	A	B	C	D	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
1																			
2	SCF Control	SCF Control Name	SCF Control	RASCI Summary	Cybersecurity Legal Advice	Executive Cybersecurity Leadership	Privacy Compliance	Product Support Management	Program Management	Secure Project Management	Security Control Assessment	Systems Authorization	Systems Security Management	Technology Portfolio Management	Technology Program Audit	Cybersecurity Supply Chain Risk Management	Board of Directors (BoD)	Chief Executive Officer (CEO)	Chief Operating Officer (COO)
3					OG-WRL-006	OG-WRL-007	OG-WRL-008	OG-WRL-009	OG-WRL-010	OG-WRL-011	OG-WRL-012	OG-WRL-013	OG-WRL-014	OG-WRL-015	OG-WRL-016	OG-WRL-017	OG-SCF-001	OG-SCF-002	OG-SCF-003
370	CPL-01	Statutory, Regulatory & Contractual Compliance	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and	Responsible: Cybersecurity Policy and Planning (OG-WRL-002), Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Systems Security Management (OG-WRL-014), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018), Cybersecurity Architecture (DD-WRL-001)	Consulted	Accountable / Responsible	Consulted		Responsible	Supporting			Responsible					Consulted	Informed
371	CPL-01.1	Non-Compliance Oversight	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual	Responsible: Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Systems Security Management (OG-WRL-014), Technology Program Auditing (OG-WRL-016), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018), Cybersecurity Architecture (DD-WRL-001)		Accountable / Responsible	Consulted		Responsible	Supporting			Responsible		Responsible				
372	CPL-01.2	Compliance Scope	Mechanisms exist to document and validate the scope of security, compliance and resilience controls that are	Responsible: Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Systems Security Management (OG-WRL-014), Line of Business (LOB) Executive (OG-SCF-010), Asset Owner (OG-SCF-011), Process Owner (OG-SCF-012), Compliance Manager (OG-SCF-013), Compliance Specialist (OG-SCF-018)		Accountable / Responsible	Consulted		Responsible	Supporting			Responsible		Informed				
373	CPL-01.3	Ability To Demonstrate Conformity	Mechanisms exist to ensure the organization is able to demonstrate security, compliance and/or resilience capability	Responsible: Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Systems Security Management (OG-WRL-014), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018), Cybersecurity Architecture (DD-WRL-001)		Accountable / Responsible	Consulted		Responsible	Supporting			Responsible						
374	CPL-01.4	Conformity Assessment	Mechanisms exist to conduct assessments to demonstrate security, compliance and/or resilience capability conformity	Responsible: Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Systems Security Management (OG-WRL-014), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018), Cybersecurity Architecture (DD-WRL-001)		Accountable / Responsible	Consulted		Responsible	Supporting			Responsible						
375	CPL-01.5	Declaration of Conformity	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document:	Responsible: Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Systems Security Management (OG-WRL-014), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018), Cybersecurity Architecture (DD-WRL-001)		Accountable / Responsible	Consulted		Responsible	Supporting			Responsible						
376	CPL-01.6	Assessment Team Subject Matter Expertise	Mechanisms exist to ensure individuals performing audits and/or assessments have reasonable:	Responsible: Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018)		Accountable / Responsible			Responsible	Supporting									
377	CPL-01.7	Designated Certifying Official	Mechanisms exist to designate an individual the authority to make statements of conformity on behalf of the organization.	Responsible: Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018)	Consulted	Accountable / Responsible			Responsible	Supporting									
378	CPL-01.8	Conformity Attestations	Mechanisms exist for the certifying official to attest to the accuracy of conformity attestations, based on applicable	Responsible: Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018)		Accountable / Responsible			Responsible	Supporting									
379	CPL-02	Security, Compliance & Resilience Controls Oversight	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the	Responsible: Program Management (OG-WRL-010), Systems Security Management (OG-WRL-014), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018), Cybersecurity Architecture (DD-WRL-001)		Consulted			Responsible	Supporting			Accountable / Responsible						
380	CPL-02.1	Internal Audit Function	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with	Responsible: Program Management (OG-WRL-010), Technology Program Auditing (OG-WRL-016), Governance Manager (OG-SCF-013), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018)		Informed			Responsible	Supporting					Responsible				
381	CPL-02.2	Periodic Audits	Mechanisms exist to conduct periodic audits of security, compliance and resilience controls to evaluate conformity	Responsible: Program Management (OG-WRL-010), Technology Program Auditing (OG-WRL-016), Governance Manager (OG-SCF-013), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018)		Informed			Responsible	Supporting					Responsible				
382	CPL-02.3	Corrective Action	Mechanisms exist to take corrective action to remediate instances of non-conformity with applicable statutory,	Responsible: Program Management (OG-WRL-010), Governance Manager (OG-SCF-013), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018)		Consulted			Responsible	Supporting									
383	CPL-03	Security, Compliance & Resilience Assessments	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the	Responsible: Program Management (OG-WRL-010), Line of Business (LOB) Executive (OG-SCF-010), Asset Owner (OG-SCF-011), Process Owner (OG-SCF-012), Governance Manager (OG-SCF-013), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018)		Consulted			Responsible	Supporting			Supporting						
384	CPL-03.1	Independent Assessors	Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or	Responsible: Program Management (OG-WRL-010), Technology Program Auditing (OG-WRL-016), Governance Manager (OG-SCF-013), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018)		Informed			Responsible	Supporting					Responsible				
