CCF Control				Applicability																				Mapping													
CCF ID	Control Domain	Control Name	Control Description	NIST Cybersecurity	BSI C5	CIS V8	MLPS	ISO 22301	Cyber Essentials UK	ENS	ISO 27001	ISO 27002 (ISO 27001 Annex A)	ISO 27017	ISO 27018	TX_RAMP L1	FEDRAMP Tailored	FEDRAMP Moderate	HIPAA Security	IRAP	ISMAP	MAS	PCI-DSS 4.0	KPSI	SOC 2	NIST Cybersecurity Ref#	BSI C5 Ref #	CIS V8 Ref #	MLPS Ref #	ISO 22301 Ref #	Cyber Essentials UK Ref #	ENS Ref #	ISO 27001 Ref #	ISO 27002 Ref #	ISO 27017 Ref #	ISO 27018 Ref #	TX_RAMP L1 Ref #	FEDRAMP TAILORED Ref #	FEDRAMP MODERATE Ref #	HIPAA Security Ref #	IRAP Ref #	ISMAP Ref #	MAS Ref #	PCI-DSS V4 Ref #	KPSI Ref #	SOC 2 Ref#
AM-01	Asset Management	Inventory Management	Organization maintains an inventory of information systems, which is reconciled on a periodic basis.	X	X	X	X			X					X	X	X	X	X	X	X	X	X	X	ID.AM-2 ID.AM-1	AM-01 AM-06	1.1 6.6	8.1.4.2 8.1.10.2			8 9 10 26					CM-08	CM-08	CM-08 CM-08 (01)	164.310(d)(1)	ISM-1551 ISM-1549 ISM-1359 ISM-1753 ISM-1493 ISM-0336		8.1.1.1 8.1.1.2 8.1.1.3 8.1.1.4 8.1.1.5 8.1.1.6.PB 8.3.1.3 8.3.1.8 8.3.1.11 11.2.1.9 18.1.1.12 18.1.2.4	3.3	12.5.1, 12.5.2, 12.5.2.1, 9.5.1.1	3.1.1	CC6.1
AM-02	Asset Management	Inventory Management: Applications	Organization maintains an inventory of application assets, which is reconciled on a periodic basis.	X	X	X	X			X					X	X	X	X	X	X	X	X	X	X	ID.AM-2 ID.AM-1	AM-01 AM-06	1.1 6.6	8.1.4.2 8.1.10.2			8 9 10 26					CM-08	CM-08	CM-08 CM-08 (01)	164.310(d)(1)	ISM-1551 ISM-1549 ISM-1359 ISM-1753 ISM-1493 ISM-0336		8.1.1.1 8.1.1.2 8.1.1.3 8.1.1.4 8.1.1.5 8.1.1.6.PB 8.3.1.3 8.3.1.8 8.3.1.11 11.2.1.9 18.1.1.12 18.1.2.4	3.3	12.5.1, 12.5.2, 12.5.2.1, 9.5.1.1	3.1.1	CC6.1
AM-03	Asset Management	Inventory Reconciliation: ARP Table	Organization reconciles network discovery scans against the established device inventory on a quarterly basis; non-inventoried devices are assigned an owner.			X	X															X					1.2 1.3 1.5	8.1.10.2															11.2., 11.2.1, 11.2.2, 11.3.1, 11.3.1.3, 11.4.5, 11.4.6			
AM-04	Asset Management	Inventory Reconciliation: Logging	Organization reconciles the enterprise log repository against the established device inventory on a quarterly basis; non-inventoried devices are assigned an owner.			X											X					X					1.4										CM-08 (03)					12.5.1, 12.5.2, 12.5.2.1, 9.4.5, 9.4.5.1			
AM-05	Asset Management	Inventory Labels	Organization assets are labeled and have designated owners.		X	X	X			X		X			X	X	X		X	X	X	X	X	X		AM-01 AM-06	1.1	8.1.4.2			8 9 10 26 92 93 80			5.13			CM-08	CM-08	CM-08		ISM-0294 ISM-1217 ISM-0332 ISM-0325 ISM-0330 ISM-0831 ISM-0378 ISM-1187 ISM-1071 ISM-1525		8.1.2.1 8.1.2.2 8.1.2.3 8.1.2.4 8.1.2.5 8.1.2.6	3.3	9.4.2	3.1.1	CC6.1
AM-06	Asset Management	Media Marking	Where applicable, Organization marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information. Exemptions must be approved by management and remain in a specific controlled area.				X					X					X		X	X		X						8.1.10.3							5.1 7.8			MP-03		ISM-1074 ISM-1599 ISM-0323 ISM-0037 ISM-0325 ISM-0330 ISM-0831 ISM-0379		18.1.3.2 18.1.3.4 18.1.3.5 18.1.3.7		9.4		
AM-07	Asset Management	Asset Transportation Authorization	Organization authorizes and records the entry and exit of systems at datacenter locations.	X						X		X		X	X	X	X	X	X	X		X		X	ID.AM-4 PR.DS-3						57 68 69 84			7.1		A.10.4	MA-02 PE-08	MA-02 PE-08	MA-02 PE-08 SA-09 (05)	164.310(d)(1) 164.310(d)(2)(iii)	ISM-1243 ISM-1779		4.1.2.2 8.3.1.2 11.2.3.1 11.2.5.2 11.2.5.3 11.2.5.4 11.2.6.2		9.4.4		CC6.7
AM-08	Asset Management	Asset Transportation Documentation	Organization documents the transportation of physical media outside of datacenters. Physical media is packaged securely and transported in a secure, traceable manner.				X			X				X	X	X	X		X	X		X					8.1.10.3 8.1.10.4						57 68 69					A.10.4	MA-02	MA-02	MA-02 MP-05		ISM-0310		8.3.3.1 8.3.3.2 8.3.3.3 8.3.3.4 8.3.3.5 11.2.5.1 11.2.6.3 11.2.6.5		9.4.3		
AM-09	Asset Management	Use of Portable Media	The use of portable media in Organization datacenters is prohibited unless explicitly authorized by management.												X	X	X					X														MP-07	MP-07	MP-07 MP-05					9.4.4		
AM-10	Asset Management	Maintenance of Assets	Equipment maintenance is documented and approved according to management requirements.	X	X		X			X		X			X	X	X	X	X	X	X	X		X	PR.DS-8 PR.MA-1	PS-06		8.1.10.4 8.1.10.6			13 29			7.1.3			CM-08 MA-02 MA-04 MP-01	CM-08 MA-02 MA-04 MP-01 SA-22 SR-11 (02)	CM-08 MA-02 MA-04 MP-01 MA-03	164.310(a)(2)(iv)	ISM-0305 ISM-0307 ISM-0306 ISM-1098		8.3.1.5 8.3.1.4 8.3.1.5 8.3.1.6 8.3.1.9 11.2.1.10 11.2.4.1 11.2.4.2 11.2.4.3 11.2.4.4 11.2.4.5 11.2.4.6 11.2.4.7 11.2.4.8 11.2.4.9 11.2.4.10 11.2.4.11	7.3	9.4.4		A1.2
AM-11	Asset Management	Tampering of Payment Card Capture Devices	Devices that physically capture payment card data are inspected for evidence of tampering on a semi-annual basis.																			X																				9.5.1.2		
AM-12	Asset Management	Component Installation Inspection and Approval	Prior to installation in a production network, hardware components are inspected for improper or unauthorized modifications.			X	X									X	X					X					AM-03	4.2												SR-11 SR-11 (01)	MA-03 (02)			ISM-1418 ISM-0343				2.2, 6.5.1		
AM-13	Asset Management	Software bill of Material	Organization maintains a comprehensive software bill of materials																	X																				ISM-1730					
BC-01	Business Continuity	Business Continuity Plan	Organization's business contingency plan is periodically reviewed, approved by management and communicated to relevant team members.	X	X		X	X		X					X	X	X	X			X	X	X	X	RC/IM-2	BCM-01 BCM-02 BCM-03 BCM-04		8.1.10.13	4.4 5.1(a) 5.1(b) 5.1.K 5.1(g) 6.2.1(a) 6.2.1(e) 6.3(a) 6.3(b) 7.5.1(a) 7.5.1(b) 8.10 8.2.1(b)			42 43 44 70					CP-01 CP-02	CP-01 CP-02	CP-01 CP-02 CP-02 (01)	164.308(a)(7)(i) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(D)			17.1.1.1 17.1.1.3 17.1.2.1 17.1.2.3 17.1.2.4 17.1.2.5 17.1.3.4	8.2		5.1.1	CC7.5
BC-02	Business Continuity	Business Continuity Plan: Personal Health Information	Organization's Business Contingency Plan addresses how to access facilities and obtain data during an emergency.				X											X										8.1.10.13															164.310(a)(2)(i) 164.312(a)(2)(ii)						
BC-03	Business Continuity	Business Continuity Plan: Roles and Responsibilities	Business contingency roles and responsibilities are assigned to individuals and their contact information is communicated to authorized personnel.					X										X											4.2.1(a) 4.2.1(b) 5.1.0 5.1.7 5.1.7(i) 5.3.1(a) 5.3.1(b) 6.2.2.0 6.3.0(f) 7) 7.1.1(b) 7.1.1(d)											CP-01 CP-02 IA-02	CP-01 CP-02 IA-02	CP-01 CP-02 IA-02					10.7.3		
BC-04	Business Continuity	Continuity Testing	Organization performs business contingency and disaster recovery tests on a periodic basis and ensures the following: - tests are executed with relevant contingency teams - test results are documented - corrective actions are taken for exceptions noted - plans are updated based on results	X	X		X	X		X					X	X	X	X		X	X	X	X	X	RC/IM-2 PR.IP-9 PR.IP-10 ID.SC-5 PR.PT-5	BCM-01 BCM-02 BCM-03 BCM-04 OPS-08 PS-02		8.1.10.12 8.1.10.13	6.2.1(b) 8.4.5 8.5 8.5(a) 8.5(b) 8.5.0 8.5(d) 8.5.E 8.5(f) 8.5(g) 8.4(b)			42 44 45 70			5.3			CP-04	CP-04	CP-04 CP-04 (01)	164.308(a)(7)(i)(B) 164.308(a)(7)(ii) 164.308(a)(7)(ii)(D) 164.310(a)(2)(i)			17.1.1.4 17.1.2.4 17.1.3.1 17.1.3.2 17.1.3.3	8.2 8.3	10.7.3	5.2.1 5.2.2	CC7.5 A1.3
BC-05	Business Continuity	Business Impact Analysis	Organization identifies the business impact of relevant threats to assets, infrastructure, and resources that support critical business functions. Recovery objectives are established for critical business functions.	X	X			X		X		X			X	X	X	X	X	X	X		X		ID.BE-5 PR.IP-9	BCM-02 BCM-03 BCM-04 OPS-08			3.1 4.3.0.a 4.3.1.0.b 4.3.1.10 4.3.2.0.a 4.3.2.0.b 6.2.1.10 6.2.1.0.f) 6.2.1.K 6.2.1.(f) 6.2.2.1 6.2.2.2(a) 6.2.2.2(b)			42 43 70			5.29			CP-09 CP-09 (08) CP-09 (03)	CP-09 CP-09	CP-09 CP-02 (08) CP-09 (03)	164.308(a)(7)(ii)(B)	ISM-0246		12.2.1.10 12.2.1.11 17.1.1.2 17.1.2.2	8.2	10.7.3		CC7.5
BC-06	Business Continuity	Capacity Forecasting	Budgets for infrastructure capacity are established based on analysis of historical business activity and growth projections; purchases are made against the established budget and plans are updated on a quarterly basis.		X			X		X		X			X	X		X			X				BCM-01 OPS-01				6.3.0 8.3.4(a) 8.3.4(b) 8.3.4.0 8.3.4(d) 8.3.4.K 8.3.4(f) 8.3.4(g) 8.3.4(h)			42 70			8.6			CA-02 (03)	164.308(a)(7)(i)(A		12.1.3.8	8.1			CC3.1 A1.1
BM-01	Backup Management	Backup Configuration	Organization configures redundant systems or performs periodic backups of data to resume system operations in the event of a system failure.	X	X	X	X					X		X	X	X	X	X	X	X	X	X	X	PR.IP-4	OPS-06 OPS-07 PS-02	11.2	8.1.2.1 8.1.4.9 8.1.5.1 8.1.10.11 8.2.4.6 (a) 8.2.4.6 (b)						5.33 8.13 8.14		A.10.3	CP-09 CP-10	CP-09 CP-10	CP-09 CP-10 CP-02 (03) CP-06 CP-07 CP-09 (01)	164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.310(d)(2)(iv)	ISM-1547 ISM-1511		8.3.1.7 17.2.1.3 14.1.2.15	8.1 8.4	10.7.3	5.1.1 5.2.1	CC7.5 CC9.1 A1.2 C1.1
BM-02	Backup Management	Resilience Testing	Organization performs annual backup restoration or data replication tests to confirm the reliability and integrity of system backups or recovery operations.	X	X	X	X			X		X		X	X	X	X	X	X	X	X	X	X	PR.IP-4	OPS-06 OPS-08 OPS-09 PS-02	11.1 11.3 11.5	8.1.4.9 8.1.10.11			100			8.13		A.10.3	CP-10	CP-10	CP-10 CM-02 (02) CP-06 CP-07 CP-09 (01)	164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.310(d)(2)(iv)	ISM-1548 ISM-1511 ISM-1515 ISM-0455		12.3.1.1 12.3.1.2 12.3.1.3 12.3.1.4 12.3.1.5 12.3.1.6 12.3.1.7 12.3.1.8 12.3.1.9 12.3.1.10 12.3.1.11 12.3.1.13 12.3.1.14	8.4	10.7.3	5.2.1 5.2.2	CC7.5 CC9.1 A1.2 A1.3 C1.1
BM-03	Backup Management	Backup Failure Review	Failed backup jobs are periodically reviewed and resolved in a timely manner.			X	X	X													X		X		OPS-06	11.1 11.5	8.1.10.11																12.3.1.12			10.7.3			
BM-04	Backup Management	Alternate Storage	Organization backups are securely stored in an alternate location from source data.				X											X			X					11.4												CP-06 (01) CP-09 (05) SA-09 (05)				14.1.3.5		5.2.1	
BM-05	Backup Management	Alternate Telecommunication	Alternate telecommunication service agreements have been established to resume business when the primary service gets disrupted. Service agreements contain priority of service provisions.															X																				CP-07 (03) CP-08 (01) CP-08 (02)							

CFM-01	Configuration Management	Baseline Configuration Standard	Organization ensures security hardening and baseline configuration standards have been established according to industry standards and are reviewed and updated periodically.	X	X	X	X			X		X	X		X	X	X	X	X	X	X	X	X	X	DE.AE-1 PR.IP-1 PR.PT-3	AM-03 COS-03 OPS-04 OPS-05 OPS-23 PSS-11	4.1 4.2 16.7	8.1.3.2 8.1.5.1 8.1.10.6 8.1.10.8 8.2.4.4			4 13 88 89 90		8.9	CLD.9.5.2		CA-03 CM-01 CM-02 CM-06	CA-03 CM-01 CM-02 CM-06 PL-10 PL-11	CA-03 CM-01 CM-02 CM-06 CM-02 (03) SA-10	164.308(a)(5)(ii)(B)	ISM-0289 ISM-1743 ISM-1744 ISM-1408 ISM-1406 ISM-1409 ISM-1654 ISM-1655 ISM-1492 ISM-0843 ISM-1490 ISM-1656 ISM-1657 ISM-1658 ISM-1582 ISM-1392 ISM-1746 ISM-1544 ISM-1659 ISM-0846 ISM-1621 ISM-1622 ISM-1623 ISM-1624	9.5.2.1.PB 12.5.1.7	7.2 11.3 12.2	1.2, 1.2.1, 2.2, 2.2.1	8.1.1	CC6.8 CC7.1 CC8.1
CFM-02	Configuration Management	Default "Deny-all" Settings	Where applicable, the information system default access configurations are set to "deny-all."			X	X		X								X		X			X					4.5	8.1.3.2		Firewalls								AU-09 (04)		ISM-1654 ISM-1655 ISM-1492 ISM-0843 ISM-1490 ISM-1656 ISM-1657 ISM-1658 ISM-1582 ISM-1392 ISM-1746 ISM-1544 ISM-1659 ISM-0846 ISM-1621 ISM-1622 ISM-1623 ISM-1624 ISM-1486 ISM-1485 ISM-1666 ISM-1668 ISM-1670 ISM-1601			2.2.6, 7.3.3		
CFM-03	Configuration Management	Remote Access: Prohibited Protocols and Commands	Organization defines a listing of prohibited user commands and prohibited protocols that can be used in a remote session.			X									X	X	X					X					13.5									AC-17	AC-17	AC-17 AC-17 (04) AU-09 (04)					1.2.5, 1.2.6, 2.2.4, 2.2.5, A2.1, A2.1, 2.1.2		
CFM-04	Configuration Management	Data Execution Prevention	Organization ensures data execution prevention (DEP) security features are enabled on production hosts to restrict code execution within memory.			X											X					X					10.5											CM-07 (02) SI-16					2.2.6		
CFM-05	Configuration Management	Client Run Time Technologies	Organization disables prohibited client run time technologies on information systems.			X											X					X					9.4											CA-03 (05)					1.2.5, 1.2.6, 2.2.4, 2.2.5		
CFM-06	Configuration Management	Prohibited Activity Monitoring	Organization information systems are configured to explicitly deny a predefined list of activities.														X		X			X																AU-09 (04) CA-03 (05)		ISM-1654 ISM-1655 ISM-1492 ISM-0843 ISM-1490 ISM-1656 ISM-1657 ISM-1658 ISM-1582 ISM-1392 ISM-1746 ISM-1544 ISM-1659 ISM-0846 ISM-1621 ISM-1622 ISM-1623 ISM-1624 ISM-1486 ISM-1485 ISM-1666 ISM-1668 ISM-1670 ISM-1601			1.2.5, 1.2.6, 2.2.4, 2.2.5		
CFM-07	Configuration Management	Configuration Checks	Organization uses mechanisms to detect deviations from baseline configurations on production environments.		X		X			X		X			X	X	X	X			X	X		X		AM-03 COS-03 OIS-04 OPS-04 OPS-05 OPS-23		8.2.4.4			4 13 15 88 89 90		8.18			CM-06 CM-07	CM-06 CM-07	CM-06 CM-07 CM-06 (01) CM-09 SA-10	164.308(a)(5)(ii)(B)			7.2 11.3 12.2	11.6, 11.6.1		CC6.8 CC7.1
CFM-08	Configuration Management	Configuration Check Reconciliation: Logging	Organization reconciles the established device inventory against the enterprise log repository on a quarterly basis; devices which do not forward security configurations are remediated.				X															X						8.1.10.6															10.4 ,10.4.1, 10.4.1.1, 10.4.2, 10.4.2.1		
CFM-09	Configuration Management	Time Clock Synchronization	Systems are configured to synchronize information system time clocks based on International Atomic Time or Coordinated Universal Time (UTC).			X				X		X					X			X		X	X				8.4				13 37		8.17					AC-21			12.4.4.1 12.4.4.2 12.4.4.3 12.4.4.4.PB		10.6, 10.6.1, 10.6.2, 10.6.3	9.1.1	
CFM-10	Configuration Management	Time Clock Configuration Access	Access to modify time data is restricted to authorized personnel.														X					X																SA-10					10.6.3		
CFM-11	Configuration Management	Default Device Passwords	Vendor-supplied default passwords are changed according to Organization standards prior to device installation on the Organization network or immediately after software or operating system installation.				X		X	X									X			X						8.1.4.2 8.1.10.9		Firewalls Secure Configuration	13									ISM-1260 ISM-1304 ISM-1316			2.2.2		
CFM-12	Configuration Management	Process Isolation	Organization implements only one primary function per server within the production environment; the information system maintains a separate execution domain for each executing process.			X				X							X		X			X					12.8				13							AC-04 (21) SC-02		ISM-1750 ISM-1381 ISM-0385 ISM-1479			2.2.2, 8.2.2		
CFM-13	Configuration Management	Collaborative Devices	Where applicable, collaborative computing devices used at Organization are configured to restrict remote activation and provide an explicit indication that they are in use.			X				X						X	X					X					12.8				13						SC-15	SC-15					8.2.2, 8.2.5		
