STA-04 STA-09		5.19 5.20 5.21 5.31 6.6	5.1.1 CLD.6.3.1 13.1.2 13.2.4 15.1.2		6.1.3(h)		A.10.2 A.10.3	ID.DE-P3 GV.PO-P4 GV.AT-P4	SR-3(3)	SA-9(3)	PO.1	GV.OC-02 GV.OC-03 GV.SC-02 GV.SC-05 GV.SC-06	8.2.3 12.4.2 12.4.2.1 12.8.2 12.8.5	52.204-21(b)(1)(ii)			314.4(e) 314.4(a)(1) 314.4(a)(2) 314.4(a)(3)
TPM-05.2	CC2.3-POF12 CC9.2-POF1 CC9.2-POF10 CC9.2-POF9 P6.4-POF3							6.1.3(h)				SR-3(3)	SR-3(3)		GV.OC-03 GV.SC-02 GV.SC-05 GV.SC-06 GV.SC-10		52.204-21(b)(1)(ii)			
TPM-05.3															GV.SC-06 GV.SC-10	8.2.3				
TPM-05.4	CC1.1-POF5 CC1.3-POF3 CC1.3-POF4 CC1.3-POF5 CC2.2-POF5	15		4.3(c)	5.2 5.23	5.1.1 6.1.1 CLD.6.3.1				5.3 A.10 A.10.2 A.10.3 A.10.4		SA-9(3)	SA-9(3)		GV.OC GV.OC-02 GV.RM-05 GV.RR GV.RR-02	12.4.1 12.8.2 12.8.5 12.9 12.9.1				
TPM-05.5	CC2.2-POF9 CC3.4-POF5 CC9.2-POF12 CC9.2-POF7	15								4.3					GV.SC-06	12.5.2.1 12.5.3 12.8 12.8.1 A3.2.1				
TPM-05.6	CC3.2-POF8 CC9.2-POF10 CC9.2-POF11 CC9.2-POF12 CC9.2-POF9														GV.SC-06					
TPM-05.7	CC9.2-POF8 CC9.2-POF9 P6.4-POF2 P6.5-POF1 P6.5-POF2											SA-9(3)	SA-9(3)		GV.SC-06					
TPM-06	CC1.1-POF5 CC9.1		STA-04		5.2 5.19 8.30	6.1.1					ID.IM-P2 GV.PO-P4 GV.AT-P4				GV.SC-06 ID.AM			D1.G.SP.B.7 D4.RM.Co.B.2 D4.RM.Co.B.5		
TPM-08	CC1.4-POF2 CC1.4-POF3 CC3.4 CC3.4-POF5 CC9.1	15 15.6	STA-05 STA-07 STA-10 STA-11 STA-13		5.19 5.20 5.22 8.21	13.1.2 15.2.1						SR-6 SR-6(1)	SR-6		GV.SC-07 ID.IM-01 ID.IM-02	12.4.2 12.4.2.1 12.8.4				314.4(f)(3)
TPM-09	CC4.2 CC9.1 CC9.2-POF8 P6.4-POF2 P6.5-POF1		SEF-02 SEF-06		5.19										GV.SC-06 GV.SC-07 GV.SC-08					
TPM-10	CC3.4 CC3.4-POF5 CC9.1 CC9.2-POF8	15.7	STA-05 STA-10 STA-13		5.20 5.22	15.2.2						SA-4	SA-4		GV.SC-08					
TPM-11	CC7.3 P6.5 P6.6		SEF-02 SEF-06		5.19							IR-4(10)	IR-4(10)		GV.SC-08	10.7 10.7.1 10.7.2 10.7.3				
THR-01	CC3.2-POF6 CC3.2-POF7 CC3.3 CC3.3-POF1 CC3.3-POF2				5.7							PM-15 PM-16	AT-3(8) PM-15 PM-16		DE DE.AE-07 ID.RA-03 ID.RA-08	6.3		D1.G.SP.Inn.1		
THR-02	CC3.2-POF6 CC3.2-POF7 CC3.3 CC9.2-POF13				5.7										DE DE.CM ID.RA-03 ID.RA-05 ID.RA-08					
THR-03	CC3.2-POF6 CC3.2-POF7 CC9.2-POF13			7.4 7.4(a) 7.4(b) 7.4(c) 7.4(d)	5.7							PM-16(1) SI-5 SI-5(1)	AT-3(8) SI-5		DE DE.AE-07 ID.RA-02 ID.RA-03 ID.RA-08	6.3.1		D2.TI.Ti.B.1		
THR-04	CC3.3 CC3.3-POF1 CC3.3-POF2 CC3.3-POF3 CC3.3-POF4											PM-12	PM-12		ID.RA-03					
