SCF Domain	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	What Is The Current Maturity Level of This Control?	How Likely Is It For This Control To Fail To Operate As Expected?	What Is The Potential Impact If This Control Fails To Operate As Expected?	How Strong Are Compensating Controls To Reduce The Risk Associated With This Control?	Risk Assessment Notes *(Explanation of compensating factors to justify reduction in risk)*	*Risk Factor* *(unweighted)*		*Risk Factor* *(compensated & weighted)*	
Cybersecurity & Data Protection Governance	Publishing Cybersecurity & Data Protection Documentation	GOV-02	The third-party entity establishes, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	0 - Non-Existent	Highly Unlikely	Moderate	None		6	MODERATE	60	MODERATE
Cybersecurity & Data Protection Governance	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	The third-party entity assigns one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	1 - Performed Informally	Unlikely	Moderate	N/A		9	MODERATE	90	MODERATE
Cybersecurity & Data Protection Governance	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	The third-party entity compels data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	3 - Well Defined	Unlikely	Moderate	Moderate		9	MODERATE	40	MODERATE
Asset Management	Asset Inventories	AST-02	The third-party entity performs inventories of technology assets that: (1) Accurately reflects the current systems, applications and services in use; (2) Identifies authorized software products, including	2 - Planned & Tracked	Unlikely	Moderate	Minimal		9	MODERATE	73	MODERATE
Asset Management	Data Action Mapping	AST-02.8	The third-party entity create and maintain a map of technology assets where sensitive/regulated data is stored, transmitted or processed.	2 - Planned & Tracked	Unlikely	Moderate	Moderate		9	MODERATE	51	MODERATE
Asset Management	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	The third-party entity maintains network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network	3 - Well Defined	Highly Unlikely	Minor	Moderate		4	LOW	20	LOW
Asset Management	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	The third-party entity securely disposes of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	3 - Well Defined	Highly Unlikely	Moderate	Moderate		6	MODERATE	29	LOW
Asset Management	Bring Your Own Device (BYOD) Usage	AST-16	The third-party entity implement and governs a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	1 - Performed Informally	Possible	Minor	Minimal		8	MODERATE	72	MODERATE
Business Continuity & Disaster Recovery	Contingency Plan Testing & Exercises	BCD-04	The third-party entity conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	2 - Planned & Tracked	Possible	Moderate	Minimal		12	HIGH	58	MODERATE
Business Continuity & Disaster Recovery	Data Backups	BCD-11	The third-party entity create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	4 - Quantitatively Controlled	Highly Unlikely	Minor	Moderate		4	LOW	17	LOW
Change Management	Configuration Change Control	CHG-02	The third-party entity govern the technical configuration change control processes.	3 - Well Defined	Unlikely	Minor	Moderate		6	MODERATE	24	LOW
Change Management	Security Impact Analysis for Changes	CHG-03	The third-party entity analyze proposed changes for potential security impacts, prior to the implementation of the change.	4 - Quantitatively Controlled	Highly Unlikely	Moderate	Moderate		6	MODERATE	23	LOW
Cloud Security	Cloud Services	CLD-01	The third-party entity facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	0 - Non-Existent	Highly Unlikely	Insignificant	None		2	LOW	20	LOW
Cloud Security	Sensitive Data In Public Cloud Providers	CLD-10	The third-party entity limit and manage the storage of sensitive/regulated data in public cloud providers.	0 - Non-Existent	Highly Unlikely	Insignificant	None		2	LOW	12	LOW
Compliance	Statutory, Regulatory & Contractual Compliance	CPL-01	The third-party entity facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	4 - Quantitatively Controlled	Remote	Major	Significant		4	LOW	12	LOW
Configuration Management	System Hardening Through Baseline Configurations	CFG-02	The third-party entity develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	3 - Well Defined	Highly Unlikely	Moderate	Moderate		6	MODERATE	29	LOW
Configuration Management	Least Functionality	CFG-03	The third-party entity configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	2 - Planned & Tracked	Highly Unlikely	Moderate	Minimal		6	MODERATE	49	MODERATE
Continuous Monitoring	Reviews & Updates	MON-01.8	The third-party entity review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	2 - Planned & Tracked	Highly Unlikely	Moderate	Moderate		6	MODERATE	38	MODERATE
Continuous Monitoring	Content of Event Logs	MON-03	The third-party entity configure systems 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;	3 - Well Defined	Highly Unlikely	Moderate	Moderate		6	MODERATE	29	LOW
Continuous Monitoring	Anomalous Behavior	MON-16	The third-party entity detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	4 - Quantitatively Controlled	Highly Unlikely	Major	Significant		8	MODERATE	24	LOW
Cryptographic Protections	Transmission Confidentiality	CRY-03	The third-party entity protect the confidentiality of data being transmitted.	4 - Quantitatively Controlled	Remote	Moderate	Significant		3	LOW	9	LOW
Cryptographic Protections	Encrypting Data At Rest	CRY-05	The third-party entity prevent unauthorized disclosure of data at rest.	4 - Quantitatively Controlled	Remote	Minor	Significant		2	LOW	6	LOW
Cryptographic Protections	Cryptographic Key Management	CRY-09	The third-party entity facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	3 - Well Defined	Highly Unlikely	Moderate	Moderate		6	MODERATE	29	LOW
Data Classification & Handling	Sensitive / Regulated Data Protection	DCH-01.2	The third-party entity protect sensitive/regulated data wherever it is stored.	3 - Well Defined	Highly Unlikely	Moderate	Moderate		6	MODERATE	26	LOW
Data Classification & Handling	Defining Access Authorizations for Sensitive/Regulated Data	DCH-01.4	The third-party entity explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive/regulated data.	3 - Well Defined	Highly Unlikely	Moderate	Moderate		6	MODERATE	26	LOW
Data Classification & Handling	Data & Asset Classification	DCH-02	The third-party entity ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	4 - Quantitatively Controlled	Highly Unlikely	Major	Significant		8	MODERATE	24	LOW
Data Classification & Handling	Use of External Information Systems	DCH-13	The third-party entity govern how external parties, systems and services are used to securely store, process and transmit data.	2 - Planned & Tracked	Unlikely	Minor	Moderate		6	MODERATE	34	LOW
Data Classification & Handling	Ad-Hoc Transfers	DCH-17	The third-party entity secure ad-hoc exchanges of large digital files with internal or external parties.	2 - Planned & Tracked	Highly Unlikely	Moderate	Moderate		6	MODERATE	30	LOW
Endpoint Security	Malicious Code Protection (Anti-Malware)	END-04	The third-party entity utilize antimalware technologies to detect and eradicate malicious code.	4 - Quantitatively Controlled	Remote	Moderate	Significant		3	LOW	9	LOW