CFM-14	Configuration Management	Software Installation	Installation of software or programs in the production environment is approved by authorized personnel.			X	X		X			X			X	X	X		X	X		X					2.4 2.5 2.6	8.1.4.4 8.1.10.6 8.3.3.2		Malware protection			8.19			CM-11	CM-11	CM-11		ISM-1584 ISM-1491 ISM-1592 ISM-0382	9.4.4.2 9.4.4.4 9.4.4.5 9.4.4.8 12.5.1.12 12.5.1.13 12.6.2.1 12.6.2.3		2.2.4, 6.3.3		
CFM-15	Configuration Management	Job Schedules	Schedule changes or the modifications of production jobs require: • documented approval from authorized personnel • documented monitoring details																X			X																		ISM-1211			6.5, 6.5.1		
CHM-01	Change Management	Change Management Workflow	Change scope, change type, and roles and responsibilities are pre-established and documented in a change control workflow; notification and approval requirements are also pre-established based on risk associated with change scope and type.	X	X		X			X		X			X	X	X			X	X	X	X	X	PR.IP-3	DEV-01 DEV-03 DEV-05 DEV-07		8.1.7.3 8.1.10.10			30 87		8.32			SA-03	SA-03 CM-05	SA-03 CM-03 CM-05 (05) SA-10			4.5.4.4 12.1.2.1 12.1.2.2 12.1.2.3 12.1.2.4 12.1.2.5 12.1.2.6 12.1.2.7 12.1.2.8 12.1.2.9 14.2.2.1 14.2.2.2 14.2.2.3 14.2.2.4 14.2.2.5 14.2.2.6 14.2.2.7 14.2.2.8 14.2.2.9 14.2.2.10 14.2.2.11 14.2.2.12 14.2.2.13 14.2.2.15	5.4 7.5	6.5, 6.5.1	3.2.1 8.1.1	CC8.1
CHM-02	Change Management	Change Approval	Prior to introducing changes into the production environment, approval from authorized personnel is required based on the following: • change description • impact of change • test results • back-out plan		X		X			X		X	X		X	X	X			X	X	X	X	X		AM-03 DEV-05 DEV-06 DEV-07 DEV-09 OIS-04 PSS-02 PSS-09		8.1.9.4			30 88 89 90		8.3	CLD.12.1.5		CM-04 CM-06	CM-04 CM-06	CM-04 CM-06 CM-03 SA-10			12.1.2.1 12.1.2.2 12.1.2.3 12.1.2.4 12.1.2.5 12.1.2.6 12.1.2.7 12.1.2.8 12.1.2.10 12.5.1.3 12.5.1.4 12.5.1.5 12.5.1.6 12.5.1.8 12.5.1.10 14.2.3.1 14.2.3.2 14.2.3.3 14.2.4.10 14.2.8.1 14.2.8.3 14.2.9.1 14.2.9.2 9.4.4.11.P	5.5 5.7 5.8 6.3 7.4 7.5	6.5.1	3.2.1	CC8.1
CHM-03	Change Management	Segregation of Duties	Changes to the production environment are implemented by authorized personnel.	X	X					X					X		X			X	X	X	X	X	PR.AC-4	DEV-07 OIS-04					2 4 5 16 87					CM-05		CM-03 CM-05 (05) SA-10			6.1.2.2 12.5.1.1 14.2.6.11 14.2.6.12	6.3 7.6	6.5.4	2.1.2	CC6.1
CHM-04	Change Management	Communication of Maintenance and Downtime	Customer-impacting product and system changes are publicly communicated on the company website.										X							X			X	X										CLD.12.4.5							12.1.2.11.PB 12.1.5.1.PB			3.2.1	CC2.3
CMS-01	Customer Managed Security	Customer Administrative Access	For products that enable customers to manage their end users, privileged user roles exist with the capability to manage end user access to the relevant applications.		X																					PSS-05 PSS-08																			
CMS-02	Customer Managed Security	Customer Authentication	Authentication to organization customer-facing applications are performed through secure log-on procedures.		X																		X			PSS-05																		7.3.1	
CMS-03	Customer Managed Security	Customer Systems Monitoring	As necessary, event logs are made available to customers.		X																					OPS-03																			
CMS-04	Customer Managed Security	Customer Security Engagements	Organization supports customer-requested security inquiries, questionnaires, and audits: • in accordance with customer contracts and agreements • to facilitate due diligence prior to licensing organization products																				X																					6.1.3	
CRY-01	Cryptography	Encryption Key Maintenance	Cryptographic keys are invalidated when compromised or at the end of their defined lifecycle period.							X					X	X	X		X	X		X	X								24 25 38 39 94					PS-05 SC-12	PS-05	PS-05		ISM-1611 ISM-1612 ISM-1614 ISM-1615 ISM-1091	18.1.5.2 9.3.1.3 10.1.1.4		3.7.4, 3.7.5	10.2.2	
CRY-02	Cryptography	Encryption Key Distribution	Organization prohibits the distribution of cryptographic keys in clear text.												X					X		X														SC-12					9.4.2.14 9.4.3.9		3.7.6		
CRY-03	Cryptography	Encryption Key Storage	Encryption keys are securely stored in an approved encryption platform.																			X																					3.7.3		
CRY-04	Cryptography	Clear Text Key Management	If applicable, manual clear-text cryptographic key-management operations must be managed using split knowledge and dual control.																			X																					3.7.6		
CRY-05	Cryptography	Encryption of Data in Transit	Organization restricted data that is transmitted over public networks is encrypted.	X	X	X	X			X				X	X	X	X	X	X	X	X	X	X	X	PR.DS-2 PR.DS-5	COS-08 CRY-01 CRY-02 OPS-14 PI-01	3.10	8.1.4.8 8.1.5.4 8.2.4.5 (a)			24 25 73 74 75 76 77 91 94 95 96 97				A.11.2	IA-05 (01) IA-07	IA-05 (01) IA-07 SC-08 SC-08 (01)	IA-05 (01) IA-07	164.312(a)(2)(i) 164.312(a)(2)(iv) 164.312(c)(1) 164.312(e)(1) 164.312(e)(2)(i) 164.312(e)(2)(ii)	ISM-1059 ISM-1552 ISM-1277 ISM-0571 ISM-0572 ISM-1589 ISM-1781 ISM-0457 ISM-0469 ISM-0465 ISM-0467 ISM-0263 ISM-0958 ISM-1293	10.1.1.1 13.2.1.1 13.2.1.3 13.2.1.4 13.2.1.6 13.2.3.1 14.1.1.11 14.1.2.4 14.1.2.5 14.1.2.6 14.1.2.7 14.1.2.8 14.1.2.9 14.1.2.10 14.1.2.11 14.1.3.1 14.1.3.2 14.1.3.3 14.1.3.4 18.1.5.1 10.1.1.5 10.1.1.7 13.2.3.2 13.2.1.8	11.1	4.2	10.2.1	CC6.1 CC6.7

CRY-06	Cryptography	Encryption of Data at Rest	Organization restricted data at rest is encrypted.		X	X	X			X						X	X	X	X	X	X	X	X	X		COS-08 CRY-01 CRY-03 PSS-07	3.11 11.3	8.1.4.8			4 24 25 73 74 91 94 95 96 97						SC-28 SC-28 (01)	SC-28 SC-28 (01)	164.312(a)(2)(iv) 164.312(c)(1) 164.312(e)(2)(ii)	ISM-1597 ISM-1402 ISM-1080 ISM-0457 ISM-0460 ISM-0459	8.2.3.1 8.2.3.2 8.2.3.3 8.2.3.4 8.2.3.5 8.2.3.6 8.2.3.7 10.1.1.1 14.1.3.5 10.1.1.5 10.1.1.7 18.1.5.5	8.4 11.1	3.3.2, 3.5, 3.5.1, 3.5.1.1	10.2.1	CC6.1 CC6.7
CRY-07	Cryptography	Approved Cryptographic Technology	Where applicable, strong industry standard cryptographic ciphers and keys with an effective strength greater than 112 bits are required for cryptographic security operations.		X	X	X			X		X				X			X	X		X				CRY-02 CRY-04 IDM-08	3.11	8.1.2.2 8.1.9.3 8.1.10.9 8.2.4.4			82		8.24				SC-12 SC-13			ISM-0955 ISM-1597 ISM-1402 ISM-1552 ISM-0457 ISM-0994 ISM-0472 ISM-1446 ISM-0474 ISM-1761 ISM-1762 ISM-0475 ISM-1763 ISM-1764 ISM-0476 ISM-1765 ISM-1766 ISM-1767 ISM-1768 ISM-1769 ISM-1770 ISM-0479 ISM-0481 ISM-1139	10.1.1.6 13.2.3.4 10.1.1.5 10.1.1.7 10.1.1.8 10.1.2.2 18.1.5.3 18.1.5.4 18.1.5.5		4.2.1, A3.2.6		
CRY-08	Cryptography	Key Repository Access	Access to the cryptographic keystores is limited to authorized personnel.		X					X		X			X			X		X	X	X	X	X		CRY-01 CRY-03 CRY-04					24 25 38 39 94 95 96 97		8.24			SC-12			164.308(a)(5)(ii)(D)		9.2.4.1 10.1.1.2 10.1.2.1 10.1.2.3 10.1.2.4 10.1.2.5 10.1.2.6 10.1.2.7 10.1.2.8 10.1.2.9 10.1.2.10 10.1.2.11 10.1.2.12 10.1.2.13 10.1.2.14 10.1.2.15 10.1.2.16 10.1.2.17 10.1.2.18 18.1.3.3	9.2 10.2	3.7.1, 3.7.2, 3.7.3	10.2.2	CC6.1
CRY-09	Cryptography	Key Store Review	Management reviews and authorizes key store locations.												X					X		X														SC-12					9.4.3.8		3.7.3		
CRY-10	Cryptography	Full Disk Encryption Access	Where full disk encryption is used, logical access must be managed independently of operating system authentication; decryption keys must not be associated with user accounts.														X					X																AC-19 (05)					3.5.1.2, 3.5.1.3		
CRY-11	Cryptography	Key Custodians Agreement	Cryptographic Key Custodians and Cryptographic Materials Custodians (CMC) acknowledge in writing or electronically that they understand and accept their cryptographic-key-custodian responsibilities.																X	X		X																		ISM-0507	6.1.1.13.PB		3.6.1		
CRY-12	Cryptography	Approved Certificate Authorities	Organization restricts the use of digital certificates to those that are signed by approved certificate authorities; a certification path to an accepted trust anchor is established.				X										X		X	X		X						8.3.4.2										IA-05 (02)		ISM-1471 ISM-1674 ISM-1675 ISM-1676 ISM-1324 ISM-1323 ISM-1327	14.1.3.6		4.2.1, 4.2.1.1, 8.3.11		
CRY-13	Cryptography	Installation of Software: Certificate Verification	Digital Certificates are verified by information system components prior to installation on the production network.												X	X	X		X	X		X														CM-11	CM-11	CM-11		ISM-1674 ISM-1675 ISM-1676	14.1.3.6		4.2.1, 4.2.1.1, 8.3.11		
CRY-14	Cryptography	Public Key Infrastructure-based Authentication	Information systems are configured to follow an established certification path to an accepted trust anchor; in the case of network failure, a local cache of revocation data is maintained to support validation.														X		X			X																IA-05 (02)		ISM-1324 ISM-1323 ISM-1327			4.2.1, 4.2.1.1, 8.3.11		
CRY-15	Cryptography	Software Signing	Organization uses a software signing infrastructure to restrict access to organization's code signing private keys used to sign organization authorized software builds.			X						X															2.7						8.24												
DM-01	Data Management	Data Classification Criteria	Organization's data classification criteria are periodically reviewed, approved by management, and communicated to authorized personnel; the data security management team determines the treatment of data according to its designated data classification level.	X	X	X	X			X		X		X	X	X	X	X	X	X	X	X	X	X	ID.AM-5	AM-06 CRY-01 OPS-11 OPS-12	3.1 3.7	8.1.9.1 8.1.10.2			4 91 92 93		5.12		A.10.12 A.10.2 A.10.4 A.10.5 A.10.6 A.10.7 A.11.2	MP-06 RA-02 SI-12	MP-06 RA-02 SI-12	MP-06 RA-02 SI-12	164.308(a)(1)(i)	ISM-0810 ISM-1083 ISM-0393 ISM-0462	8.2.1.1 8.2.1.2 8.2.1.3 8.2.1.4 8.2.1.5 8.2.1.6 8.2.1.7 8.2.1.8 8.2.1.9 8.2.1.10 8.2.2.1 8.2.2.2 8.2.2.3 8.2.2.4 8.2.2.5 8.2.2.6 8.2.3.1 8.3.1.1 18.1.3.1 18.1.3.6 18.1.3.12 7.1.2.4	3.3 11.1	3.2.1	3.1.1 10.1.1	CC3.2 CC6.1 CC6.5 C1.1
DM-02	Data Management	Data Inventory	Organization should identify, label and classify Data based on the Data Classification Criteria.	X	X	X	X			X		X		X	X	X	X	X	X	X	X	X	X	X	ID.AM-5	AM-06 CRY-01 OPS-11 OPS-12	3.1 3.7	8.1.9.1 8.1.10.2			4 91 92 93		5.12		A.10.12 A.10.2 A.10.4 A.10.5 A.10.6 A.10.7 A.11.2	MP-06 RA-02 SI-12	MP-06 RA-02 SI-12	MP-06 RA-02 SI-12	164.308(a)(1)(i)	ISM-0810 ISM-1083 ISM-0393 ISM-0462	8.2.1.1 8.2.1.2 8.2.1.3 8.2.1.4 8.2.1.5 8.2.1.6 8.2.1.7 8.2.1.8 8.2.1.9 8.2.1.10 8.2.2.1 8.2.2.2 8.2.2.3 8.2.2.4 8.2.2.5 8.2.2.6 8.2.3.1 8.3.1.1 18.1.3.1 18.1.3.6 18.1.3.12 7.1.2.4	3.3 11.1	3.2.1	3.1.1 10.1.1	CC3.2 CC6.1 CC6.5 C1.1
DM-03	Data Management	Terms of Service	Consent is obtained for Organization's Terms of Service (ToS) prior to collecting personal information and when the ToS is updated.				X													X			X					8.2.4.5													16.1.7.13.PB			10.1.2	
DM-04	Data Management	Personal Information Access Requests	In accordance with Organization policy, upon request, authenticated individuals are provided with a copy of their personal information or disclosures of their personal information in an understandable form and within the defined timeframe.											X									X												A.1.1									10.1.5	
DM-05	Data Management	Personal Information Deletion Requests	In accordance with Organization policy, Organization processes requests for the deletion of personal information.											X									X												A.1.1									10.1.6	
DM-06	Data Management	External Privacy Inquiries	In compliance with Organization policy, Organization reviews privacy-related inquiries, complaints, and disputes.							X																					91														
DM-07	Data Management	Test Data Sanitization	Restricted data is redacted prior to use in a non-production environment.		X					X		X							X	X		X	X			DEV-10					87 88 89 90		8.33							ISM-1420 ISM-1273 ISM-1274	14.3.1.1 12.1.4.9 14.3.1.2 14.3.1.3 14.3.1.4 14.3.1.5 14.3.1.6		6.5.5, 6.5.6	9.1.2	
DM-08	Data Management	Personal Information Updates	Organization allows authenticated users to review and update their personal information.											X																					A.1.1										
DM-09	Data Management	Credit Card Data Restrictions	Organization does not store full track credit card data, credit card authentication information, credit card verification code, or credit personal identification number (PIN) which Organization processes for payment.																			X																					3.3, 3.3.1, 3.3.1.1, 3.3.1.2, 3.3.1.3		
DM-10	Data Management	Primary Account Number Data Restrictions	Organization restricts primary account number (PAN) data such that only the first six and last four digits are displayed; authorized users with a legitimate business need may be provided the full PAN.									X					X					X											8.11										3.4, 3.4.1, 3.4.2		
DM-11	Data Management	Personal Information Inventory	Organization maintains a documented inventory of media containing personal information.			X											X										3.2																		
DM-12	Data Management	Changes to Data at Rest	Organization uses mechanisms to detect direct changes to the integrity of customer data and personal information; Organization takes action to resolve confirmed unauthorized changes to data.			X	X										X					X	X				3.12	8.1.4.11 8.2.4.5										SC-04 SI-07					11.6, 11.6.1	8.1.3 10.1.3	
DM-13	Data Management	Data Processing Integrity	System checks are in place to ensure both complete and accurate capture of data in process.			X	X																X				3.12	8.1.2.2 8.1.4.4 8.1.4.7 8.2.4.5																10.1.3	
DM-14	Data Management	Secure Disposal of Media	Organization securely erases media containing decommissioned restricted data and obtains a certificate or log of erasure; media pending erasure are stored within a secured facility.	X	X	X	X			X		X			X	X	X	X	X	X	X	X	X	X	PR.IP-6	AM-01 AM-04	3.5	8.1.4.10 8.1.10.4 8.2.4.7			85 86		7.14 8.10			MA-02 MP-06	MA-02 MP-06 SR-12	MA-02 MP-06 MP-04	164.310(d)(2)(i) 164.310(d)(2)(ii)	ISM-1741 ISM-0311 ISM-1742 ISM-1223 ISM-1550 ISM-0316 ISM-1642 ISM-0363 ISM-1361 ISM-0370 ISM-0371 ISM-0372 ISM-0373 ISM-0840 ISM-0374 ISM-0375	8.3.2.1 8.3.2.2 8.3.2.3 8.3.2.4 8.3.2.5 8.3.2.6 8.3.2.7 8.3.2.8 11.2.7.1 11.2.7.2 11.2.7.3 11.2.7.4.PB	11.1	3.2.1, 9.4.6, 9.4.7	8.1.2 11.2.3	CC6.5 C1.2
DM-15	Data Management	Customer Data Retention and Deletion	Organization purges or archives data according to customer requests or legal and regulatory mandates.		X	X				X			X							X	X	X	X	X		PI-03	3.5				99			CLD.8.1.5							12.7.1.4 13.2.1.7	11.1	3.2.1, 9.4.6, 9.4.7	10.1.1	C1.1 C1.2
DM-16	Data Management	Removal of PHI from Media	Organization removes electronic protected health information from electronic media if the media is made available for re-use.															X																					164.310(d)(2)(ii)						
DM-17	Data Management	Secure Disposal of Media: Testing	Organization tests sanitization procedures and equipment annually for effectiveness.												X	X	X		X																	MP-06	MP-06 SR-12	MP-06		ISM-0313 ISM-1741 ISM-0311 ISM-1742 ISM-1223 ISM-1550 ISM-0316 ISM-1600 ISM-0947 ISM-0348 ISM-0351 ISM-1735 ISM-0368 ISM-0370 ISM-0371 ISM-0372 ISM-0373 ISM-0374 ISM-0375					
DM-18	Data Management	Personal Information Retention and Deletion	Organization retains and deletes personal information from Organization and service provider systems in accordance with Organization policy.			X								X						X			X				3.4 15.7								A.9.3						12.3.1.15 18.1.3.8 18.1.3.9 18.1.3.10 18.1.3.11			8.1.2 10.1.6	
DM-19	Data Management	Temporary Storage of Personal Information	Temporary files and documents containing personal information are deleted in accordance with a timeframe consistent with Organization policy.											X					X																A.4.1					ISM-1245					