THR-05												AT-2(2)	AT-2(2)		ID.RA-03					
THR-07												RA-10 SC-48	RA-10		DE ID.RA-03					
THR-09	A1.2-POF11 CC3.2-POF6 CC9.1														DE ID.RA-03 ID.RA-04 ID.RA-05 PR.IR-02					
THR-10	A1.2-POF11 CC3.2-POF6 CC3.2-POF9 CC3.4-POF6														DE DE.AE-07 ID.RA-04 ID.RA-05					
VPM-01	CC3.2-POF7 CC3.2-POF9 CC3.4-POF6 CC6.1-POF14 CC6.1-POF16	7 7.1 18	AIS-07 TVM-01 TVM-02 UEM-07		8.8	12.6.1					PR.PO-P10	SI-2 SI-3	SI-2 SI-3		ID.RA-01 ID.RA-08 PR.PS-02	6.3 6.3.1 6.3.3 11.3	52.204-21(b)(1)(xii)	D2.TI.Ti.B.2 D3.DC.Th.B.1 D1.RM.RA.E.2 D3.DC.Th.E.5 D3.DC.Th.A.1		314.4(d)(2)
VPM-01.1	CC2.2-POF9 CC3.2-POF7 CC3.2-POF9 CC3.4-POF6 CC9.2-POF13		TVM-07		8.8					4.3		SA-11(6) SA-11(7)			PR.PS-02	6.3.1 6.3.2 11.3.1 11.3.1.1 11.3.1.2				
VPM-02	CC4.2 CC5.3-POF4 CC7.4-POF8	7.2 7.7	AIS-07 TVM-03		8.8	12.6.1				10.2 10.2(a) 10.2(a)(1) 10.2(a)(2) 10.2(b)		PM-4 SC-18(1)	PM-4	RV.2.2	ID.RA-08 PR.PS-02	11.3 11.3.1 11.3.1.1 11.3.1.2 11.3.1.3	52.204-21(b)(1)(xiii)			
VPM-03	CC3.4-POF6		TVM-08		8.8										ID.RA-08	6.3.1 11.3				
VPM-05	CC6.1-POF14 CC6.1-POF16	7.3 7.4 12.1 18.3	UEM-07		8.8	12.6.1						SI-2 SI-2(4) SI-3	SI-2 SI-3		PR.PS-02	6.3.3	52.204-21(b)(1)(xii)			
VPM-06	CC3.2-POF7 CC3.4-POF6 CC7.1 CC7.1-POF5 CC9.2-POF13	7.5 7.6	TVM-03 TVM-07		8.8							RA-5	RA-5		ID.RA-01	6.4.1 11.3 11.3.1 11.3.1.1 11.3.1.2		D3.DC.Th.E.5		314.4(d)(2) 314.4(d)(2)(ii)

SCF #	US HIPAA Administrative Simplification 2013	US HIPAA Security Rule / NIST SP 800-66 R2	US HIPAA HICP Small Practice	US HIPAA HICP Medium Practice	US HIPAA HICP Large Practice	US SEC Cybersecurity Rule	US-MA 201 CMR 17.00	US-NY DFS 23 NYCRR500 2023 Amd 2	US-OR 646A	US-OR CPA	US-TX SB 2610	EMEA EU DORA	EMEA EU GDPR	EMEA EU NIS2	EMEA EU NIS2 Annex	APAC India SEBI CSCRF	APAC New Zealand HISF 2022	APAC New Zealand HISF Suppliers 2023	APAC New Zealand NZISM 3.6	Americas Canada OSFI B-13	Americas Canada PIPEDA	SCF CORE Fundamentals
TDA-06.1																			14.4.6.C.01 14.4.6.C.02 14.4.6.C.03	2.4.5		
TDA-06.2																			14.4.6.C.01 14.4.6.C.02 14.4.6.C.03	2.4.4 3.1.6		
TDA-06.3																						
TDA-09							17.03(2)(d)(B)(i)	500.8(a)							6.2.2(d) 6.5.1	PR.IP.S6				3.2.9		
TDA-09.1																						
TDA-14							17.03(2)(d)(B)(i)															
TDA-14.1															6.6.1(c)							