SCF Domain	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	What Is The Current Maturity Level of This Control?	How Likely Is It For This Control To Fail To Operate As Expected?	What Is The Potential Impact If This Control Fails To Operate As Expected?	How Strong Are Compensating Controls To Reduce The Risk Associated With This Control?	Risk Assessment Notes *(Explanation of compensating factors to justify reduction in risk)*	*Risk Factor (unweighted)*		*Risk Factor (compensated & weighted)*	
Endpoint Security	Phishing & Spam Protection	END-08	The third-party entity utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.	3 - Well Defined	Unlikely	Moderate	Moderate		9	MODERATE	44	MODERATE
Human Resources Security	Personnel Screening	HRS-04	The third-party entity manage personnel security risk by screening individuals prior to authorizing access.	4 - Quantitatively Controlled	Highly Unlikely	Major	Moderate		8	MODERATE	34	LOW
Human Resources Security	Terms of Employment	HRS-05	The third-party entity require all employees and contractors to apply cybersecurity & data privacy principles in their daily work.	2 - Planned & Tracked	Unlikely	Moderate	Moderate		9	MODERATE	57	MODERATE
Identification & Authentication	User & Service Account Inventories	IAC-01.3	The third-party entity maintain a current list of authorized users and service accounts.	3 - Well Defined	Highly Unlikely	Moderate	Moderate		6	MODERATE	29	LOW
Identification & Authentication	Multi-Factor Authentication (MFA)	IAC-06	The third-party entity enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/or	3 - Well Defined	Highly Unlikely	Minor	Minimal		4	LOW	23	LOW
Identification & Authentication	User Provisioning & De-Provisioning	IAC-07	The third-party entity utilize a formal user registration and de-registration process that governs the assignment of access rights.	4 - Quantitatively Controlled	Unlikely	Major	Significant		12	HIGH	36	LOW
Identification & Authentication	Role-Based Access Control (RBAC)	IAC-08	The third-party entity enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	3 - Well Defined	Unlikely	Moderate	Moderate		9	MODERATE	40	MODERATE
Identification & Authentication	Authenticator Management	IAC-10	The third-party entity securely manage authenticators for users and devices.	3 - Well Defined	Unlikely	Minor	Moderate		6	MODERATE	29	LOW
Identification & Authentication	Default Authenticators	IAC-10.8	The third-party entity ensure default authenticators are changed as part of account creation or system installation.	3 - Well Defined	Unlikely	Moderate	Moderate		9	MODERATE	44	MODERATE
Identification & Authentication	Account Management	IAC-15	The third-party entity proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	4 - Quantitatively Controlled	Highly Unlikely	Major	Significant		8	MODERATE	24	LOW
Identification & Authentication	Privileged Account Management (PAM)	IAC-16	The third-party entity restrict and control privileged access rights for users and services.	4 - Quantitatively Controlled	Highly Unlikely	Major	Significant		8	MODERATE	24	LOW
Identification & Authentication	Periodic Review of Account Privileges	IAC-17	The third-party entity periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	4 - Quantitatively Controlled	Unlikely	Moderate	Significant		9	MODERATE	27	LOW
Identification & Authentication	Least Privilege	IAC-21	The third-party entity utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5 - Continuously Improving	Remote	Critical	Significant		5	MODERATE	13	LOW
Incident Response	Incident Handling	IRO-02	The third-party entity cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis;	3 - Well Defined	Unlikely	Moderate	Moderate		9	MODERATE	44	MODERATE
Incident Response	Incident Response Plan (IRP)	IRO-04	The third-party entity maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	1 - Performed Informally	Possible	Minor	Minimal		8	MODERATE	65	MODERATE
Network Security	Layered Network Defenses	NET-02	The third-party entity implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers.	1 - Performed Informally	Possible	Minor	Minimal		8	MODERATE	65	MODERATE
Network Security	Guest Networks	NET-02.2	The third-party entity implement and manage a secure guest network.	0 - Non-Existent	Almost Certain	Insignificant	None		6	MODERATE	36	LOW
Network Security	Boundary Protection	NET-03	The third-party entity monitor and control communications at the external network boundary and at key internal boundaries within the network.	1 - Performed Informally	Possible	Minor	Moderate		8	MODERATE	56	MODERATE
Network Security	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	The third-party entity implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	3 - Well Defined	Possible	Minor	Moderate		8	MODERATE	39	MODERATE
Network Security	Remote Access	NET-14	The third-party entity define, control and review organization-approved, secure remote access methods.	0 - Non-Existent	Almost Certain	Insignificant	N/A		6	MODERATE	60	MODERATE
Network Security	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	The third-party entity define secure telecommuting practices and govern remote access to systems and data for remote workers.	0 - Non-Existent	Possible	Insignificant	N/A		4	LOW	40	MODERATE
Network Security	Wireless Networking	NET-15	The third-party entity control authorized wireless usage and monitor for unauthorized wireless access.	2 - Planned & Tracked	Possible	Moderate	Moderate		12	HIGH	68	MODERATE
Network Security	DNS & Content Filtering	NET-18	The third-party entity force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	2 - Planned & Tracked	Unlikely	Moderate	Minimal		9	MODERATE	66	MODERATE
Physical & Environmental Security	Physical Access Authorizations	PES-02	The third-party entity maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	2 - Planned & Tracked	Highly Unlikely	Moderate	Moderate		6	MODERATE	26	LOW
Physical & Environmental Security	Physical Access Control	PES-03	he third-party entity enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	3 - Well Defined	Possible	Major	Minimal		16	HIGH	101	MODERATE
Physical & Environmental Security	Visitor Control	PES-06	The third-party entity identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	4 - Quantitatively Controlled	Unlikely	Major	Moderate		12	HIGH	45	MODERATE
Risk Management	Risk Identification	RSK-03	The third-party entity identifies and documents risks, both internal and external.	4 - Quantitatively Controlled	Highly Unlikely	Moderate	Significant		6	MODERATE	16	LOW
Risk Management	Risk Assessment	RSK-04	The third-party entity conducts recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.	3 - Well Defined	Unlikely	Major	Moderate		12	HIGH	59	MODERATE
Risk Management	Risk Register	RSK-04.1	The third-party entity maintains a risk register that facilitates monitoring and reporting of risks.	2 - Planned & Tracked	Possible	Moderate	Minimal		12	HIGH	97	MODERATE