DM-20	Data Management	Social Media	Sharing Organization restricted data via messaging technologies, social media, and public websites is prohibited.													X	X		X	X		X															PL-04 (01)	PL-04 (01)		ISM-0820 ISM-1146	8.3.1.10 14.1.1.10		4.2.2		
DM-21	Data Management	Publicly Accessible Content	Organization protects its public information system presence with the following processes: only authorized and trained individuals may post public information, content is reviewed prior to publishing, information on public systems is reviewed periodically, and non-public information is removed from public systems upon discovery.													X	X																				AC-22 PL-04 (01)	AC-22 IR-09 (02)		ISM-1146 ISM-0821 ISM-0824					
DM-22	Data Management	Data Loss Prevention	Data loss prevention capabilities are implemented to protect sensitive information as it is stored, transmitted, and processed.			X																	X				3.13																	10.1.4	
EM-01	Entity Management	Board of Directors Structure and Purpose	The Board of Directors provides corporate oversight, strategic direction, and review of management for Organization. The Board of Directors meets at least quarterly and has 3 sub-committees: • Audit Committee • Executive Compensation and Nominating Committee • Governance Committee					X			X										X			X					4.1			5.1										3.1			CC1.1

EM-02	Entity Management	Audit Committee	The Audit Committee is governed by a Charter, is independent from Organization Management, composed of outside directors (Industry Experts), and meets quarterly. The Audit Committee oversees: •Financial Statement Quality •Enterprise Risk Management •Regulatory & Legal Compliance •Internal Audit Functions •Information Security Functions •External Audit Functions				X	X			X	X								X	X			X				8.1.7.4	4.1 4.2.2(a) 4.2.2(b)			5.1 5.3	5.31								3.1.4.2 3.1.5.1 4.4.2.1 6.1.4.1 6.1.4.2 6.1.4.3 6.1.4.4 6.1.4.5 6.1.4.6 18.1.1.1 18.1.1.2 18.1.1.3 18.1.1.5.P	3.1			CC1.2
EM-03	Entity Management	Organizational Structure	Organization Management ensures that its organization is aligned with the corporate strategy by assigning key managers with responsibilities to execute the corporate strategy.								X	X							X													5.1a	5.2							ISM-1617 ISM-0717 ISM-0039					
EM-04	Entity Management	Operating Plans	Annual operating plans are aligned with Corporate Objectives, which are established on an annual basis during the Company's planning process. Priorities are set and plans are communicated appropriately.								X								X													5.1 (a) 7.1								ISM-0724					
EM-05	Entity Management	Cyber Security Insurance	Organization purchases cyber security insurance to mitigate risk of material financial impact that could result from a cyber security event.								X									X	X			X								7.1									6.2.2.18 14.1.2.12 14.1.2.13	4.4			CC9.1
EM-06	Entity Management	Internal Audit Function	Quarterly, the Chief Audit Executive meets with the Audit Committee to review key risk issues. The Audit Committee approves the annual Internal Audit Plan. Results of quarterly audits and subsequent issue tracking summaries are presented to the Audit Committee.								X									X												9.2									3.1.4.1 12.7.1.2 14.1.1.2 18.2.1.7 18.2.1.12.P 18.2.1.13.P 18.2.2.3 18.2.2.4 18.2.2.5 18.2.2.6				
EM-07	Entity Management	Financial Control Review	Internal financial control assessment results are reported to the Audit Committee by the Chief Audit Executive on a quarterly basis and support the CEO/CFO 302/404 certifications.								X																					9.2													
EM-08	Entity Management	Information Security Function	Quarterly, the Chief Security Officer meets with the Audit Committee to review key Information Security issues. Results of continuous monitoring activities and current security compliance status are presented to the Audit Committee and the Board of Directors.				X				X								X	X								8.1.7.4				9.3								ISM-1478	3.1.4.4 3.1.6.1				
EM-09	Entity Management	Information Security Compliance Review	Information Security compliance results are reported to the Audit Committee by the Chief Security Officer on a quarterly basis and support information security compliance certifications														X			X	X		X	X														AU-07			4.6.2.6 18.2.1.6 18.2.1.8 18.2.2.7	3.1 4.5 15.1		1.3.1	CC4.2
EM-10	Entity Management	Common Controls Framework	Organization maintains a Common Control Framework (CCF) that is used in the implementation of control measures as a risk mitigation strategy to support organization operations, technology infrastructure, and security management activities.																					X																					CC5.1 CC5.2
EM-11	Entity Management	Service Agreement	When customers sign-up for Organization's product and services, the customer is required to acknowledge a service agreement which includes considerations for protecting security, availability, confidentiality and indicates the responsibilities of the users and organization's responsibilities and commitments.		X																			X		COM-01 OIS-02 OIS-03 PI-02																			CC2.3 CC3.1
IAM-01	Identity and Access Management	Logical Access Provisioning	Logical access provisioning to information systems requires approval from appropriate personnel.	X	X	X	X		X	X		X		X	X	X	X	X	X	X	X	X	X	X	PR.AC-1	DEV-07 IDM-01 IDM-02 IDM-06 OIS-04 OPS-16	5.6 6.1 6.7	8.1.3.2 8.1.4.2 8.1.7.3 8.2.3.1 8.2.4.2 (a)		Secure Configuration	2 3 4 14 15 16 17 88 89 90		5.9 5.15		A.10.9	AC-01 AC-02 AC-03 CP-09 IA-04 IA-05 MP-02	AC-01 AC-02 AC-03 CP-09 IA-04 IA-05 MP-02 CM-05	AC-01 AC-02 AC-03 CP-09 IA-04 IA-05 MP-02 AC-04 (21)	164.308(a)(3)(i) 164.308(a)(3)(ii)(A) 164.308(a)(3)(ii)(B) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)© 164.312(a)(1) 164.312(c)(1)	ISM-1733 ISM-1610 ISM-1611 ISM-1612 ISM-1614 ISM-1615 ISM-1271 ISM-1272	6.1.2.1 9.1.1.1 9.1.1.2 9.1.1.3 9.2.1.1 9.2.1.3 9.2.1.4 9.2.1.5 9.2.2.2 9.2.2.3 9.2.2.4 9.2.2.5 9.2.2.6 9.2.2.7 9.2.6.2 9.2.6.3 9.2.6.4 9.3.1.2 9.4.1.1 9.5.1.1.P 12.6.2.4 15.1.1.1	9.1 11.4	7.2, A3.4	2.1.2 7.1.1 8.3.1	CC6.2 CC6.3
IAM-02	Identity and Access Management	Change of Access Notification	Changes made to system access trigger a notification that is sent to designated personnel.			X									X	X	X		X			X	X				3.14									**AC-02**	AC-02	AC-02 AC-02 (04)		ISM-1650 ISM-1651 ISM-1652			7.2.3, 8.2.4	7.3.2	
IAM-03	Identity and Access Management	Logical Access De-provisioning	Logical access that is no longer required in the event of a termination is documented, communicated to management, and revoked.	X	X	X	X		X	X					X	X	X	X	X	X	X	X	X	X	PR.AC-1	IDM-01 IDM-02 IDM-03 IDM-04	6.2 15.7	8.1.4.2 8.1.8.4		Secure Configuration User Access Control	2 3 14 15 16 17 60					AC-02 PS-04	AC-02 PS-04	AC-02 PS-04 AC-02 (02)	164.308(a)(3)(i) 164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)© 164.308(a)(4)(i) 164.308(a)(4)(ii)© 164.312(a)(1) 164.312(c)(1)	ISM-0430 ISM-1591 ISM-1404 ISM-1648 ISM-1716 ISM-1647 ISM-1734	7.3.1.1 7.3.1.2 7.3.1.3 9.2.1.1 9.2.2.1 9.2.6.1 9.2.6.5 9.2.6.6 9.4.1.1 9.5.1.1.P	9.1	8.2.4, 8.2.5	2.1.3 7.1.1	CC6.2 CC6.3
IAM-04	Identity and Access Management	Logical Access De-provisioning: Notification	The People Resources system sends a notification to relevant personnel in the event of a termination of an information system user.			X	X								X	X	X					X					6.2	8.1.8.2								PS-04	PS-04	PS-04 AC-02 (02)					8.2.4, 8.2.5		
IAM-05	Identity and Access Management	Logical Access Review	Organization performs account and access reviews on a quarterly basis; corrective action is taken where applicable.		X	X	X		X	X		X			X	X	X	X	X	X	X	X	X	X		IDM-01 IDM-02 IDM-03 IDM-04 IDM-05 OIS-04 OIS-07	5.1 5.3 5.5 6.8	8.1.3.2 8.1.4.2 8.1.10.6 8.2.3.1 8.2.4.2 (a)		Secure Configuration User Access Control User Access Control	15 17		5.18			IA-05 PS-05	IA-05 PS-05	IA-05 PS-05 AC-02 (03)	164.308(a)(3)(i) 164.308(a)(3)(ii)(A) 164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)© 164.308(a)(4)(i) 164.308(a)(4)(ii)© 164.312(a)(1)	ISM-0407 ISM-1610 ISM-1271 ISM-1272	9.2.5.1 9.2.5.2 9.2.5.3 9.2.5.4 9.2.5.5 9.2.5.6 9.4.1.1 9.4.4.9 11.1.2.1 11.1.2.2 12.5.1.17	9.1	8.2.6, A3.4.1	7.2.1	CC6.2 CC6.3
IAM-06	Identity and Access Management	Role Change: Access De-provisioning	Upon notification of an employee reassignment or transfer, management reviews the employee's access for appropriateness. Access that is no longer required is revoked and documented.			X	X								X	X	X					X	X				6.2	8.1.10.6								AC-02 PS-05	AC-02 PS-05	AC-02 PS-05					8.2.4	2.1.3	
IAM-07	Identity and Access Management	Shared Logical Accounts	Organization restricts the use of shared and group authentication credentials. Authentication credentials for shared and group accounts are reset every 90 days.		X		X											X	X	X		X		X		CRY-01		8.3.2.3											164.308(a)(5)(ii)(D)	ISM-0415	9.2.4.2 9.2.4.3 9.2.4.4 9.2.4.5 9.2.4.6 9.2.4.7 9.2.4.8 9.3.1.1		8.2.2, 8.2.3, 8.2.6		CC6.1
IAM-08	Identity and Access Management	Shared Logical Accounts: Group Member	Passwords for shared and group accounts are reset when a member of the shared group leaves.																			X																					8.2.2, 8.2.5		
IAM-09	Identity and Access Management	Shared Account Restrictions	Where applicable, the use of generic and shared accounts to administer systems or perform critical functions is prohibited; generic user IDs are disabled or removed.			X											X		X	X		X					4.7											AC-02 (09)		ISM-0380 ISM-0383	9.2.3.9		2.2.2, 8.2.2		
IAM-10	Identity and Access Management	Role Change: People Resources Notification	The People Resources system sends a notification to relevant management and relevant information system administrators in the event of an employee reassignment or transfer of an information system user.			X																X					6.1																7.2.3		
IAM-11	Identity and Access Management	Temporary Account Termination	Temporary and emergency accounts are automatically terminated 90 days from the date they are generated.						X								X		X											Secure Configuration User Access Control								AC-02 (01)		ISM-1610					
IAM-12	Identity and Access Management	Unique Identifiers	Organization requires unique identifiers for user accounts and prevents identifier reuse.		X	X	X			X		X		X	X	X	X	X	X	X	X	X		X		COS-06 IDM-01 OPS-24 PSS-07	3.14	8.1.4.1			15 17 21 22 23 24 25		5.16		A.10.8 A.10.10	AC-02 IA-04 IA-05 IA-08	AC-02 IA-04 IA-05 IA-08	AC-02 IA-04 IA-05 IA-08 IA-03 IA-04 (04)	164.312(a)(1) 164.312(a)(2)(i) 164.312(d)	ISM-0414 ISM-1583 ISM-1685 ISM-1262	9.4.1.1 9.4.1.2 9.4.1.3 9.4.1.4 9.4.1.5 9.4.1.6 9.4.1.7 9.4.2.1	9.1	8.2.1		CC6.1
IAM-13	Identity and Access Management	Password Authentication	User and device authentication to privileged information systems is protected by passwords that meet Organization's password complexity requirements.		X		X		X	X		X			X	X	X	X		X	X	X	X	X		COS-05 IDM-01 IDM-08 IDM-09 PSS-07		8.1.10.9		Secure Configurations User Access Control	15 17 18 19 20 21 22 23 24 25		5.17 8.5			AC-14 IA-05 (01)	AC-14 IA-05 (01) IA-02 (08)	AC-14 IA-05 (01)	164.308(a)(5)(ii)(D) 164.312(d)		9.4.2.3 9.4.2.5 9.4.2.6 9.4.2.7 9.4.2.8 9.4.2.13 9.4.3.1 9.4.3.2 9.4.3.3 9.4.3.4 9.4.3.5 9.4.3.6 9.4.3.7	9.1 9.3	8.3.5, 8.3.6, 8.3.9	7.3.2 10.2.1	CC6.1
IAM-14	Identity and Access Management	Multifactor Authentication	Multi-factor authentication is required for: • remote VPN sessions • access to trusted data environments	X	X	X	X			X					X	X	X	X	X	X	X	X	X	X	PR.AC-7	COS-02 COS-04 COS-05 COS-08 IDM-01 IDM-08 IDM-09 OPS-14 OPS-16	5.2 6.3 6.4 6.5 13.5	8.1.4.1 8.2.4.1			15 17 21 22 23 24 25 57 68 69					AC-20 IA-02 (01) IA-08 MA-04	AC-20 IA-02 (01) IA-02 (12) IA-08 MA-04 IA-02 (02)	AC-20 IA-02 (01) IA-02 (12) IA-08 MA-04 IA-02 (02)	164.312(d)	ISM-0974 ISM-1173 ISM-1504 ISM-1679 ISM-1680 ISM-1681 ISM-1505 ISM-1401 ISM-1682 ISM-1559 ISM-1683 ISM-1684	9.4.2.2.B	9.1 9.3	8.4, 8.4.1, 8.4.2, 8.4.3	7.3.1	CC6.1 CC6.6
IAM-15	Identity and Access Management	Authentication Credential Maintenance	Authorized personnel verify the identity of users before modifying authentication credentials on their behalf.							X					X	X	X		X	X		X									18 19 20					AC-14 IA-05 IA-05 (01)	AC-14 IA-05 IA-05 (01)	AC-14 IA-05 IA-05 (01) IA-03		ISM-1584 ISM-1491 ISM-1592 ISM-0382 ISM-1593	14.1.1.5		8.3.3		
IAM-16	Identity and Access Management	Session Timeout	Information systems are configured to terminate inactive sessions after 15 minutes or when the user terminates the session.		X	X	X		X						X	X	X	X	X	X		X				PSS-06	4.3	8.1.4.1		Secure Configuration						MA-04	MA-04	MA-04 AC-11 AC-12 SC-10 SC-23	164.312(a)(2)(iii)	ISM-1649 ISM-0853 ISM-0428	9.2.1.1 9.2.1.2 9.4.2.15 9.4.2.16 11.2.8.2 11.2.8.3 11.2.8.4		8.2.8		
IAM-17	Identity and Access Management	Session Limit	Information systems are configured to limit concurrent login sessions and the inactive user interface is not displayed when the session is terminated.		X														X			X				PSS-06														ISM-0853			8.2.8		
IAM-18	Identity and Access Management	Account Lockout: Cardholder Data Environments	Users are locked out of information systems after 6 invalid attempts for a minimum of 30 minutes, or until an administrator enables the user ID.			X	X		X						X	X	X			X		X					4.10	8.1.4.1		Secure Configuration						AC-07	AC-07	AC-07 AC-02 (05)			9.4.2.9		8.3.4		
IAM-19	Identity and Access Management	Account Lockout	Users are locked out of information systems after multiple, consecutive invalid attempts within a defined period; accounts remain locked for a defined period.			X											X		X			X					4.10											AC-02 (05) AC-11		ISM-1403			8.3.4		
IAM-20	Identity and Access Management	Login Banner	Systems leveraged by the U.S. Federal Government present a login screen that displays the following language: • users are accessing a U.S. Government information system • system usage may be monitored, recorded, and subject to audit • unauthorized use of the system is prohibited and subject to criminal and civil penalties • use of the system indicates consent to monitoring and recording													X	X																				AC-08	AC-08							
IAM-21	Identity and Access Management	Credentials Validation	Organization systems utilize Federal Identity, Credential, and Access Management (FICAM) components and conform to FICAM-issued profiles; systems verify and accept the following external credentials: • personal Identity Verification (PIV) credentials from federal agencies, and • FICAM-approved credentials from non-federal third-parties													X																					IA-08 (01) IA-08 (02) IA-08 (04)								
IAM-22	Identity and Access Management	Password Authentication Standard: Federal Systems	Organization information systems obscure feedback of authentication information during the authentication process (e.g., the system does not disclose error information such as "'user1' is not a valid username") and have the following password requirements: • minimum of 12 characters • contains at least one upper-case letter, lower-case letter, number, and a special character • at least one of the characters is changed when the new passwords are created. • the password life span is between 1 to 60 days • password reuse is prohibited for 24 generations • only allow the use of temporary password system logons with an immediate change to a permanent password			X									X	X			X	X							5.2									IA-06	IA-06			ISM-1595 ISM-1590	9.3.1.4				