TDA-14.2																						
TDA-17																	HHSP43 HML43		12.4.7.C.01	2.2.5		
TPM-01	164.308(b)(1) 164.312(d)	164.308(b)(1) 164.312(d)			9.L.C	17 CFR 229.106(b)(1)(iii)		500.11(a) 500.11(a)(1) 500.11(b) 500.3(i) 500.4(a)(1)				30.3(and) 31.12		21.2(d) 21.2(e) 21.3	6.2.3	GV.SC.S3 GV.SC.S1 PR.IP.S15	HHSP25 HML25 HSUP67	HSUP67	2.2.6.C.01 2.2.6.C.02 23.2.19.C.01			
TPM-01.1								500.11(a)(1)				28.1 28.1(a) 28.1(b) 28.1(b)(i) 28.1(b)(ii)		21.3	5.2 5.2(a)	GV.OC.S3 GV.SC.S1 GV.SC.S2						TPM-01.1
TPM-02	164.308(a)(7)(ii)(E)	164.308(a)(7)(ii)(E)			9.L.C	17 CFR 229.106(b)(1)(iii)		500.11(a)(1) 500.11(a)(4)				8.4		21.3		GV.OC.S3 GV.SC.S1 GV.SC.S2			12.7.17.C.01			
TPM-03			5.S.B	5.M.B	5.M.B 9.L.C	17 CFR 229.106(b)(1)(iii)						30.3(f)		21.2(d) 21.3	5.1.6	GV.OC.S3 GV.SC.S1			12.7.14.C.01 12.7.14.C.02 12.7.14.C.03 12.7.15.C.01 12.7.15.C.02			TPM-03
TPM-03.2					9.L.C									21.3								
TPM-03.3														21.3								
TPM-04	164.308(b)(1)	164.308(b)(1)			9.L.C		17.03(2)(f)(1)	500.11(a)(1)	622(2)(d)(A)(v)			29.1		21.3								
TPM-04.1					9.L.C		17.03(2)(f)(2)	500.11(a)(1) 500.11(a)(3)	622(2)(d)(A)(v)			28.4(a) 28.4(b) 28.4(c) 28.4(d) 28.4(e)		21.3	2.1.2(d)		HHSP25 HML25 HSUP67	HSUP67				
TPM-04.3					9.L.C																	
TPM-04.4					9.L.C									21.3							Sec 20	
TPM-05	164.308(b)(1) 164.308(b)(2) 164.308(b)(3) 164.314(a)(2)(iii) 164.314(b)(1)	164.308(b)(1) 164.308(b)(2) 164.308(b)(3) 164.314(a)(2)(iii) 164.314(b)(1)			9.L.C	17 CFR 229.106(b)(1)(iii)		500.10(a)(1) 500.10(b) 500.11(a)(1) 500.11(a)(2) 500.11(b)		6(2)(a) 6(2)(b) 6(2)(c) 6(2)(d) 6(2)(e)		28.1(a) 29.2 30.1 30.2 30.2(a)		21.3	1.2.2 13.1.2(a) 3.3.2 4.3.2(a) 5.1.2	GV.OC.S3 GV.SC.S3 GV.SC.S3 GV.SC.S8 PR.AT.S3	HHSP09 HHSP36 HHSP72 HML09 HML36	HSUP63 HSUP68	2.3.30.C.01 23.2.19.C.01			TPM-05
TPM-05.2	164.308(b)(1) 164.308(b)(2) 164.314(a)(2)(i)(B) 164.314(a)(2)(iii) 164.502(e)(1)(ii)	164.308(b)(1) 164.308(b)(2) 164.314(a)(2)(i)(B) 164.314(a)(2)(iii)						500.10(a)(1) 500.11(a)(1) 500.11(a)(2) 500.11(b) 500.11(b)(1)				29.2		21.3	5.1.4(g)	GV.SC.S3 GV.SC.S8						
TPM-05.3								500.11(b)(1)														
TPM-05.4	164.308(b)(1)	164.308(b)(1)				17 CFR 229.106(b)(1)(ii)		500.10(a)(1) 500.10(b) 500.2(d) 500.4(a)(1) 500.4(a)(2)						21.3	10.1.2(a) 4.3.2(a) 8.1.1	GV.OC.S3 GV.SC.S3 PR.AT.S3						TPM-05.4