385	CPL-03.2	Functional Review Of Security, Compliance & Resilience Controls	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the	Responsible: Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Technology Program Auditing (OG-WRL-016), Governance Manager (OG-SCF-013), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018)		Accountable / Responsible			Responsible	Supporting					Responsible				
386	CPL-03.3	Assessor Access	Mechanisms exist to grant assessors minimum necessary access to conduct conformity assessments, including:	Responsible: Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Line of Business (LOB) Executive (OG-SCF-010), Asset Owner (OG-SCF-011), Process Owner (OG-SCF-012), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018)		Accountable / Responsible			Responsible	Supporting									
387	CPL-03.4	Assessment Methods	Mechanisms exist to define acceptable methods to conduct a cybersecurity and/or data protection assessment.	Responsible: Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Systems Security Management (OG-WRL-014), Technology Program Auditing (OG-WRL-016), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018)		Accountable / Responsible	Consulted		Responsible	Supporting			Responsible		Responsible				
388	CPL-03.5	Assessment Rigor	Mechanisms exist to define the level of assessment rigor necessary to conduct a cybersecurity and/or data protection	Responsible: Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Systems Security Management (OG-WRL-014), Technology Program Auditing (OG-WRL-016), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018)		Accountable / Responsible	Consulted		Responsible	Supporting			Responsible		Responsible				
389	CPL-03.6	Evidence Request List (ERL)	Mechanisms exist to define an Evidence Request List (ERL) prior to the start of a cybersecurity and/or data protection	Responsible: Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Systems Security Management (OG-WRL-014), Technology Program Auditing (OG-WRL-016), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018)		Accountable / Responsible	Consulted		Responsible	Supporting			Responsible		Responsible				
390	CPL-03.7	Evidence Sampling	Mechanisms exist to define evidence sampling criteria for cybersecurity and/or data protection assessments.	Responsible: Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Systems Security Management (OG-WRL-014), Technology Program Auditing (OG-WRL-016), Line of Business (LOB) Executive (OG-SCF-010), Asset Owner (OG-SCF-011), Process Owner (OG-SCF-012), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018)		Accountable / Responsible	Consulted		Responsible	Supporting			Responsible		Responsible				
391	CPL-04	Audit Activities	Mechanisms exist to thoughtfully plan audits by including input from operational risk and compliance partners to	Responsible: Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Technology Program Auditing (OG-WRL-016), Line of Business (LOB) Executive (OG-SCF-010), Asset Owner (OG-SCF-011), Process Owner (OG-SCF-012), Governance Manager (OG-SCF-013), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018)		Accountable / Responsible			Responsible	Supporting					Responsible				
392	CPL-05	Legal Assessment of Investigative Inquires	Mechanisms exist to determine whether a government agency has an applicable and valid legal basis to request data from	Responsible: Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Systems Security Management (OG-WRL-014), Line of Business (LOB) Executive (OG-SCF-010), Asset Owner (OG-SCF-011), Process Owner (OG-SCF-012), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018)	Consulted	Accountable / Responsible	Consulted		Responsible	Supporting			Responsible						
393	CPL-05.1	Investigation Request Notifications	Mechanisms exist to notify customers about investigation request notifications, unless the applicable legal basis for a	Responsible: Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Systems Security Management (OG-WRL-014), Line of Business (LOB) Executive (OG-SCF-010), Asset Owner (OG-SCF-011), Process Owner (OG-SCF-012), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018)	Consulted	Accountable / Responsible	Consulted		Responsible	Supporting			Responsible						
394	CPL-05.2	Investigation Access Restrictions	Mechanisms exist to support official investigations by provisioning government investigators with "least privileges"	Responsible: Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Systems Security Management (OG-WRL-014), Line of Business (LOB) Executive (OG-SCF-010), Asset Owner (OG-SCF-011), Process Owner (OG-SCF-012), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018)	Consulted	Accountable / Responsible	Consulted		Responsible	Supporting			Responsible						
395	CPL-06	Government Surveillance	Mechanisms exist to constrain the host government from having unrestricted and non-monitored access to the	Responsible: Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018)	Consulted	Accountable / Responsible			Responsible	Supporting									
396	CPL-07	Grievances	Mechanisms exist to govern the intake and analysis of grievances related to the organization's cybersecurity and/or	Responsible: Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018)	Consulted	Accountable / Responsible			Responsible	Supporting									
397	CPL-07.1	Grievance Response	Mechanisms exist to respond to legitimate grievances related to the organization's cybersecurity and/or data protection	Responsible: Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018)	Consulted	Accountable / Responsible			Responsible	Supporting									
398	CPL-08	Localized Representation	Mechanisms exist to appoint localized representation with a physical presence in localities, as required by applicable laws	Responsible: Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Line of Business (LOB) Executive (OG-SCF-010), Asset Owner (OG-SCF-011), Process Owner (OG-SCF-012), Compliance Manager (OG-SCF-017), Compliance Specialist (OG-SCF-018)	Consulted	Accountable / Responsible			Responsible	Supporting									
			Mechanisms exist to contract localized representation to	Responsible: Executive Cybersecurity Leadership (OG-WRL-007), Program Management (OG-WRL-010), Line of		Accountable /													

SCF RASCI (2026.1) | NIST NICE-Based Roles | +