IAM-23	Identity and Access Management	Privileged Session Management	Privileged logical access to trusted data environments is enabled through an authorized session manager; session user activity is recorded and tunnelling to untrusted data environments is restricted.			X	X					X			X	X	X		X	X		X	X				3.3 3.14 5.4	8.1.5.1 8.1.5.2 8.1.10.6					8.2			IA-05 IA-08 IA-11	IA-02 (12) IA-05 IA-08 IA-02 (08) IA-11	IA-02 (12) IA-05 IA-08 AC-02 (07) AC-06 (05) AC-06 (09) AC-06 (10) SC-23		ISM-1566 ISM-1509 ISM-1650 ISM-1651 ISM-1652 ISM-1620 ISM-1402 ISM-1385 ISM-1388 ISM-1705 ISM-1706 ISM-1707 ISM-1708 ISM-1429	9.2.3.1 9.2.3.2 9.2.3.3 9.2.3.4 9.2.3.5 9.2.3.6 9.2.3.7 9.2.3.8 9.2.3.10 9.2.3.11.PB 14.1.1.6 14.2.6.1		7.2.6	7.1.1 7.2.2	
IAM-24	Identity and Access Management	Zero Trust Enterprise Network	Organization users are authenticated against a Zero Trust model prior to gaining access to organization resources.									X		X																			5.17 5.15		A 1.1										
IAM-25	Identity and Access Management	Logical Access Role Permission Authorization	Initial permission definitions, and changes to permissions, associated with logical access roles are approved by authorized personnel.			X						X			X	X	X		X	X		X	X				6.1 6.8						8.3			AC-02	AC-02	AC-02 AC-05 AC-06 AC-06 (01) AC-06 (02)		ISM-0405 ISM-1507 ISM-1733 ISM-1508 ISM-1175 ISM-1653 ISM-0445 ISM-0441	14.1.2.3		7.2.1	7.2.1 8.1.4	
IAM-26	Identity and Access Management	Source Code Security	Access to modify source code is restricted to authorized personnel.							X		X					X		X	X		X	X								15 87		8.4					AC-06 (10)		ISM-1584 ISM-1491 ISM-1592 ISM-0382	9.4.5.1 14.2.6.2		7.2.1	2.1.2	
IAM-27	Identity and Access Management	Service Account Restrictions	Individual user or administrator use of service accounts for O/S, applications, and databases is prohibited.																X			X																		ISM-0341 ISM-1619 ISM-1261			8.2.1		
IAM-28	Identity and Access Management	PCI Account Restrictions	Organization clients with access to the cardholder data environment (CDE), as users or processes, are assigned unique accounts that cannot modify shared binaries or access data, server resources, or scripts owned by another CDE or Organization; application processes are restricted from operating in privileged-mode.																			X																					8.2.1		
IAM-29	Identity and Access Management	Least Privilege	Role-based access is defined and deployed to restrict privileged access to information resources based on the concept of least privilege.			X	X					X					X		X	X		X	X				3.3 5.4 6.8 12.2	8.1.4.2 8.1.5.3					5.3					AC-02 (07) AC-06 AC-06 (01) AC-06 (02) AC-06 (05)		ISM-1392 ISM-1746 ISM-0846 ISM-1748 ISM-1489 ISM-1546 ISM-0042 ISM-1380 ISM-1687 ISM-1688 ISM-1689 ISM-1387 ISM-1381 ISM-1705 ISM-1706 ISM-1707 ISM-1708 ISM-1249 ISM-1250 ISM-1263 ISM-1264 ISM-1256 ISM-1255 ISM-1268	9.1.1.16 9.4.2.4 9.4.4.1 9.4.4.3 9.4.4.7 12.6.2.2 15.1.1.5 12.7.1.3 6.1.2.3		7.2.1, 7.2.2, A1.1, A1.1.1, A1.1.2, A1.1.3 8.3.11	2.1.1 7.1.1 7.2.2 10.1.4	
IAM-30	Identity and Access Management	Virtual Private Network	Remote connections to the corporate network are accessed via VPN through managed gateways.		X	X	X			X		X			X	X	X	X	X		X	X		X		COS-02 COS-04 COS-05 COS-08 IDM-09	12.7 13.5	8.1.4.1			57 68 69		6.7			AC-20 MA-04	AC-20 MA-04	AC-20 MA-04	164.312(a)(2)(iv) 164.312(d)	ISM-1392 ISM-1746 ISM-0846 ISM-1748 ISM-1489 ISM-1546 ISM-0042 ISM-1380 ISM-1687 ISM-1688 ISM-1689 ISM-1381 ISM-1705 ISM-1706 ISM-1707 ISM-1708 ISM-1249 ISM-1250 ISM-1263 ISM-1264 ISM-1256 ISM-1255 ISM-1268 ISM-0611		9.3	12.2.1		CC6.1 CC6.7
IAM-31	Identity and Access Management	Virtual Private Network: Restrict Split-Tunneling	VPN configurations restrict split-tunneling capabilities.																X			X																		ISM-0705			12.2.1		
IAM-32	Identity and Access Management	Ability to Disable Remote Sessions	Organization has a defined process and mechanisms in place to expeditiously disable or disconnect remote access to information systems within a defined time frame based on business need.			X	X												X	X		X					13.5	8.1.10.6												ISM-1439	11.2.1.3		12.2.1		
IAM-33	Identity and Access Management	Remote Maintenance: Authentication Sessions	Vendor accounts used for remote access are enabled only during the time period needed, disabled when not in use, and monitored while in use.			X																X					13.5																8.2.7		
IAM-34	Identity and Access Management	Remote Maintenance: Unique Authentication Credentials for each Customer	Where applicable, Service providers with remote access to customer premises (e.g., for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.																			X																					8.2.3		
IAM-35	Identity and Access Management	Remote Maintenance: Authentication	Remote maintenance and diagnostic tool utilization are restricted to the minimum required level, strong authentication is required, and remote sessions are recorded.														X					X																MA-03 (01)					8.2.7		
IAM-36	Identity and Access Management	Remote Maintenance: Audit	Organization documents and maintains records for vendor remote maintenance, diagnostic activities, and permissions granted. A listing of vendor remote maintenance connections is documented as well.																			X																					8.2.7		
IAM-37	Identity and Access Management	End-user Environment Segmentation	Where applicable, processes that run as part of an Organization shared hosting platform will run under unique credentials that permit access to only one customer environment.																X	X		X																		ISM-1749	9.4.1.8.PB		8.2.3		
IAM-38	Identity and Access Management	End-user Access to Applications and Data	Organization applications secure user data and maintain confidentiality by default or according to permissions set by the individual; Organization authenticates individuals with unique identifiers and passwords prior to enabling access to: • use the application • view or modify their own data				X		X				X	X					X	X		X						8.2.4.2		Secure Configuration				CLD.9.5.1	A.1.1 A.10.13					ISM-0843 ISM-1490 ISM-1656 ISM-1657 ISM-1658 ISM-1582 ISM-1392 ISM-1746 ISM-0846	9.2.1.6.PB 9.2.2.8.PB 9.2.4.9.PB 14.1.2.2		8.3.10, 8.3.10.1		
IAM-39	Identity and Access Management	Hardware Tokens	Where applicable, hardware token-based authentication is facilitated only by approved organizations.																			X																					4.2.1, 4.2.1.1, 8.3.11		
IR-01	Incident Response	Incident Response Plan	Organization defines the types of incidents that need to be managed, tracked and reported, including: • procedures for the identification and management of incidents • procedures for the resolution of confirmed incidents • key incident response systems • incident coordination and communication strategy • contact method for internal parties to report incidents • support team contact information • notification to relevant management in the event of a security breach • provisions for updating and communicating the plan • provisions for training of support team • preservation of incident information • management review and approval, annually, or when major changes to the organization occur	X	X	X	X			X		X			X	X	X	X	X	X	X	X	X	X	ID.RA-4 PR.IP-9 RS.RP-1 RS.CO-3 RS.CO-2 RS.CO-1 RS.AN-4 RS.AN-2 RS.IM-1 RS.MI-1 RC.IM-1 RC.RP-1	COS-01 SIM-01 SIM-05	17.1 17.4 17.8 17.9	8.1.10.12			2 3 32 36 60		5.24 5.27 5.28			IR-04 IR-06 IR-07 IR-08	IR-04 IR-06 IR-07 IR-08 AT-02 (02)	IR-04 IR-06 IR-07 IR-08 IR-04 (01) IR-09 (03)	164.308(a)(6)(i) 164.308(a)(6)(ii)	ISM-0576 ISM-0125 ISM-0133 ISM-1609 ISM-1731 ISM-1732 ISM-0138 ISM-0123 ISM-0141 ISM-0043 ISM-0109 ISM-1228 ISM-0142	4.9.1.1 5.1.1.31.P 6.1.3.2 16.1.1.1 16.1.1.2 16.1.1.3 16.1.1.4 16.1.1.5 16.1.1.6.P 16.1.1.14 16.1.2.1 16.1.4.1 16.1.4.2 16.1.5.1 16.1.5.2 16.1.5.3 16.1.5.4 16.1.5.5 16.1.5.6 16.1.5.7 16.1.5.8 16.1.6.2 16.1.7.1 16.1.7.2	7.7 7.8 12.3	12.10.1	6.1.1 6.2.1	CC7.4 CC7.5
IR-02	Incident Response	Incident Response Testing	Organization tests incident response processes on an annual basis. Results from the tests are documented.		X	X	X										X					X	X			SIM-02	17.7	8.1.10.12										IR-03					12.10.2, 12.10.4, 12.10.4.1	5.1.3	
IR-03	Incident Response	Incident Response	Confirmed incidents are assigned a priority level and managed to resolution. If applicable, Organization coordinates the incident response with business contingency activities.	X	X	X				X		X			X	X	X	X	X	X	X	X	X	X	DE.DP-3 DE.DP-5 RS.CO-3 RS.CO-4 RS.MI-2 RS.IM-2	COS-01 OPS-20 SIM-01 SIM-02 SIM-03 SIM-05	17.9				2 3 32 36 60		5.25 5.26			IR-04 IR-05	IR-04 IR-05	IR-04 IR-05 IR-09 IR-03 (02)	164.308(a)(6)(i) 164.308(a)(6)(ii)	ISM-0125 ISM-0133 ISM-1609 ISM-1731 ISM-1732 ISM-0138 ISM-0123 ISM-0141	16.1.2.2 16.1.2.3 16.1.2.4 16.1.2.5 16.1.2.6 16.1.2.7 16.1.2.8 16.1.2.9 16.1.2.10 16.1.5.9 16.1.6.1 16.1.7.12	7.7 12.3	12.10.1	5.1.3 6.2.1	CC7.4
IR-04	Incident Response	External Communication of Incidents	Organization defines external communication requirements for incidents, including: • information about external party dependencies • criteria for notification to external parties as required by Organization policy in the event of a security breach • contact information for authorities (e.g., law enforcement, regulatory bodies, etc.) • provisions for updating and communicating external communication requirement changes	X	X	X	X	X		X				X					X	X	X	X	X	X	RC.CO-2	OIS-03 OPS-21 SIM-05	17.2 17.6	8.1.7.4 8.2.6.2	7.4(a)		1 5 32				A.9.1					ISM-1433 ISM-0140	6.1.3.1	12.1 12.3	12.10.1	5.1.1 5.1.2 6.2.1 8.1.3 8.2.1	CC2.3 CC7.4
IR-05	Incident Response	Incident Reporting Contact Information	Organization provides a contact method to: • submit complaints and inquiries • report incidents		X	X				X		X			X	X	X			X	X			X		OIS-05 SIM-04	17.3				32 60		6.8			IR-06	IR-06	IR-06			16.1.3.2 16.1.2.11.P 16.1.2.12.P	7.7			CC2.3
IR-06	Incident Response	Incident External Communication	Organization communicates a response to external stakeholders as required by the Incident Response Plan.	X	X	X	X							X						X	X	X	X	X	RS.CO-5	OPS-21 SIM-03	17.4 17.6	8.2.6.2							A.9.1						12.6.1.18.PB 16.1.2.13.P	7.7 12.3	12.10.1	5.1.2 6.1.1 6.2.1	CC2.3
IR-07	Incident Response	External Communication of Incidents: Protected Health Information	Organization communicates the discovery and status of the breach of Protected Health Information (PHI) to the covered entity within 60 days or as required by the Business Associates Agreement (BAA) and provides the following information if available: • description of the Event • description of the Information that was compromised • identification of the Individuals whose PHI were compromised • steps Required to Protect Individuals • investigation Plan • contact Information																																										
IR-08	Incident Response	Problem Management	Organization resolves customer support inquiries.																				X																					1.3.1 6.1.1 11.1.2 11.2.2	
MDM-01	Mobile Device Management	Mobile Device Enrollment	Mobile devices (i.e., laptops, smartphones, tablets) must be configured with the appropriate Mobile Device Management (MDM) profile when used as a medium to access Organization internal resources.		X	X	X					X			X	X	X		X	X		X				AM-05	1.1 4.11 4.12	8.3.3.1 8.3.3.2					8.1			AC-19 MP-07	AC-19 MP-07	AC-19 MP-07		ISM-1533 ISM-1195 ISM-1297 ISM-1082 ISM-0871	6.2.1.1 6.2.1.2 6.2.1.3 6.2.1.4 6.2.1.5 6.2.1.6 6.2.1.7 6.2.1.8 6.2.1.10 6.2.1.11 6.2.1.12 6.2.1.13 6.2.1.16 6.2.1.17 6.2.1.18 6.2.1.19 6.2.1.21 6.2.1.22 11.2.6.1		1.5, 1.5.1, 5.2, 5.2.1, 5.2.2, 5.2.3, 5.2.3.1, 5.3, 5.3.1, 5.3.2, 5.3.2.1, 5.3.3, 5.3.4, 5.3.5		
MDM-02	Mobile Device Management	Mobile Device Encryption	Mobile devices (i.e., laptops, smartphones, tablets) that are used to access data from Organization internal resources are encrypted.			X						X					X		X	X		X					3.6 3.9						8.1					AC-17 (02)		ISM-0869 ISM-1085 ISM-1084	6.2.1.1 6.2.1.9 6.2.1.15 10.1.1.3		1.5, 1.5.1, 5.2, 5.2.1, 5.2.2, 5.2.3, 5.2.3.1, 5.3, 5.3.1, 5.3.2, 5.3.2.1, 5.3.3, 5.3.4, 5.3.5		
MDM-03	Mobile Device Management	Configuration Management: Mobile Devices	Organization Mobile devices (i.e., laptops, smartphones, tablets) are configured to ensure unnecessary hardware capabilities and functionalities are disabled, and management defined security features are enabled.			X	X					X			X	X	X		X	X		X					4.3 4.8	8.3.3.2 8.3.4.1					8.1			AC-19	AC-19	AC-19		ISM-1400 ISM-1482 ISM-0863 ISM-0864 ISM-1366 ISM-0870	6.2.1.23		1.5, 1.5.1, 5.2, 5.2.1, 5.2.2, 5.2.3, 5.2.3.1, 5.3, 5.3.1, 5.3.2, 5.3.2.1, 5.3.3, 5.3.4, 5.3.5		
MDM-04	Mobile Device Management	Configuration Management: High Risk Travel Locations	Organization has a documented list of travel locations considered high risk for the use of mobile devices (i.e., laptops, smartphones, tablets). Employees procure alternate equipment before traveling to these locations.				X										X		X	X								8.1.10.3										CM-02 (07)		ISM-1298 ISM-1554 ISM-1555 ISM-1299 ISM-1088 ISM-1300 ISM-1556	6.2.1.1 6.2.2.2 6.2.2.3 6.2.2.9 6.2.2.10 6.2.2.11 6.2.2.12 6.2.2.13 6.2.2.14 6.2.2.15 6.2.2.16 6.2.2.17 6.2.2.19				

NO-01	Network Operations	Network Policy Enforcement Points	Network traffic to and from untrusted networks passes through a policy enforcement point; firewall rules are established in accordance with identified security requirements and business justifications.	X	X	X	X		X	X		X	X		X	X	X	X	X	X	X	X	X	X	PR.PT-4	COS-01 COS-03 COS-04 COS-05 COS-06 COS-08 OPS-24	4.4 4.5 12.5	8.1.2.1 8.1.3.1 8.1.3.2 8.1.10.6 8.2.2.1 8.2.3.1 8.3.2.3 8.2.2.1 (a)		Firewalls	4 8 9 10 24 25 73 74 75 76 77 94		8.2	CLD.13.1.4		CA-03 CM-07 SC-05 SC-07	CA-03 CM-07 SC-05 SC-07	CA-03 CM-07 SC-05 SC-07 SC-07 (04) SI-04 (04)	164.312(c)(1)	ISM-1416 ISM-1386 ISM-1528 ISM-0639	13.1.1.1 13.1.1.2 13.1.1.3 13.1.1.4 13.1.1.5 13.1.1.6 13.1.1.7 13.1.1.8 13.1.1.9 13.1.1.10 13.1.4.1.P 13.1.4.2.P 14.1.2.1 12.2.1.5	11.2	1.2	8.3.1	CC6.6
NO-02	Network Operations	Inbound and Outbound Network Traffic: DMZ Requirements	Network traffic to and from untrusted networks passes through a Demilitarized Zone (DMZ).		X		X		X			X							X	X		X	X			COS-02 COS-03 COS-04 COS-06 OPS-24		8.1.2.1 8.1.3.2 8.1.3.3		Firewalls			8.23							ISM-1181 ISM-1577 ISM-0637	13.1.3.1		1.4, 1.4.1	8.3.2	
NO-03	Network Operations	Ingress and Egress Points	Organization maintains an inventory of ingress and egress points on the production network and performs the following for each: • inventory is reduced to the minimum possible level • permitted ports, protocols and services are inventoried and validated • documents security features that are implemented for insecure protocols			X	X										X		X			X					4.5 4.6 12.1 12.2 12.6 13.9	8.1.4.4										CM-07 (01)		ISM-1502 ISM-1182 ISM-1627 ISM-1628 ISM-1427 ISM-0629			1.2.5, 1.2.6		
NO-04	Network Operations	Non-disclosure of Routing Information	Organization does not disclose private IP addresses and routing information to unauthorized parties.																			X																					1.4.3, 1.4.5		
NO-05	Network Operations	Dynamic Packet Filtering	Where applicable, Organization enables dynamic packet filtering on the network.			X	X								X	X	X		X			X					9.3 13.4 13.10	8.1.3.2								SC-05	SC-05	SC-05		ISM-1234 ISM-1289			1.3.1		
NO-06	Network Operations	Firewall Rule Set Review	Network infrastructure rule sets are reviewed every 6 months.						X										X			X								Firewalls										ISM-0521 ISM-1186 ISM-1428 ISM-1430			1.2.7		