TPM-05.5								500.11(a)(3) 500.11(a)(4)						21.3								
TPM-05.6	164.308(b)(2) 164.502(e)(1)(i) 164.502(e)(1)(ii)	164.308(b)(2)						500.11(a)(3) 500.11(b)(4) 500.4(b)(1) 500.4(b)(2) 500.4(b)(3)						21.3		PR.IP.S5						
TPM-05.7	164.504(e)(2)(iii)											28.7 28.7(a) 28.7(b) 28.7(c) 28.7(d)		21.3		GV.SC.S3						
TPM-06					9.L.C			500.10(b)						21.3	10.2.1 5.1.4(c)	PR.AT.S3						
TPM-08					9.L.C			500.11(a)(3) 500.11(a)(4)				28.6 30.3(e)		21.3	5.1.7(a) 5.1.7(b) 5.1.7(c)	GV.SC.S4	HHSP25 HHSP73 HML25 HML73 HMS04	HSUP64 HSUP67				TPM-08
TPM-09					9.L.C			500.4(b)(6)						21.3 21.4		GV.SC.S4						
TPM-10					9.L.C		17.03(2)(d)(B)(i)							21.3	5.1.7(d)	GV.SC.S4						
TPM-11																						
THR-01			8.S.B					500.10(a)(2) 500.10(a)(3)				13.1 45.1 45.1(a) 45.1(b) 45.1(c)				EV.ST.S1				3.0 3.1 3.1.1 3.1.6		
THR-02																				3.1		
THR-03			8.S.B 8.M.C		7.L.A 8.L.B 9.L.D			500.9(b)(1)	622(2)(d)(B)(iii)			13.1			6.10.2(a)	EV.ST.S1 EV.ST.S4 ID.RA.S3 RS.AN.S1				3.0 3.1 3.1.1 3.1.5		
THR-04																				3.0		
THR-05																						
THR-07																DE.DP.S5				3.0		
THR-09	164.306(b)(2)(iv)	164.306(b)(2)(iv)						500.9(b)(1)							13.2.1					3.0 3.1.6		
THR-10	164.306(b)(2)(iv)	164.306(b)(2)(iv)				17 CFR 229.106(a)		500.9(b)(1)								ID.RA.S4				3.1 3.1.1 3.1.2 3.1.6		
VPM-01			2.S.A 7.S.A	2.M.A 7.M.D	2.M.A 7.M.D 7.L.A 7.L.B 9.L.A			500.3(e)				25.1 25.2 25.3 9.4(f)		21.2(e)	6.10.1 6.10.2(a) 6.10.2(d) 6.6.1	PR.IP.S12	HHSP19 HHSP26 HML19 HML26 HSUP17	HSUP17	6.2.4.C.01	2.6 3.1		
VPM-01.1								500.5(a)(1)											6.2.4.C.01			
VPM-02			2.S.A 7.S.A	2.M.A 7.M.D	2.M.A 7.M.D 7.L.B		17.03(2)(j)	500.4(b)(6) 500.5(c)	622(2)(d)(A)(i)					21.4	6.10.1 6.10.2(c) 6.10.3	PR.MA.S3	HHSP19 HHSP59 HML19 HML59 HSUP17	HSUP17 HSUP51	6.2.6.C.01 23.2.19.C.01	2.6		VPM-02
VPM-03				7.M.D	7.M.D			500.5(c)								PR.MA.S3				3.1.3		
VPM-05			2.S.A 7.S.A	2.M.A 7.M.D	2.M.A 7.M.D		17.04(6)		622(2)(d)(B)(iii)			9.4(f)			6.6.1(a)	PR.MA.S3	HHSP19 HML19 HSUP17	HSUP17	23.2.19.C.01	2.6 2.6.1 3.2.6		VPM-05
VPM-06			2.S.A 7.S.A	7.M.A 7.M.B	7.M.A 7.M.B 7.L.A 9.L.A 9.L.B			500.5(a)(2)	622(2)(B)(iii) 622(2)(d)(A)(iii)			25.1 25.2 25.3			6.10.2(b)	ID.RA.S1	HHSP26 HHSP59 HML26 HML59 HSUP51	HSUP51	6.2.5.C.01	3.1.2 3.1.3		VPM-06