SCF Domain	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	What Is The Current Maturity Level of This Control?	How Likely Is It For This Control To Fail To Operate As Expected?	What Is The Potential Impact If This Control Fails To Operate As Expected?	How Strong Are Compensating Controls To Reduce The Risk Associated With This Control?	Risk Assessment Notes *(Explanation of compensating factors to justify reduction in risk)*	*Risk Factor* *(unweighted)*		*Risk Factor* *(compensated & weighted)*	
Risk Management	Risk Remediation	RSK-06	The third-party entity remediates risks to an acceptable level.	4 - Quantitatively Controlled	Highly Unlikely	Moderate	Moderate		6	MODERATE	25	LOW
Security Awareness & Training	Cybersecurity & Data Privacy Awareness Training	SAT-02	The third-party entity provides all employees and contractors appropriate awareness education and training that is relevant for their job function.	4 - Quantitatively Controlled	Remote	Moderate	Significant		3	LOW	7	LOW
Third-Party Management	Third-Party Inventories	TPM-01.1	The third-party entity maintains 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 systems, applications, services and data.	2 - Planned & Tracked	Unlikely	Moderate	Moderate		9	MODERATE	45	MODERATE
Third-Party Management	Supply Chain Protection	TPM-03	The third-party entity evaluates security risks associated with the services and product supply chain.	1 - Performed Informally	Likely	Major	Minimal		20	*SEVERE*	162	HIGH
Third-Party Management	Third-Party Contract Requirements	TPM-05	The third-party entity requires contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	3 - Well Defined	Unlikely	Moderate	Moderate		9	MODERATE	44	MODERATE
Third-Party Management	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	The third-party entity documents and maintains a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service	3 - Well Defined	Highly Unlikely	Moderate	Moderate		6	MODERATE	24	LOW
Third-Party Management	Review of Third-Party Services	TPM-08	The third-party entity monitors, regularly reviews and assesses External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls.	2 - Planned & Tracked	Possible	Moderate	Moderate		12	HIGH	68	MODERATE
Vulnerability & Patch Management	Vulnerability Remediation Process	VPM-02	The third-party entity ensures that vulnerabilities are properly identified, tracked and remediated.	4 - Quantitatively Controlled	Highly Unlikely	Moderate	Significant		6	MODERATE	18	LOW
Vulnerability & Patch Management	Software & Firmware Patching	VPM-05	The third-party entity conducts software patching for all deployed operating systems, applications and firmware.	4 - Quantitatively Controlled	Highly Unlikely	Minor	Significant		4	LOW	12	LOW
Vulnerability & Patch Management	Vulnerability Scanning	VPM-06	The third-party entity detects vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	3 - Well Defined	Possible	Moderate	Minimal		12	HIGH	68	MODERATE
									7	MODERATE	40	MODERATE
									Averaged Risk Factor *(unweighted)*		*Averaged Risk Factor* *(compensated & weighted)*	