NO-07	Network Operations	Ingress and Egress Points: Fail Secure	The information system fails securely in the event of an operational failure of a boundary protection device.				X										X					X						8.3.2.1										MA-06 SC-07 (18)					1.4.1		
NO-08	Network Operations	Traffic Flow: Managed Proxy	Organization requires egress traffic initiated from within the Organization network to pass through a managed proxy.			X											X		X			X					13.10											SC-07 (04) SC-07 (08)		ISM-0260 ISM-0963 ISM-0961 ISM-1237 ISM-1236 ISM-1171 ISM-0659 ISM-0651 ISM-0652 ISM-1524 ISM-1293 ISM-1389 ISM-0649 ISM-1284 ISM-1286 ISM-1287 ISM-0677			1.3.2		
NO-09	Network Operations	Domain Name Services Security Extensions (DNSSec)	Organization establishes a DNSSec implementation standard and uses mechanisms to verify the DNS infrastructure for compliance.			X										X			X								4.9 9.2										SC-21			ISM-1782					
NO-10	Network Operations	Email Spam Protection	Organization has documented procedures and protection mechanisms in place to protect its information and information systems from spam and ensures that signature definitions are updated whenever new releases are available.			X	X										X		X	X							9.1 9.5 9.6	8.1.3.4										SI-08 SI-08 (02)		ISM-0264 ISM-0267 ISM-0271 ISM-0272 ISM-1089 ISM-0565 ISM-1023 ISM-1024 ISM-1431 ISM-1458	13.2.1.2 13.2.3.6				
NO-11	Network Operations	Denial of Service (DOS)	Organization implements a Denial of Service (DOS) protection plan, identifies threatening DOS attacks, and configures boundary protection devices according to the DOS plan.				X												X									8.1.3.3 8.3.2.3												ISM-1019 ISM-1579 ISM-1431 ISM-1458 ISM-1435					
NO-12	Network Operations	Trusted Connections	All trusted connections are documented and approved by authorized personnel; management ensures the following documentation is in place prior to approval: • agreement with vendor • security requirements • nature of transmitted information			X	X								X	X	X		X			X					12.4	8.1.2.3 8.1.3.6 8.1.4.6								CA-03 SC-07 SC-21 SC-22	CA-03 SC-07 SC-21 SC-22	CA-03 SC-07 SC-21 SC-22		ISM-0516 ISM-0518 ISM-1178			1.3.1, 1.3.2		
NO-13	Network Operations	Network Segmentation	Production environments are logically segregated from non-production environments.	X	X	X	X			X		X			X	X	X		X	X	X	X	X	X	PR.DS-7 PR.AC-5	COS-05 COS-06 DEV-10 OPS-24	16.8	8.1.2.1 8.1.9.4			78 87 88 89 90		8.22 8.31			SC-39	SC-39	SC-39		ISM-0400 ISM-1419 ISM-1269 ISM-1270	9.5.1.2.P 9.5.1.3.P 12.1.4.1 12.1.4.2 12.1.4.3 12.1.4.4 12.1.4.5 12.1.4.6 12.1.4.7 13.1.3.1 13.1.3.2 13.1.3.3 13.1.3.4 13.1.3.5 13.1.3.6 13.1.3.7 13.1.3.10.P 13.1.3.11.P 14.2.1.1 14.2.6.7 12.2.1.14	5.7 5.8 11.2	6.5.3	8.3.2 8.3.3 10.1.4	CC6.1
NO-14	Network Operations	Card Processing Environment Segmentation	Where applicable, Organization segregates the Primary Account Number (PAN) infrastructure including payment card collection devices; Organization limits access to the segregated environment to authorized personnel.																			X																					6.5.3		
NO-15	Network Operations	Traffic Flow	Organization documents the approved traffic flow at each managed interface and configures the managed interface accordingly. Exceptions to traffic flow are documented, reviewed periodically, and removed when there is no longer a business requirement.			X	X					X					X		X			X					12.4	8.2.3.2					8.21					AC-04		ISM-0631 ISM-1192			1.3.1, 1.3.2		
NO-16	Network Operations	Disable Rogue Wireless Access Points	Organization employs mechanisms to detect and disable the use of unauthorized wireless access points.				X										X		X			X	X					8.1.2.3 8.1.4.6 8.3.2.3										AC-18 (01) SC-04		ISM-0345 ISM-1314 ISM-1315 ISM-1334 ISM-1338 ISM-1335			11.2, 11.2.1, 11.2.2	11.1.2	
NO-17	Network Operations	Wireless Access Points	Organization maintains an inventory of authorized wireless access points including a documented business justification.				X										X					X	X					8.3.2.1 8.3.2.3										AC-17 (03)					11.2, 11.2.1, 11.2.2	11.1.2	
NO-18	Network Operations	Authentication: Wireless Access Points	Organization restricts access to network services via wireless access points to authenticated users and services; approved wireless encryption protocols are required for wireless connections.			X	X								X	X	X		X	X		X					12.5 12.6	8.1.4.1 8.1.4.4 8.3.2.1 8.3.2.2								AC-18	AC-18	AC-18 AC-17 (01) AC-17 (03) AC-19 (05)		ISM-1532 ISM-0529 ISM-0530 ISM-0535 ISM-1364 ISM-0536 ISM-1317 ISM-1322 ISM-1454 ISM-0484 ISM-0485 ISM-1449 ISM-0487 ISM-0488 ISM-0489 ISM-0494 ISM-0496 ISM-1233	6.2.2.4 6.2.2.7 13.1.3.8 13.1.3.9		2.3, 2.3.1, 2.3.2, 4.2.1.2		
PR-01	People Resources	Background Checks	New hires are required to pass a background check as a condition of their employment.	X	X		X			X	X	X			X	X	X		X	X	X	X		X	PR.AC-6 PR.IP-11	HR-01		8.1.8.1			59 61 62	7.2	6.1			PS-03	PS-03	PS-03		ISM-0434	7.1.1.1 7.1.1.2 7.1.1.3 7.1.1.4 7.1.1.5 7.1.1.6 7.1.1.7 7.1.1.8 7.1.1.9 7.1.1.10 7.1.1.11 7.1.1.12 7.1.1.13 7.1.2.8 7.1.2.9	3.5	12.7, 12.7.1		CC1.4
PR-02	People Resources	Performance Management	Organization has established a check-in performance management process for on-going dialogue between managers and employees. Quarterly reminders are sent to managers to perform their regular check-in conversation.																					X																					CC1.4 CC1.5
PR-03	People Resources	Hiring Process	Job candidates apply for roles that are listed on the Organization career portal; candidates are interviewed to determine their knowledge and competence for their prospective roles and compatibility with Organization values.		X		X	X												X						HR-01		8.1.8.1 8.3.4.1	7.2(a) 7.2(b) 7.2© 7.2(d) 7.2												4.5.2.2 6.1.1.11 7.1.2.7 18.2.1.5				
PR-04	People Resources	Organization Property Collection	Upon employee termination, management is notified to collect Organization property from the terminated employee.		X		X			X		X			X	X	X			X						AM-05 HR-05		8.1.8.2			2 3 14 16 17 60		5.11			PS-04	PS-04	PS-04			6.2.2.21 8.1.3.2 8.1.4.1 8.1.4.2 8.1.4.4 8.1.5.2.P 8.1.5.3.P 9.2.2.1 9.2.6.1				
PR-05	People Resources	Exit Interviews	Upon employee termination, management conducts exit interviews for the terminated employee.		X										X	X	X									HR-05										PS-04	PS-04	PS-04							
PR-06	People Resources	Disciplinary Process	Employees that fail to comply with Organization policies are subject to a disciplinary process.		X			X		X	X	X			X	X	X	X		X				X		HR-04			7.3©		60	7.3(c)	6.4			PS-08	PS-08	PS-08	164.308(a)(1)(ii)(C)		4.5.2.8 7.1.2.6 7.2.3.1 7.2.3.2 7.2.3.3 7.2.3.4				CC1.5
PR-07	People Resources	Code of Ethics	Organization has a Code of Ethics for Senior Officers. The Senior Officers and CEO certify that they understand the Code on an annual basis.												X	X	X																			PL-04	PL-04	PL-04							
PR-08	People Resources	Business Ethics Hotline	Organization has a business ethics hotline for employees and external parties to report ethical misconduct. Allegations are investigated and Organization will take appropriate action for confirmed violations. Hotline reports are reported to the Audit Committee on a quarterly basis.												X	X	X			X				X												PS-08	PS-08	PS-08			7.2.1.7 18.1.2.13.PB				CC2.2
PR-09	People Resources	National Security Clearance	Organization conducts screening and rescreening of authorized personnel for roles that require national security clearances. For national security clearances; a reinvestigation is required during the 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance. In addition, for law enforcement and high impact public trust level, a reinvestigation is required during the 5th year.												X	X	X																			PS-03	PS-03	PS-03							
PR-10	People Resources	Code of Business Conduct	Organization has documented the Code of Business Conduct and Business Partner Code of Conduct, which are reviewed, updated if applicable, and approved by senior management annually.												X	X	X							X												PL-04	PL-04	PL-04							CC1.1
PRIV-01	Privacy	Privacy Program	Organization privacy policies for individuals, including relevant updates, are communicated on the public company website or on the internal corporate network.											X						X															A.7.1						18.1.4.1 18.1.4.2 18.1.4.3 18.1.4.4				
PRIV-02	Privacy	Privacy Program Review	On an annual basis, Organization performs a review of privacy practices to ensure the following: • consent is obtained for users whose personal information (PI) is managed by Organization • PI inventory integrity and accuracy • data access request response template is understandable • standard agreement templates are up-to-date • requests to delete, access or update PI are processed accurately and within a timeframe consistent with Organization policy • compliance with Organization's privacy commitments • known privacy issues are remediated • opt-in and opt-out compliance with applicable law • Organization privacy documentation and practices are relevant to applicable law • compliance with relevant industry Codes of Conduct (e.g., EDAA) • if applicable, joint controller responsibilities are clearly defined and communicated to both data controllers and the data subject									X		X					X														5.34		A.11.1					ISM-1451					
PRIV-03	Privacy	Privacy Readiness Review	Organization performs privacy readiness reviews to identify high-risk processing activities that impact personal data; identified non-compliance with Organization privacy practices is tracked through remediation.							X																					91														
PRIV-04	Privacy	Privacy Notice	Individuals are given appropriate notice and an opportunity to consent or decline to Organization privacy practices such as accessing, collecting, processing, transferring, or storing personal information.		X									X					X							IDM-07									A.2.1 A.2.2 A.7.1					ISM-0347 ISM-0663 ISM-0661					

PRIV-05	Privacy	Personal Information Notice and Consent: Additional Processing Activities	Where appropriate, Organization obtains individual consent for processing activities for which consent has not been previously obtained.		X		X							X												IDM-07		8.1.4.11							A.2.2										
PRIV-06	Privacy	Notice of Personal Information Disclosure	In accordance with Organization policy, Organization provides notice to individuals regarding legally-required disclosures of personal information.				X							X										X				8.2.4.5 (a)							A.5.1										C1.1
PRIV-07	Privacy	PII Processing Agreements	Personal information is handled and processed in accordance with contractual requirements.		X							X		X						X						PSS-12 INQ-2 INQ-3 INQ-4							5.34		A 2.1						18.1.5.6				
PRIV-08	Privacy	Record of Processing Activity	Organization documents, reviews, and approves a record of processing activities related to personal information.									X								X													5.34								18.1.4.6				
PRIV-09	Privacy	Document Management Standard: HIPAA	Documentation that impacts personal health information, including policies, procedures, and the documentation of actions, activities, or assessments, are retained for 6 years from the date of its creation, or the date when it last was in effect, whichever is later.															X																					164.316(b)(2)(i)						
PRIV-10	Privacy	Law Enforcement Requests	Law enforcement agencies may submit requests for evidence; submitted requests are reviewed and tracked to resolution.		X							X														INQ-01							5.34												
PS-01	Proactive Security	Endpoint Detection and Response	Endpoint Detection and Response (EDR) software is deployed to continuously monitor, detect, and respond to cyber threats and patterns of malicious behavior and activity.			X																					13.2 13.7																		
PS-02	Proactive Security	Threat Hunting	Organization performs threat hunting to identify, track, and disrupt threats that evade existing security controls.									X																					5.7												
PS-03	Proactive Security	Threat Modeling	Organization performs periodic threat modeling to ensure that potential threats are identified and assessed.			X																					16.14																		
PS-04	Proactive Security	Adversary Intelligence	Organization gathers intelligence on adversary personas to assist in the prioritization of security activities.									X																					5.7												
RM-01	Risk Management	Service Risk Rating Assignment	Annually, Organization prioritizes the frequency of vulnerability discovery activities based on an assigned service risk rating.							X	X				X	X	X		X			X									1 6 7 47 48 49	4.1 8.1 8.2 8.3 10.2 6.1.1 6.1.2 6.1.3 6.2(c) 9.1				CA-07	CA-07	CA-07 RA-05 (02) RA-05 (03)		ISM-1608 ISM-1588 ISM-1698 ISM-1699 ISM-1700 ISM-1701 ISM-1702 ISM-1752 ISM-1703 ISM-1616 ISM-1755			12.3, 12.3.1, 12.3.2, 12.3.3, 12.3.4		
RM-02	Risk Management	Risk Assessment	Organization management performs an annual risk assessment. Results from risk assessment activities are reviewed to prioritize mitigation of identified risks.	X	X			X		X	X				X	X	X		X	X	X	X		X	ID.GV-4 ID.RA-6 ID.RM-1 ID.RM-2 ID.RM-3	COM-03 DEV-01 OIS-04 OIS-06 OIS-07 OPS-20 SSO-05			6.1.1(a) 6.1.1(b) 6.1.1.(c) 6.1.2(b.2) 8.2.3(a) 8.2.3(b) 8.2.3© 8.3.1 8.3.2(a) 8.3.2(b) 8.3.2© 8.3.2(d)		1 5 6 7 47 48 49	4.1 8.1 8.2 8.3 10.2 6.1.1 6.1.2 6.1.3 6.1.3(a) 6.1.3(b) 6.1.3(e) 6.1.3(f) 6.2(c) 9.1				CA-07 (04)	RA-03 CA-07 (04)	RA-03 SA-09 (01)		ISM-0726 ISM-1587 ISM-1631 ISM-1567 ISM-1563 ISM-1588	3.1.2.2 3.1.3.1 3.1.4.3 4.4.6.1 4.4.7.1 4.4.7.2 4.4.7.3 4.4.7.4 4.4.8.1 4.4.8.4 4.4.8.5 4.5.4.1 4.5.5.1 4.6.1.1 4.8.1.1 4.9.2.1 4.9.2.2 6.1.1.3 14.1.1.1 14.2.6.3 14.2.6.4 14.2.6.5 14.2.6.9 14.2.6.10	3.1 4.1 4.2 4.3	12.3, 12.3.1, 12.3.2, 12.3.3, 12.3.4		CC3.2 CC3.3 CC3.4 CC9.1
RM-03	Risk Management	Risk Assessment: HIPAA Criteria	Organization's periodic risk assessment for systems that process, transmit or store Protected Health Information (PHI) includes the following: • identify and classify assets • identify threats • identify vulnerabilities • identify controls • perform threat likelihood analysis • perform threat impact analysis • identify residual risk • identify appropriate safeguards															X																					164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(8)						
RM-04	Risk Management	Continuous Monitoring	The design and operating effectiveness of internal controls are continuously evaluated against the established Common Controls Framework by Organization. Corrective actions related to identified deficiencies are tracked to resolution.		X		X	X		X	X	X			X	X	X	X	X	X	X	X	X	X		COM-02 COM-03		8.1.10.6	8.1(a) 8.1(b)		2 3 5 47 48 49	9.1 9.3 10.1	5.29			CA-05 CA-07	CA-05 CA-07	CA-05 CA-07	164.308(a)(8)	ISM-1700 ISM-1701 ISM-1702 ISM-1752 ISM-1703	3.1.4.2 4.4.8.2 4.4.8.3 4.5.4.1 4.5.4.3 4.6.2.3 4.6.2.4 4.6.3.1 4.7.1.2 4.7.1.3 4.7.1.4 4.7.1.6 12.7.1.1 12.7.1.5 12.7.1.6 18.2.1.2 18.2.1.3 18.2.1.4 18.2.2.1 18.2.2.2 18.2.3.1 18.2.3.2	3.2 4.1 15.1	12.3, 12.3.1, 12.3.2, 12.3.3, 12.3.4, A3.3.3	2.2.1	CC2.1 CC4.1 CC4.2
RM-05	Risk Management	Self-Assessments: PCI	On a quarterly basis, reviews shall be performed with approved documented specification to confirm personnel are following security policies and operational procedures pertaining to: • daily log reviews • firewall rule-set reviews • applying configuration standards to new systems • responding to security alerts • change management processes																X			X																		ISM-1294			12.4.2, 12.4.2.1		
