

CONFIDENTIAL
Access Limited to Authorized Personnel

CONFIDENTIAL
Access Limited to Authorized Personnel

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 <i>(Explanation of compensating factors to justify reduction in risk)</i>				
									<i>Risk Factor (unweighted)</i>		<i>Risk Factor (compensated & weighted)</i>	
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
									<i>Averaged Risk Factor (unweighted)</i>		<i>Averaged Risk Factor (compensated & weighted)</i>	

Third-Party Risk Management (TRPM)
Risk Assessment Summary

8/20/2025

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)

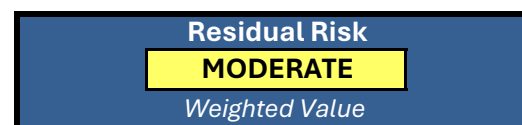
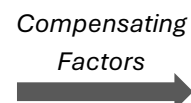
INITIAL RISK ASSESSMENT (INHERENT) - UNWEIGHTED & AVERAGED - Risk Scoring Range (1 to 36)				
LOW (1-4)	MODERATE (5-11)	HIGH (12-19)	SEVERE (20-29)	EXTREME (>30)



*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)



CONFIDENTIAL

Access Limited to Authorized Personnel