TPRM Risk Assessment		Occurrence Likelihood					
		Remote *[<1% chance of occurrence]*	**Highly Unlikely** *[1% to 10% chance of occurrence]*	**Unlikely** [10% to 25% chance of occurrence]	**Possible** [25% to 70% chance of occurrence]	**Likely** [70% to 99% chance of occurrence]	**Almost Certain** [>99% chance of occurrence]
Impact Effect	**Catastrophic**	6	12	18	24	30	36
	Critical	5	10	15	20	25	30
	Major	4	8	12	16	20	24
	Moderate	3	6	9	12	15	18
	Minor	2	4	6	8	10	12
	Insignificant	1	2	3	4	5	6

Risk Appetite (*Medium Risk)*

INITIAL RISK ASSESSMENT (INHERENT) - UNWEIGHTED & AVERAGED - Risk Scoring Range (1 to 36)				
LOW (1-4)	**MODERATE** (5-11)	**HIGH** (12-19)	**SEVERE** (20-29)	EXTREME (>30)

**Compensating Controls & Control Weighting Convert Risk Score To*

FINAL RISK ASSESSMENT (RESIDUAL) - WEIGHTED & AVERAGED - Risk Scoring Range (1 to 360)				
LOW (1-36)	**MODERATE** (36.1-108)	**HIGH** (108.1-198)	**SEVERE** (198.1-288)	EXTREME (>288)

Initial Risk		Residual Risk
MODERATE	*Compensating Factors* →	**MODERATE**
Raw Value		*Weighted Value*