RM-06	Risk Management	Internal Audits	Organization establishes internal audit requirements based on the Common Controls Framework by Organization and executes audits on information systems and processes at planned intervals.		X			X		X	X	X			X	X	X			X						COM-03			8.6(d) 9.2.1(a.1) 9.2.2(a.2) 9.2.3(b) 9.2.2(a) 9.2.2.(b) 9.2.2.(c) 9.2.2.(d) 9.2.2.(e) 9.2.2.(g)		2 3 5	9.2	5.36 8.34			AU-01 CA-05 CA-07	AU-01 CA-05 CA-07	AU-01 CA-05 CA-07			4.6.2.2 4.6.2.7				
RM-07	Risk Management	ISMS Internal Audit Requirements	Internal audit establishes and executes a plan to evaluate applicable controls in the Information Security Management System (ISMS) at least once every 3 years.								X				X	X	X			X												9.2				CA-02	CA-02	CA-02			4.7.1.5				
RM-08	Risk Management	Remediation Tracking	Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.			X		X		X	X				X	X	X			X		X					16.3		6.1.2(a) 6.1.2(b.1) 9.2.2(f) 10.1.1 10.1.2(a.1) 10.1.2(a.2) 10.1.2(b.1) 10.1.2(b.2) 10.1.2(b.3) 10.1.2© 10.1.2(d) 10.1.2€ 10.1.2		5 6 7	6.1.3(e) 6.1.3(f) 8.3 10.1 10.2				RA-03 RA-07	RA-03 RA-07	RA-03			4.5.5.2 4.7.1.1 12.7.1.8		12.3, 12.3.1, 12.3.2, 12.3.3, 12.3.4		
RM-09	Risk Management	ISMS Corrective Action Plans	Management prepares a Corrective Action Plan (CAP) to manage the resolution of nonconformities identified in independent audits.								X				X	X	X		X	X												6.1.3(e) 6.1.3(f) 10.1 10.2				RA-03	RA-03	RA-03		ISM-1564	3.1.5.2				
RM-10	Risk Management	Statement of Applicability	Management prepares a statement of applicability that includes control objectives, implemented controls, and business justification for excluded controls. Management aligns the statement of applicability with the results of the annual risk assessment.							X	X											X									2 3 5	6.1.3(b) 6.1.3(c) 6.1.3(d)											12.3, 12.3.1, 12.3.2, 12.3.3, 12.3.4		
SDD-01	System Design Documentation	System Documentation	Documentation of system boundaries and key aspects of their functionality are published to authorized Organization personnel on the Organization intranet.		X	X	X								X	X	X				X	X		X		COS-07 COS-08 PI-01	3.8	8.1.9.5								CA-03 CA-09 SA-05	CA-03 CA-09 SA-05	CA-03 CA-09 SA-05				5.6	12.5.1, 12.5.2, 12.5.2.1, 12.5.3		CC2.2
SDD-02	System Design Documentation	Whitepapers	Organization publishes whitepapers to its public website that describe the purpose, design and boundaries of the system and system components.		X		X													X				X		COS-02 COS-07 COS-08 OIS-03 PI-01 PSS-01		8.2.2.1 8.2.4.5 8.2.4.6 8.2.5.1													4.5.3.1 6.1.3.3.PB 6.3.1.1.PB 8.2.2.7.PB 10.1.1.9.PB 10.1.1.10.P 13.1.1.11.P 13.1.3.12.P 14.1.1.19.P 14.2.1.13.PB 16.1.1.7.P 16.1.1.8.P 16.1.1.9.P 16.1.1.10.P 16.1.1.11.P 16.1.1.12.P 16.1.1.15.P 18.1.1.4.P 18.1.1.6.P 18.1.1.7.P 18.1.3.13.PB 18.1.5.7.PB 18.2.1.9.P 10.1.2.20.PB				CC2.3
SG-01	Security Governance	Policy and Standard Review	Organization's policies and standards are periodically reviewed, approved by management, and communicated to Organization personnel.	X	X	X	X	X		X	X	X		X	X	X	X	X	X	X	X	X	X	X	ID.GV-1 ID.AM-6	AM-02 COM-01 COM-02 COM-03 COS-08 CRY-01 DEV-01 DEV-03 IDM-01 OIS-02 OIS-06 OPS-04 OPS-06 OPS-10 OPS-11 OPS-12 OPS-18 SP-01 SP-02	7.1 11.1 12.4 18.1	8.1.5.4 8.2.5.1	4.1 5.2.1(a) 5.2.1(b) 5.2.1© 5.2.1(d) 5.2.2(a) 5.2.2(b) 5.2.2© 7.3(a)		1 2 3 4 27 28 88 89 90	5.1(a) 5.1(d) 5.2(d) 5.2(e) 5.2(g) 7.3(a) 7.3(b) 7.3(c) 7.5.1(b) 7.5.2(a) 7.5.2(b) 7.5.2(c) 7.5.3(a) 7.5.3(b) 7.5.3(c) 7.5.3(d) 7.5.3(e) 7.5.3(f)	5.1		A.9.2 A.10.12	PL-01 PS-06	PL-01 PS-06	PL-01 PS-06	164.308(a)(1)(i) 164.308(a)(3)(i) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)© 164.308(a)(7)(i) 164.308(a)(7)(ii)(D) 164.308(a)(8) 164.310(a)(1) 164.312(c)(1) 164.316(b)(1)(i) 164.316(b)(1)(ii) 164.316(b)(2)(ii) 164.316(b)(2)(iii)	ISM-0888 ISM-1602	3.1.3.2 4.4.1.1 4.4.5.1 4.4.5.3 4.5.2.6 4.5.2.7 4.8.1.1 4.8.2.1 4.8.2.2 5.1.1.1 5.1.1.2 5.1.1.3 5.1.1.4 5.1.1.5 5.1.1.6 5.1.1.8 5.1.1.9 5.1.1.10 5.1.1.11 5.1.1.12 5.1.1.13 5.1.1.14 5.1.1.15 5.1.1.16	3.1 3.2 4.4 5.1 5.4 7.1	1.1, 1.1.1, 2.1, 2.1.1, 3.1, 3.1.1, 4.1, 4.1.1, 5.1, 5.1.1, 6.1, 6.1.1, 7.1, 7.1.1, 8.1, 8.1.1, 9.1, 9.1.1, 10.1, 10.1.1, 11.1, 11.1.1, 12.1, 12.1.1, A3.1.3	1.1.1 1.1.2	CC2.2 CC5.3
SG-02	Security Governance	Exception Management	Organization reviews exceptions to policies, standards and procedures; exceptions are documented and approved based on business need and removed when no longer required.		X	X	X			X										X	X			X		SP-03	2.2	8.1.5.1			1 2 3										5.1.1.1 5.1.1.7	3.2			CC3.2 CC5.3
SG-03	Security Governance	Document Control	Organization's document management criteria is periodically reviewed, approved by management, and communicated to authorized personnel; management determines the treatment and retention of documentation according to legal and regulatory requirements.		X		X	X						X					X	X		X				SP-01		8.1.5.4	4.2.2 © 7.5.2(a) 7.5.2(b) 7.5.2© 7.5.3.1(a) 7.5.3.1(b) 7.5.3.2(a) 7.5.3.2(b) 7.5.3.2© 7.5.3.2(d)						A.9.2					ISM-0047	5.1.2.2		1.1, 1.1.1, 2.1, 2.1.1, 3.1, 3.1.1, 4.1, 4.1.1, 5.1, 5.1.1, 6.1, 6.1.1, 7.1, 7.1.1, 8.1, 8.1.1, 9.1, 9.1.1, 10.1, 10.1.1, 11.1, 11.1.1, 12.1, 12.1.1		

SG-04	Security Governance	Information Security Program Content	The Chief Security Officer conducts a periodic staff meeting to communicate and align on relevant security threats, program performance, and resource prioritization.	X	X					X	X	X			X	X	X	X	X	X		X		X	ID.AM-3 PR.IP-8	COM-01 OIS-05 SP-01					1 2 3 4 5 15 24 25 60 68 69 73	5.1 5.1(e) 5.1(f) 5.1(g) 5.1(h) 6.2(b) 7.5.2 7.5.2(a) 7.5.2(b) 8.1 6.3	5.35 8.26			AT-01 CA-06 IA-01 PL-02	AT-01 CA-06 IA-01 PL-02 SA-02	AT-01 CA-06 IA-01 PL-02 SA-02	164.308(a)(5)(ii)(A)	ISM-0432	3.1.3.3 4.4.1.1 4.6.1.2 4.8.2.1 11.2.9.6		12.4.2, 12.4.2.1		CC1.3 CC3.1
SG-05	Security Governance	Procedures	Organization's key control capabilities are supported by documented procedures that are communicated to authorized personnel.									X			X	X	X			X		X											5.37			AC-01 AT-01 AU-01 CA-01 CM-01 IA-01 IR-01 IR-08 MA-01 MP-01 PE-01 PL-01 PL-02 PS-01 RA-01 SA-01 SC-01 SI-01	AC-01 AT-01 AU-01 CA-01 CM-01 IA-01 IR-01 IR-08 MA-01 MP-01 PE-01 PL-01 PL-02 PS-01 RA-01 SA-01 SC-01 SI-01	AC-01 AT-01 AU-01 CA-01 CM-01 IA-01 IR-01 IR-08 MA-01 MP-01 PE-01 PL-01 PL-02 PS-01 RA-01 SA-01 SC-01 SI-01			8.1.4.3 12.1.1.1 12.1.1.2 12.1.1.4 12.1.1.5 12.1.1.6 12.1.1.7 12.1.1.8 12.1.1.9 12.1.1.10 12.1.1.11 12.1.1.12 12.1.1.13		1.1, 1.1.1, 2.1, 2.1.1, 3.1, 3.1.1, 4.1, 4.1.1, 5.1, 5.1.1, 6.1, 6.1.1, 7.1, 7.1.1, 8.1, 8.1.1, 9.1, 9.1.1, 10.1, 10.1.1, 11.1, 11.1.1, 12.1, 12.1.1		
SG-06	Security Governance	Proprietary Rights Agreement	Organization regular employees consent to a proprietary rights agreement.		X					X		X		X						X						HR-06 IDM-08					40 60		5.32 6.2		A.10.1						7.1.2.3 18.1.2.3 7.1.2.4 7.1.2.5				
SG-07	Security Governance	Review of Confidentiality Agreements	The Organization Proprietary Rights Agreement and Organization Network Access Agreement are reviewed on a periodic basis.		X					X					X	X	X			X						HR-06					40 60					PS-06	PS-06	PS-06			18.1.2.11				
SG-08	Security Governance	Information Security Program	Organization has an established security leadership team including key stakeholders in the Organization Information Security Program; goals and milestones for deployment of the information security program are established and communicated to the company through the periodic security all-hands meeting.	X	X		X			X	X	X			X	X	X	X	X	X	X	X	X	X	ID.BE-2 ID.BE-3	BCM-01 COM-01 OIS-01 OIS-02 OIS-06 SP-01		8.1.6.1 8.1.7.1 8.1.7.2 8.1.9.2			1	4.2 5.1 5.1(a) 5.1(e) 5.1(f) 5.1(g) 5.1(h) 5.2(d) 5.2(f) 6.2(a) 6.2(d) 6.2(e) 6.2(f) 6.2(i) 6.2(j) 7.4 7.5.1(a) 9.3 6.3	5.4			CA-06 PL-02	CA-06 PL-02	CA-06 PL-02	164.308(a)(2)	ISM-0714 ISM-1478 ISM-1617 ISM-0725 ISM-0718 ISM-0733 ISM-1618 ISM-0734 ISM-0720	3.1.2.1 3.1.2.3 3.1.3.4 3.1.5.4 3.1.5.5 4.4.1.1 4.4.1.3 4.4.3.1 4.5.2.1 4.5.2.7 4.5.3.1 4.5.4.2 4.6.1.2 4.6.3.1 5.1.1.1 6.1.4.7 6.1.5.1 12.1.2.13 12.1.2.14 12.2.1.12 14.1.1.3 14.1.1.4 18.2.2.8	3.1	12.1.4	1.2.1	CC1.3
SG-09	Security Governance	Accessibility Program	Organization has an established accessibility leadership team including key stakeholders; goals and milestones for deployment of the accessibility program are established and communicated to the company.												X	X	X																			CA-06	CA-06	CA-06							
SG-10	Security Governance	Information Security Management System Scope	Information Security Management System (ISMS) boundaries are formally defined in an ISMS scoping document.				X			X	X				X	X	X			X								8.1.6.2			1 4 5 6 7 47 48 49 60	4.2 4.3 4.4 5.2 6.2 7.4 7.5.1 8.1 9.1 9.3				PL-02	PL-02	PL-02			4.4.4.1 4.4.5.2				
SG-11	Security Governance	Security Roles and Responsibilities	Roles and responsibilities for the governance of Information Security within Organization are formally documented within the Information Security Management Standard and communicated on the Organization intranet.	X	X	X	X			X	X	X			X	X	X	X	X	X	X	X	X	X	ID.AM-6 ID.BE-2 ID.BE-3 ID.GV-2 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5 DE.DP-1	BCM-01 COM-01 OIS-01 OIS-02 OIS-06	17.5	8.1.5.3 8.1.6.2 8.1.6.3 8.1.7.3 8.1.9.1 8.1.9.2 8.1.10.6			1 4 5 60 61 62	5.1(f) 5.1(g) 5.1(h) 5.3 6.2(h) 7.2	6.5			CA-06 PL-04	CA-06 PL-04 PS-09	CA-06 PL-04	164.308(a)(2) 164.308(a)(3)(i)	ISM-1071 ISM-1634 ISM-1635	3.1.5.3 4.4.1.2 4.4.3.1 4.5.2.7 6.1.1.1 6.1.1.4 6.1.1.6 6.1.1.7 6.1.1.8 6.1.1.9 6.1.1.10 6.1.1.11 6.1.5.6	3.1 4.1	12.1.3	1.2.2 2.1.1	CC1.3
SG-12	Security Governance	Security Roles and Responsibilities: Risk Designations	Organization defined security roles and responsibilities are assigned risk designations and reviewed at least once every three years.			X	X								X	X	X		X			X					17.5	8.1.6.3								PS-02	PS-02	PS-02		ISM-1525 ISM-1633 ISM-1634 ISM-1635			12.1.3		
SG-13	Security Governance	Security Roles and Responsibilities: PCI Compliance	Roles and responsibilities and a program charter for the governance of PCI DSS compliance within Organization are formally documented and communicated by management.																			X																					12.4.1, A3.1.1, A3.1.2, A3.2, A3.2.1, A3.2.2, A3.3		
SG-14	Security Governance	Information Security Resources	Information systems security implementation and management are included as part of the budget required to support the Organization Security Program.				X				X					X	X		X	X								8.1.9.6				5.1(c) 7.1					SA-02	SA-02		ISM-0732 ISM-0120	3.1.6.2 4.5.1.1 4.5.1.2 4.5.5.3				
SG-15	Security Governance	Management Review	The Information Security Management System (ISMS) steering committee conducts a formal management review of ISMS scope, risk assessment activities, control implementation, and audit results on an annual basis.		X		X	X			X				X	X	X		X	X						COM-04		8.1.6.2 8.1.6.4 8.1.10.6	9.3.1 9.3.2(a) 9.3.2(b) 9.3.2(c.1) 9.3.2(c.2) 9.3.2(c.3) 9.3.2(d) 9.3.2€ 9.3.2(f) 9.3.2(g) 9.3.2(h) 9.3.2(i)			9.3				CA-06	CA-06	CA-06		ISM-1636 ISM-0027 ISM-1587	4.6.3.2 4.6.3.3 4.6.3.4 4.7.1.7				
SG-16	Security Governance	Enterprise Data Catalog	Organization maintains an enterprise data catalog that encompasses key organizational data, environment metadata, and product information to facilitate continuous monitoring of the internal control environment. The enterprise data catalog is updated as part of the continuous monitoring process and upon the introduction of new service offerings and acquisitions.			X													X								3.2													ISM-1572					
SG-17	Security Governance	Software Usage Restrictions	Organization maintains software license contracts and monitors its compliance with usage restrictions.			X	X		X						X	X	X			X		X					2.1 2.2 2.3 2.4 2.5 2.6	8.1.4.4		Security Update Management						CM-10	CM-10	CM-10 AU-09 (04)			9.4.4.2 9.4.4.10.P 12.2.1.7 18.1.2.1 18.1.2.5 18.1.2.6 18.1.2.7 18.1.2.8 18.1.2.9 18.1.2.10 12.2.1.2 18.1.2.2 12.6.2.3		12.2, 12.2.1		
SLC-01	Service Lifecycle	Service Lifecycle Workflow	Major software releases are subject to the Service Life Cycle, which requires acceptance via Concept Accept and Project Plan Commit phases prior to implementation.	X	X	X				X		X			X	X	X		X	X	X	X		X	PR.IP-2	DEV-01	16.1 16.2 16.10				8 9 10 11 12 87		8.25 8.27 5.8 8.28			SA-03 SA-04	SA-03 SA-04 SA-08 PL-08	SA-03 SA-04 SA-04 (01) PL-08		ISM-1739 ISM-0041 ISM-1460 ISM-1604 ISM-0401 ISM-1780 ISM-1239 ISM-1241 ISM-1424 ISM-1278	6.1.5.2 6.1.5.3 6.1.5.4 6.1.5.5 12.5.1.14 14.1.1.7 14.1.1.12 14.1.1.14 14.1.1.15 14.1.1.16 14.1.1.17 14.1.1.18 14.2.1.2 14.2.1.4 14.2.1.7 14.2.5.1 14.2.5.2 14.2.5.3 14.2.5.4 14.2.5.5 14.2.5.6 14.2.5.8 14.2.6.8 14.2.8.2	5.1 5.2 5.4 5.7	6.1, 6.2, 6.2.1, 6.2.2, 6.2.3, 6.2.3.1		CC8.1
SLC-02	Service Lifecycle	Source Code Management	Source code is managed with Organization-approved version control mechanisms.		X	X	X			X										X	X	X		X		DEV-08	2.7 4.6 12.3	8.1.6.3 8.1.9.4 8.1.9.5 ©			87										9.4.5.2 9.4.5.3 9.4.5.4 9.4.5.5 9.4.5.6 9.4.5.7 9.4.5.8 9.4.5.9 12.5.1.2 14.2.1.5 14.2.1.6 14.2.2.14	5.7 6.3 7.6	6.1, 6.2, 6.2.1, 6.2.2, 6.2.3, 6.2.3.1		CC6.8 CC8.1
SLC-03	Service Lifecycle	Secrets in Code	Organization manages source code secrets in a centralized repository; secrets are rotated at least annually and immediately if the security of secrets is compromised.				X												X			X						8.1.5.4												ISM-1559			8.6, 8.6.1, 8.6.2, 8.6.3		
SLC-04	Service Lifecycle	Project Budget Approval	Approval for project initiation and budget is obtained from IT management and business owners.																																										
SLC-05	Service Lifecycle	Project Scope Change	Changes to finalized project scope and requirements require the review and approval from the business team and project manager.				X																					8.1.9.6																	
SLC-06	Service Lifecycle	Information System Operation Authorization	Senior management authorizes the operation of new information systems, based on security and business requirements, prior to implementation. The information system authorization is refreshed every 3 years or when significant change occurs.														X		X	X																		MA-06		ISM-1739 ISM-0041	14.2.5.9				
SLC-07	Service Lifecycle	System Acquisition Approval	Information system acquisitions require approval from authorized personnel based on verification of the following documented evidence: • security function, strength, and assurance requirements • requirements for protecting security-related documentation • system development and test requirements • acceptance criteria for releases • enumeration of Security controls • security control implementation and monitoring requirements • components are FIPS-201 approved			X	X								X	X	X										16.11	8.1.9.6 8.1.9.7								SA-04 SA-22	SA-04 SA-04 (10)	SA-04 SA-04 (02)							

SM-01	Systems Monitoring	Audit Logging	Organization logs critical information system activity.	X	X	X	X			X		X			X	X	X	X	X	X	X	X	X	X	DE.AE-3	AM-01 DEV-07 IDM-06 OIS-04 OPS-10 OPS-11 OPS-12 OPS-15 OPS-17 PSS-04	1.4 3.14 8.1 8.2 8.5 8.12 13.6	8.1.5.2 8.2.3.3			33 34 35 46		8.15 5.33			AU-02 AU-12	AU-02 AU-12	AU-02 AU-12 AU-07 (01)	164.312(b) 164.312(c)(2)	ISM-1714 ISM-1613 ISM-1660 ISM-1664 ISM-0582 ISM-1677 ISM-1607 ISM-0580 ISM-1405 ISM-1537 ISM-0634 ISM-0261 ISM-1778 ISM-1586	9.4.4.6 12.4.1.1 12.4.1.2 12.4.1.3 12.4.1.4 12.4.1.5 12.4.1.6 12.4.1.7 12.4.1.8 12.4.1.9 12.4.1.10 12.4.1.11 12.4.1.12 12.4.1.13 12.4.1.14 12.4.1.17 12.4.1.18 12.4.3.1 12.4.3.2 12.4.3.3 12.5.1.9 12.7.1.7 14.1.1.9	9.2 12.2	10.2, 10.2.1, 10.2.1.1, 10.2.1.2, 10.2.1.3, 10.2.1.4, 10.2.1.5, 10.2.1.6, 10.2.1.7, 10.2.2, A1.2, A1.2.1	1.4.1	CC7.1
SM-02	Systems Monitoring	Secure Audit Logging	Organization logs critical information system activity to a secure repository. Organization disables administrators ability to delete or modify enterprise audit logs; the number of administrators with access to audit logs is limited.		X	X											X		X			X				OPS-16	8.2 8.5 8.6 8.7 8.8 8.9 8.12 12.5											AU-06 (03) AU-07		ISM-1573 ISM-1714 ISM-1715 ISM-1663 ISM-1665 ISM-1747 ISM-1678 ISM-1683 ISM-1684 ISM-1705 ISM-1706 ISM-1707 ISM-1708 ISM-0859 ISM-0991 ISM-1536 ISM-1757 ISM-1758 ISM-1775 ISM-1776 ISM-1777			10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4		
SM-03	Systems Monitoring	Audit Logging: Cardholder Data Environment Activity	Organization logs the following activity for cardholder data environments: • individual user access to cardholder data • administrative actions • access to logging servers • failed logins • modifications to authentication mechanisms and user privileges • initialization, stopping, or pausing of the audit logs • creation and deletion of system-level objects • security events • logs of all system components that store, process, transmit, or could impact the security of cardholder data (CHD) and/or sensitive authentication data (SAD) • logs of all critical system components • logs of all servers and system components that perform security functions (e.g., firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)																X			X																		ISM-1034			10.2, 10.2.1, 10.2.1.1, 10.2.1.2, 10.2.1.3, 10.2.1.4, 10.2.1.5, 10.2.1.6, 10.2.1.7, 10.2.2		
SM-04	Systems Monitoring	Audit Logging: Cardholder Data Environment Event Information	Organization records the following information for confirmed events in the cardholder data environment: • user identification • type of event • date and time • event success or failure indication • origination of the event • identification of affected data, system component, or resource			X																X					8.1																10.2.2		
SM-05	Systems Monitoring	Audit Logging: Service Provider Logging Requirements	Organization establishes unique logging and audit trails for each entity's cardholder data environment and complies with the following: • logs are enabled for third-party applications • logs are active by default • logs are available for review by and communicated to the owning entity																			X																					10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4		
SM-06	Systems Monitoring	Configuration Management: Remote Logging	Where applicable, devices are configured to send audit log data to a remote server				X															X						8.1.10.6 8.2.3.3															5.3.4		
SM-07	Systems Monitoring	Chain of Accountability	Organization implements audit trails to link authentication events to individuals users in production systems.				X															X						8.1.3.5 8.1.4.3															10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4		
SM-08	Systems Monitoring	Audit Record Time Stamps	Organization records time stamps for audit records that can be mapped to a centralized time source.				X								X	X	X		X			X						8.1.3.5 8.1.4.3									AU-08	AU-08	AU-08		ISM-0585 ISM-0988			10.2.2		
SM-09	Systems Monitoring	Log Reconciliation: CMDB	Organization reconciles the established device inventory against the enterprise log repository on a quarterly basis; devices which do not forward log data are remediated.			X																X					8.9																10.4, 10.4.1, 10.4.1.1, 10.4.2, 10.4.2.1, 10.4.3		
SM-10	Systems Monitoring	Audit Log Capacity and Retention	Organization allocates audit record storage capacity in accordance with logging storage and retention requirements; Audit logs are retained for 1 year with 90 days of data immediately available for analysis.		X	X	X			X					X	X	X			X		X	X			OPS-14	8.1 8.3 8.9 8.10	8.1.5.2			46					AU-04 AU-11 CA-07	AU-04 AU-11 CA-07	AU-04 AU-11 CA-07 AU-06 (03)			12.4.2.3		10.5, 10.5.1,	1.4.1	
SM-11	Systems Monitoring	Enterprise Antivirus Logging	If applicable, Organization's managed enterprise antivirus deployments generate audit logs which are retained for 1 year with 90 days of data immediately available for analysis.			X				X									X			X					8.10				46									ISM-1672			10.5, 10.5.1		
SM-12	Systems Monitoring	Security Monitoring Alert Criteria	Organization defines security monitoring alert criteria, how alert criteria will be flagged, and identifies authorized personnel for flagged system alerts.	X	X	X	X	X		X					X	X	X	X		X	X			X	DE.AE-5 DE.CM-2	COS-01 IDM-06 OPS-10 OPS-13 PSS-04	13.1 13.11	8.1.5.4 8.1.9.2	9.1(a)		15 33 34 35 46					AU-02 AU-03 AU-06 AU-12	AU-02 AU-03 AU-06 AU-12	AU-02 AU-03 AU-06 AU-12 AC-02 (12) AU-06 (01) CA-07 (01) SI-04 (02) SI-04 (05)	164.308(a)(1)(ii)(D) 164.308(a)(6)(ii) 164.312(b) 164.312(c)(2)		4.6.2.1 6.1.2.4 9.4.2.10 9.4.2.11 9.4.2.12 12.4.2.1 12.4.2.2 12.7.1.9	6.4 7.7 12.2	10.4, 10.4.1, 10.4.1.1, 10.4.2, 10.4.2.1, 10.4.3		CC7.1 CC7.3
SM-13	Systems Monitoring	Security Monitoring Alert Criteria Review	Organization reviews security monitoring alert on an annual basis.			X																X					8.1																10.4, 10.4.1, 10.4.1.1, 10.4.2, 10.4.2.1, 10.4.3		
SM-14	Systems Monitoring	Log-tampering Detection	Organization monitors and flags tampering to the audit logging and monitoring tools in the production environment.			X	X			X							X			X		X	X				13.1	8.1.3.5 8.1.4.3			37							CA-07 (01)			12.5.1.18 14.1.3.5		10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4	1.4.1 8.1.3	
SM-15	Systems Monitoring	Unauthorized Devices Addition	Unauthorized devices connected to the Organization Network are: • detected within a maximum of five minutes, and • the unauthorized device is disabled, or a notification is sent to authorized Organization personnel			X											X		X			X					12.5 13.6											CM-08 (03)		ISM-0520			11.5, 11.5.1, 11.5.1.1, 11.5.2		
SM-16	Systems Monitoring	Security Monitoring Alert Criteria: Guest, Anonymous and Temp Accounts	Organization defines security monitoring alert criteria for the use of guest, anonymous, and temporary accounts on Organization's network.														X					X																AC-02 (12)					10.7, 10.7.1, 10.7.2, 10.7.3, A3.3.1, A3.3.1.2 11.5, 11.5.1, 11.5.1.1, 11.5.2		
SM-17	Systems Monitoring	Security Monitoring Alert Criteria: VoIP Usage	Organization defines security monitoring alert criteria to detect deviations from Voice over IP (VoIP) activity standards.																			X																					11.5, 11.5.1, 11.5.1.1, 11.5.2		
SM-18	Systems Monitoring	Prohibited Activity Monitoring: Remote Access	Remote sessions are monitored for prohibited activity.				X								X	X	X			X		X						8.1.3.5								AC-17	AC-17	AC-17			6.2.2.5 6.2.2.8 6.2.2.20		11.5, 11.5.1, 11.5.1.1, 11.5.2		
SM-19	Systems Monitoring	Prohibited Activity Monitoring: Client Run Time Technologies	Organization monitors and flags the use of prohibited client run time technologies on information systems.																			X																					11.5, 11.5.1, 11.5.1.1, 11.5.2		
SM-20	Systems Monitoring	Security Monitoring Alert Criteria: Wireless Access Point	Organization defines security monitoring alert criteria for attack attempts against wireless access points.				X															X						8.1.10.7 8.2.4.3															11.2, 11.2.1, 11.2.2		
SM-21	Systems Monitoring	Security Monitoring Alert Criteria: Failed Logins	Organization defines security monitoring alert criteria for failed login attempts on Organization's network.															X	X			X																	164.308(a)(5)(ii)©	ISM-1683 ISM-1684 ISM-1275			11.5, 11.5.1, 11.5.1.1, 11.5.2		
SM-22	Systems Monitoring	Security Monitoring Alert Criteria: Privileged Functions	Organization defines security monitoring alert criteria for privileged functions executed by both authorized and unauthorized users.				X										X		X			X						8.1.5.1 8.1.5.2 8.2.4.3										AC-06 (09) AC-06 (10)		ISM-1576 ISM-1275			10.2, 10.2.1, 10.2.1.1, 10.2.1.2, 10.2.1.3, 10.2.1.4, 10.2.1.5, 10.2.1.6, 10.2.1.7, 10.2.2		
SM-23	Systems Monitoring	Security Monitoring Alert Criteria: Audit Log Integrity	Organization defines security monitoring alert criteria for changes to the integrity of audit logs.																			X																					10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4		
SM-24	Systems Monitoring	Security Monitoring Alert Criteria: Cardholder System Components	Organization defines security monitoring alert criteria for system components that store, process, transmit, or could impact the security of cardholder data and/or sensitive authentication data.																			X																					10.4 10.4.1, 10.4.1.1, 10.4.2, 10.4.2.1		
SM-25	Systems Monitoring	System Security Monitoring	Critical systems are monitored in accordance with predefined security criteria and alerts are sent to authorized personnel. Confirmed incidents are tracked to resolution.	X	X		X	X		X		X			X	X	X	X		X	X			X	RS.AN-1 DE.AE-2 DE.CM-7 RS.AN-1	COS-01 COS-03 OIS-03 OPS-10 OPS-13 SIM-05 SSO-04 PSS-04		8.1.3.5 8.1.9.2 8.2.3.2	9.1(b)		33 34 35 46		8.16			AU-02 AU-05 AU-09 SI-04 SI-05	AU-02 AU-05 AU-09 SI-04 SI-05	AU-02 AU-05 AU-09 SI-04 SI-05 IR-06 (01)	164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)© 164.308(a)(6)(ii) 164.312(b) 164.312(c)(1) 164.312(c)(2)		6.1.3.5 9.4.2.10 9.4.2.11 9.4.2.12 12.4.5.5.P	7.7	12.10.1		CC6.8 CC7.2 CC7.3
SM-26	Systems Monitoring	Intrusion Detection Systems	Organization has an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) deployment(s) and ensures the following: • signature definitions are updated including the removal of false positive signatures • non-signature based attacks are defined • IDS/IPS are configured to capture malicious (both signature and non-signature based) traffic • alerts are reviewed and resolved by authorized personnel when malicious traffic is detected			X	X		X	X					X	X	X		X			X	X				8.11 13.3 13.8	8.1.3.3 8.1.3.4 8.1.4.4 8.1.4.5 8.2.2.1 8.2.3.2 8.2.4.3		Malware Protection	46					SI-04	SI-04	SI-04 SI-04 (01)		ISM-1213 ISM-1341 ISM-1034 ISM-1028 ISM-1030			11.5, 11.5.1, 11.5.1.1, 11.5.2	6.1.1 8.3.1 8.3.3	
SM-27	Systems Monitoring	System Monitoring Legal Opinion	Organization obtains legal opinion with regard to monitoring activities in accordance with applicable requirements and mandates.							X									X												46									ISM-0137 ISM-0979					
SM-28	Systems Monitoring	Privileged Session Monitoring	Organization monitors trusted data environments for unauthorized logical access connections.							X									X	X		X									46									ISM-1006	12.4.5.2.P		11.5, 11.5.1, 11.5.1.1, 11.5.2		
SM-29	Systems Monitoring	Availability Monitoring Alert Criteria	Organization defines availability monitoring alert criteria, how alert criteria will be flagged, and identifies authorized personnel for flagged system alerts.	X	X		X			X					X	X	X		X	X	X	X		X	DE.AE-5 PR.DS-4	OPS-01 OPS-02 OPS-09 PS-02		8.1.2.1			12 46 58 63 79 104 105 106					SI-05	SI-05	SI-05		ISM-1580 ISM-1441 ISM-1581 ISM-1290	12.1.3.9.PB	8.1	10.4 10.4.1, 10.4.1.1, 10.4.2, 10.4.2.1		CC3.1 CC7.2 A1.1
SM-30	Systems Monitoring	Availability Monitoring Alert Criteria Review	Organization reviews availability monitoring alert criteria on an annual basis.																X			X																		ISM-1580 ISM-1441 ISM-1581 ISM-1290			10.4 10.4.1, 10.4.1.1, 10.4.2, 10.4.2.1		
SM-31	Systems Monitoring	System Availability Monitoring	Critical systems are monitored in accordance with predefined availability criteria and alerts are sent to authorized personnel.	X	X			X		X		X			X	X	X		X	X	X	X		X	DE.CM-1 DE.DP-2	OPS-01 OPS-02 OPS-09 OPS-17 PS-06 SSO-04			9.1© 9.1(d) 9.1		12 46 58 63 79 104 105 106		8.6			SI-05	SI-05	SI-05 CP-02 (08)		ISM-1580 ISM-1441 ISM-1581 ISM-1290	12.1.3.1 12.1.3.2 12.1.3.3 12.1.3.4 12.1.3.5 12.1.3.6 12.1.3.7 14.1.1.8 17.2.1.1 17.2.1.2	8.1	10.4 10.4.1, 10.4.1.1, 10.4.2, 10.4.2.1		CC3.1 CC7.2 A1.1 A1.2
SM-32	Systems Monitoring	Remote Access: Activity Log Audit	Logs from remote sessions are audited for prohibited activity on a weekly basis.			X	X			X									X			X					8.11	8.1.3.5			46									ISM-1661 ISM-1662			10.4 10.4.1, 10.4.1.1, 10.4.2, 10.4.2.1		
SO-01	Site Operations	Secured Facility	Physical access to restricted areas of the facility is protected by walls with non-partitioned ceilings, secured entry points, and/or manned reception desks.	X	X		X			X		X			X	X	X	X	X	X	X	X	X	X	PR.AC-2 PR.IP-5	PS-01 PS-03 PS-04 PS-05 PS-06		8.1.10.1			50 51 55 56 83		7.1 7.3 7.6			PE-01 PE-02 PE-03 PE-16	PE-01 PE-02 PE-03 PE-16	PE-01 PE-02 PE-03 PE-16 MP-04 SA-09 (05)	164.310(a)(1) 164.310(a)(2)(ii)	ISM-1053 ISM-1530 ISM-0813 ISM-1074 ISM-0161	11.1.1.1 11.1.1.2 11.1.1.3 11.1.1.4 11.1.1.5 11.1.1.6 11.1.1.7 11.1.3.1 11.1.3.2 11.1.3.3 11.1.3.4 11.2.1.1 11.2.1.3 11.2.1.4 11.2.6.6	8.5	9.2, 9.2.1	11.1.1	CC6.4
SO-02	Site Operations	Physical Protection and Positioning of Cabling	Organization power and telecommunication lines are protected from interference, interception, and damage.		X		X			X		X			X	X	X			X		X				PS-06		8.1.1.1 (a) 8.1.1.3 (b) 8.1.1.10 (a) 8.1.1.10 (b) 8.3.1.1			52		7.12			PE-15	PE-15	PE-15 CP-08 (01) PE-09			11.2.3.1 11.2.3.2 11.2.3.3		9.2, 9.2.1		
SO-03	Site Operations	Global Coordination of Critical Functions: Information Security Safeguards	Organization consistently applies information security safeguards in datacenters and campuses.		X												X		X			X				PS-01												MP-04		ISM-1645			9.3, 9.3.1		
SO-04	Site Operations	Provisioning Physical Access	Physical access provisioning to an Organization datacenter requires management approval and documented specification of: • account type (e.g., standard, visitor, or vendor) • access privileges granted • intended business purpose • visitor identification method, if applicable • temporary badge issued, if applicable • access start date • access duration		X		X			X		X			X	X	X	X	X	X	X	X	X	X		PS-04		8.1.8.4			50		5.15			MA-05 PE-02 PE-03	MA-05 PE-02 PE-03 CM-05	MA-05 PE-02 PE-03	164.308(a)(4)(ii)(B) 164.310(a)(1) 164.310(a)(2)(ii) 164.310(a)(2)(iii)	ISM-1705 ISM-1706 ISM-1707 ISM-1708	11.1.2.1 11.1.2.3 11.1.2.4 11.1.2.5 11.1.2.6 11.1.2.7 11.1.2.8 11.1.2.9 11.1.2.10 11.1.2.11 11.1.2.12 11.1.2.13 11.1.6.5 11.2.1.2	8.5	9.3, 9.3.1, 9.3.1.1, 9.3.2, 9.3.3, 9.3.4	11.1.1 11.1.3	CC6.4
SO-05	Site Operations	De-provisioning Physical Access	Physical access that is no longer required in the event of a termination or role change is revoked. If applicable, temporary badges are returned prior to exiting facility.		X					X					X	X	X	X		X	X	X		X		PS-04					50					PE-02	PE-02	PE-02	164.310(a)(1) 164.310(a)(2)(ii)		7.3.1.1 7.3.1.2 7.3.1.3 9.2.6.1 11.1.2.1	8.5	9.3, 9.3.1, 9.3.1.1, 9.3.2, 9.3.3, 9.3.4		CC6.4

SO-06	Site Operations	Periodic Review of Physical Access	Organization performs physical account and access reviews on a quarterly basis; corrective action is taken where applicable.		X					X					X	X	X	X	X	X	X	X		X		PS-04					'50					PE-02 PE-06 PS-05	PE-02 PE-06 PS-05	PE-02 PE-06 PS-05	164.310(a)(1) 164.310(a)(2)(ii) 164.310(a)(2)(iii)	ISM-1053 ISM-1530 ISM-0813 ISM-1074 ISM-0164	11.1.2.1 11.2.2.2	8.5	9.3, 9.3.1, 9.3.1.1, 9.3.2, 9.3.3, 9.3.4		CC6.4
SO-07	Site Operations	Physical Access Role Permission Authorization	Initial permission definitions, and changes to permissions, associated with physical access roles are approved by authorized personnel.							X		X			X	X	X		X	X		X									50		7.2			PE-03	PE-03	PE-03		ISM-1296 ISM-0164	11.1.5.5 11.1.5.6 11.1.6.1 11.1.6.2 11.1.6.3 11.1.6.4 11.1.6.6 11.1.6.7		9.3, 9.3.1, 9.3.1.1, 9.3.2, 9.3.3, 9.3.4		
SO-08	Site Operations	Monitoring Physical Access	Intrusion detection and video surveillance are installed at Organization datacenter locations; confirmed incidents are documented and tracked to resolution.		X		X			X		X					X	X		X	X	X		X		PS-03 PS-04		8.1.1.2 8.1.1.3 ©			50		7.4					CP-08 PE-06 (01)	164.310(a)(1) 164.310(a)(2)(ii)		11.1.5.4 11.2.1.1	8.5	9.2.1.1		CC6.4
SO-09	Site Operations	Surveillance Feed Retention	Surveillance feed data is retained for 90 days.																			X																					9.2.1.1		
SO-10	Site Operations	Visitor Access	Physical access for visitors is managed through monitoring, maintaining records, escorting, and reviewing access monthly. Visitor access records to the facilities are kept for at least a year.				X								X	X	X					X						8.1.10.1								PE-03 PE-08	PE-03 PE-08	PE-03 PE-08					9.3, 9.3.1, 9.3.1.1, 9.3.2, 9.3.3, 9.3.4		
SO-11	Site Operations	Physical Access Devices	Physical access devices (i.e., keys, combinations, access cards, etc.) are maintained through an inventory and restricted to authorized individuals. Appropriate devices are rotated when compromised or upon employee termination or transfer.				X								X	X	X					X	X					8.1.1.2								PE-03	PE-03	PE-03					9.2.2, 9.2.3, 9.2.4	11.1.3	
SO-12	Site Operations	Temperature and Humidity Control	Temperature and humidity levels of datacenter environments are monitored and maintained at appropriate levels.		X		X			X		X			X	X	X			X	X		X	X		PS-05 PS-06 PS-07		8.1.10.1 8.1.1.1 (a) 8.1.1.1 (b) 8.1.1.6 (a) 8.1.1.6 (b) 8.1.1.6 © 8.1.1.8			50 52 53 54 55 56		7.5			PE-06 PE-14	PE-06 PE-14	PE-06 PE-14			11.1.4.1 11.2.1.1 11.2.1.7 11.2.2.1	8.5		11.2.2	A1.2
SO-13	Site Operations	Fire Suppression Systems	Emergency responders are automatically contacted when fire detection systems are activated; the design and function of fire detection and suppression systems are maintained at appropriate intervals.		X		X			X		X			X	X	X			X	X		X	X		PS-05 PS-07		8.1.10.1 8.1.1.5 (a) 8.1.1.5 (b) 8.1.1.5 ©			50 55 56		7.5			PE-06 PE-13	PE-06 PE-13	PE-06 PE-13 PE-13 (02)			11.2.1.1 11.2.1.5 11.2.1.6 11.2.1.8	8.5		11.2.2	A1.2
SO-14	Site Operations	Power Failure Protection	Organization employs uninterruptible power supplies (UPS) and generators to support critical systems in the event of a power disruption or failure. The design and function of relevant equipment is certified at appropriate intervals.	X	X		X			X		X					X		X	X	X		X	X	ID.BE-4	PS-06 PS-07		8.1.10.1 8.1.1.1 (a) 8.1.1.9 (a) 8.1.1.9 (b) 8.1.1.9 ©			52 53 54		7.11					PE-11		ISM-1123	11.2.2.3 11.2.2.4 11.2.2.5 11.2.2.6 11.2.2.7	8.5		11.2.2	A1.2
SO-15	Site Operations	Emergency Shutoff	Organization employs emergency power shut-off capabilities. Access to shut off power is restricted to authorized individuals.				X										X											8.1.10.1										PE-10							
SO-16	Site Operations	Emergency Lighting	Organization employs emergency lighting in the event of a power disruption or failure. The design and function of relevant equipment is certified at appropriate intervals.				X									X	X											8.1.10.1 8.1.1.4 (a) 8.1.1.4 (b) 8.1.1.7 (a) 8.1.1.7 (b)									PE-12	PE-12							
TA-01	Training and Awareness	General Security Awareness Training	Organization personnel complete security awareness training, which includes annual updates about relevant policies and how to report security events to the authorized response team. Records of training completion are documented and retained for tracking purposes.	X	X	X	X	X		X	X	X			X	X	X	X	X	X	X	X		X	PR.AT-1	AM-05 DEV-04 HR-02 HR-03 HR-04 SIM-04 SP-01	14.1 14.2 14.3 14.4 14.5 14.6 14.7 14.8	8.1.8.3 8.1.9.8 8.1.10.7	5.1(d)		2 3 32 60 61 62	5.1(d) 7.2 7.3(b) 7.3©	6.2			AT-02 AT-04 IR-07	AT-02 AT-04 IR-07 AT-02 (02)	AT-02 AT-04 IR-07 AT-02 (02)	164.308(a)(5)(i) 164.308(a)(5)(ii)(A) 164.308(a)(5)(ii)(B)	ISM-0735 ISM-0252	4.5.2.3 4.5.2.4 4.5.2.5 4.5.2.6 4.5.2.7 6.2.1.20 6.2.2.6 7.1.2.1 7.1.2.10 7.2.1.1 7.2.1.2 7.2.1.3 7.2.1.4 7.2.1.5 7.2.1.6 7.2.2.1 7.2.2.2 7.2.2.3 7.2.2.5 7.2.2.6 7.2.2.7 7.2.2.8 7.2.2.9 7.2.2.10	3.6	12.6, 12.6.1, 12.6.2, 12.6.3, 12.6.3.1, 12.6.3.2, A3.1.4		CC2.2
TA-02	Training and Awareness	Code of Conduct Training	Organization full-time and temporary employees and interns complete a code of business conduct training.		X	X				X										X				X		AM-05 HR-02 HR-03 HR-04 HR-05	14.2 14.3 14.4 14.5 14.7 14.8				2 3 60 64 65 66 67										7.1.2.1 7.2.2.1 11.2.8.1				CC1.1
TA-03	Training and Awareness	Accessibility Training	Organization personnel complete accessibility awareness training, which includes annual updates about relevant policies and how to report accessibility events internally. Records of training completion are documented and retained for tracking purposes.				X												X									8.1.9.8												ISM-0817 ISM-0435					
TA-04	Training and Awareness	Phishing Awareness	Organization performs periodic phishing campaigns.			X																					9.5																		
TA-05	Training and Awareness	Developer Security Training	Organization's software engineers are required to complete training based on secure coding techniques on an annual basis.		X	X	X					X										X				DEV-04	14.9 16.9	8.1.9.4 8.3.4.2					8.25 8.28 6.3										6.2.4		
TA-06	Training and Awareness	Payment Card Processing Security Awareness Training	Organization personnel that interact with cardholder data systems receive awareness training to be aware of attempted tampering or replacement of devices. Training should include the following: • verify the identity of third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • do not install, replace, or return devices without verification • be aware of suspicious behavior around devices (e.g., attempts by unknown persons to unplug or open devices) • report suspicious behavior and indications of device tampering or substitution to authorized personnel (e.g., to a manager or security officer)			X						X										X					14.9						6.3										9.5.1.3		
TA-07	Training and Awareness	Role-based Security Training: HIPAA	Organization personnel with access to personal health information (PHI) are required to attend and complete HIPAA privacy training.			X						X						X									14.9						6.3						164.308(a)(5)(i) 164.308(a)(5)(ii)(A)						
TA-08	Training and Awareness	Role-based Security Training	Organization personnel with key security responsibilities complete relevant role-based training on an annual basis: • personnel must complete training prior to obtaining access to privileged security systems • personnel with contingency responsibilities must complete role-based training within 10 days of assuming the role • records of training completion are documented and retained for tracking purposes			X	X					X			X	X	X		X	X		X	X				14.9	8.1.8.3					6.3			AT-03 IR-02 CP-03	AT-03 IR-02 CP-03	AT-03 IR-02		ISM-1565 ISM-0408 ISM-0612	7.2.2.4 14.2.1.11 18.2.3.5		6.2.4	6.1.2	
TA-09	Training and Awareness	Security Champion Training	Service teams select a "Security Champion" to ensure security engagement responsibilities are assigned and tracked to completion; Security Champions receive training on how to execute responsibilities.			X						X															14.9						6.3												
TPM-01	Third-Party Management	Third-Party Assurance Review	On a periodic basis, management reviews controls within third-party assurance reports to ensure that they meet organizational requirements; if control gaps are identified in the assurance reports, management takes action to address impact the disclosed gaps have on the organization.	X	X	X	X	X		X		X			X	X	X	X	X	X	X	X	X	X	ID.SC-1 ID.SC-3 ID.SC-4	DEV-01 OIS-03 OIS-07 PS-01 PS-03 SSO-01 SSO-02 SSO-04 SSO-05	15.5 15.6	8.1.9.10 8.2.6.1 8.2.6.2	8.1© 8.6©		41 47 48 49		5.22			PS-07 SA-09	PS-07 SA-09 RA-03 (01) SR-10	PS-07 SA-09 SA-09 (01)	164.308(b)(2) 164.310(a)(1) 164.310(a)(2)(ii)	ISM-0731 ISM-1452 ISM-1569 ISM-0280 ISM-0285	4.6.2.5 6.1.1.12 14.1.1.13 14.2.1.12 14.2.6.6 14.2.7.2 14.2.7.3 14.2.7.4 14.2.7.5 14.2.7.6 14.2.7.7 14.2.7.8 14.2.7.9 14.2.7.10 14.2.7.11 15.1.1.2 15.1.1.14.B 15.1.2.17 15.1.3.10.P 15.1.3.11.P 15.2.1.1 15.2.1.2 15.2.1.3 15.2.1.4	3.4 6.4	12.8, 12.8.1, 12.8.2, 12.8.3, 12.8.4, 12.8.5	4.1.1 4.2.1	CC3.2 CC4.1 CC6.4 CC9.2
TPM-02	Third-Party Management	Vendor Risk Management	Organization performs a risk assessment to determine the data types that can be shared with a managed service provider.		X	X				X		X		X	X	X	X		X	X		X				SSO-02	15.3				1 2 3 8 9 10 40 41		5.19		A.5.2 A.7.1 A.10.12	PS-07 SA-09	PS-07 RA-03 (01) SR-10	PS-07 SA-09 (01)		ISM-1737 ISM-1638 ISM-1395 ISM-0072	15.1.1.16.B		12.8.3		
TPM-03	Third-Party Management	Forensic Investigations	Organization enables procedures to conduct a forensic investigation in the event that a hosted merchant or service provider is compromised.																			X	X																				12.8.3	4.2.1	
TPM-04	Third-Party Management	Privacy Risk Assessment	Organization reviews the privacy practices of service providers who access, collect, process, transfer, or store personal information on Organization's behalf upon initial procurement and renewal; non-compliance is tracked through remediation.				X												X	X								8.2.4.5												ISM-0280 ISM-0285	4.5.4.5				
TPM-05	Third-Party Management	Network Access Agreement: Vendors	Third-party entities which gain access to the Organization network sign a network access agreement.				X			X					X	X	X			X		X						8.1.8.4			40 60					PS-07	PS-07	PS-07			12.5.1.16 14.1.2.14 15.1.3.1 15.2.2.3 18.1.2.12		8.2.7		
TPM-06	Third-Party Management	Vendor Non-disclosure Agreements	Agency temporary workers, independent contractors, and third-party entities consent to a non-disclosure clause.	X	X	X	X			X		X		X	X	X	X			X		X	X	X	DE.CM-6	AM-05 HR-02 HR-05 HR-06 SP-01	15.4	8.1.8.4 8.2.6.1			1 2 3 8 9 10 40 41 87 88 89 90		6.6		A.10.1	PS-07	PS-07	PS-07			7.1.2.1 7.1.2.2 13.2.2.1 13.2.4.1 13.2.4.2 13.2.4.4 13.2.4.5 13.2.4.6 13.2.4.7 13.2.4.8 13.2.4.9 13.2.4.10 13.2.4.11 13.2.4.12 13.2.4.13 13.2.4.14 13.2.4.15 13.2.4.16 15.1.1.13 15.1.2.1 15.1.3.2 15.1.3.3 15.1.3.4 15.1.3.5		12.7, 12.7.1	2.2.1	CC9.2 C1.1
TPM-07	Third-Party Management	Cardholder Data Security Agreement	Organization managed service providers that manage, store, or transmit cardholder data on behalf of the customer must provide written acknowledgement to customers of their responsibility to protect cardholder data and the cardholder data environment.				X												X			X						8.1.10.14												ISM-1737 ISM-1638			12.9, 12.9.1, 12.9.2		
TPM-08	Third-Party Management	HIPAA Business Associate Agreement	Organization Business Associate Agreements must contain provisions for the following: • permitted uses and disclosures of Protected Health Information (PHI) • PHI safeguards to prevent unauthorized use or disclosure • communications regarding the unauthorized use or disclosure of PHI • PHI availability • contract termination and disposition of PHI															X																					164.308(b)(2) 164.308(b)(3) 164.314(a)(2)(i) 164.314(a)(2)(iii)						
TPM-09	Third-Party Management	HIPAA Business Associate Subcontractor Agreement	Organization requires a Business Associate Subcontractor Agreement with Business Associates from which it receives or transmits protected health information (PHI); Business Associates under contract are required to provide assurance that they adhere to Organization's security standards, which includes the security of PHI and reporting security events that potentially expose PHI.															X																					164.308(b)(2) 164.308(b)(3) 164.314(a)(2)(i) 164.314(a)(2)(iii)						

TPM-10	Third-Party Management	Network Service Level Agreements (SLA)	Vendors providing networking services to Organization are contractually bound to provide secure and available services as documented in SLAs.			X	X			X				X	X	X		X	X		X					15.4	8.1.9.10 8.1.10.14 8.2.6.1			4 24 25 71 72 73 74 75 76 77 94					PS-07	PS-07	PS-07		ISM-1575 ISM-1578	13.1.2.2 10.1.2.19 15.1.1.10 13.2.3.3 13.2.3.5		12.8.2, 12.8.5		
TPM-11	Third-Party Management	Personal Information Processing and Transfer Agreement	Appropriate data processing and transfer agreements are established for the collection, processing, transfer, or storage of personal information by, or on behalf of, Organization.			X	X					X	X		X			X	X							15.4	8.2.6.1					5.14		A.2.1 A.5.1 A.7.1 A.9.3 A.10.11		SR-08			ISM-0240 ISM-0866	13.2.2.2 13.2.2.3 13.2.2.4 13.2.2.5 13.2.2.6 13.2.2.7 13.2.2.8 13.2.2.9 13.2.2.10 13.2.2.11 13.2.2.12 13.2.2.13 15.1.2.2 15.1.2.4 13.2.1.8 13.2.1.13 13.2.1.14				
TPM-12	Third-Party Management	Approved Service Provider Listing	Organization maintains a list of approved managed service providers and the services they provide to Organization.		X	X	X											X			X	X			SSO-03	15.1	8.1.9.3 8.1.10.14 8.2.6.2												ISM-1736 ISM-1737 ISM-1637 ISM-1638			12.8.1	4.1.1 4.2.1	
TPM-13	Third-Party Management	Vendor Information Security Standard	Organization has documented a Vendor Information Security Standard that defines the responsibilities and governance requirements regarding vendor information security engagements. Contractual agreements are entered into with vendors who process or store Organization data that define information Security terms and service level agreements.	X	X	X	X				X	X			X		X	X	X	X	X	X	X	ID.BE-1 ID.SC-3 ID.SC-4	COM-01 HR-06 OIS-02 OIS-03 SIM-04 SSO-01 DEV-02	15.2 15.4	8.1.9.3 8.1.9.10 8.1.10.14				7.3	5.2 5.23 5.21				SR-01 SR-02 SR-02 (01) SR-03 SR-05		164.308(a)(1)(i)	ISM-1568 ISM-1632 ISM-1571 ISM-1738 ISM-1073 ISM-0280 ISM-0285 ISM-1578	13.1.2.1 13.2.4.3 14.2.7.1 6.1.1.13.PB 7.1.2.4 7.1.2.5 15.1.1.3 15.1.1.4 15.1.1.6 15.1.1.7 15.1.1.8 15.1.1.9 15.1.1.12 15.1.2.3 15.1.2.5 15.1.2.6 15.1.2.7 15.1.2.8 15.1.2.9 15.1.2.10 15.1.2.11 15.1.2.12 15.1.2.13 15.1.2.14	3.4	12.8	1.2.2 2.2.1 4.1.1	CC1.3 C1.1
VM-01	Vulnerability Management	Vulnerability Scans	Organization conducts vulnerability scans against the production environment; scan tools are updated prior to running scans.	X	X	X	X		X	X		X		X	X	X	X	X	X	X	X	X	X	DE.CM-8 PR.IP-12 ID.RA-1	COM-03 COS-03 OPS-18 OPS-20 OPS-22 PSS-02 PSS-09 PSS-03	7.5 7.6	8.1.7.5 8.1.10.5		Security Update Management	4 27 28 29 88 89 90		8.8			CA-07 RA-05 SI-02 RA-05 (02)	CA-07 RA-05 SI-02 RA-05 (02)	CA-07 RA-05 SI-02 RA-05 (02) RA-05 (03)	164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(8)	ISM-1163 ISM-1698 ISM-1699 ISM-1700 ISM-1701 ISM-1702 ISM-1752 ISM-1754	12.6.1.1 12.6.1.2 12.6.1.3 12.6.1.4 12.6.1.5 12.6.1.6 12.6.1.7 12.6.1.8 12.6.1.9 12.6.1.10 12.6.1.11 12.6.1.12 12.6.1.13 12.6.1.14 12.6.1.15 12.6.1.16 12.6.1.17 14.2.9.3 18.2.3.3 18.2.3.4	11.3 13.1	11.3, 11.3.1, 11.3.1.1, 11.3.1.2, 11.3.1.3, 11.3.2, 11.3.2.1	3.3.1 8.1.5	CC3.2 CC7.1
VM-02	Vulnerability Management	Vulnerability Scans: Cardholder Data Environment	Vulnerability scans are conducted against cardholder environments at least quarterly or after significant change; critical vulnerability resolution is confirmed via a rescan.															X			X																		ISM-1608 ISM-1588 ISM-1698 ISM-1699 ISM-1700 ISM-1701 ISM-1702 ISM-1752			11.3, 11.3.1, 11.3.1.1, 11.3.1.2, 11.3.1.3, 11.3.2, 11.3.2.1		
VM-03	Vulnerability Management	Vulnerability Scans: Audit Log Review	When vulnerabilities are identified, Organization analyzes audit logs to see if it has been previously exploited. Identified exploitations are resolved through incident management.			X	X											X			X					18.4	8.1.10.5												ISM-0298 ISM-1643 ISM-1690 ISM-1694 ISM-1695 ISM-1696 ISM-1697 ISM-1698 ISM-1699 ISM-1700 ISM-1701 ISM-1702 ISM-1752 ISM-0109 ISM-1228 ISM-1616 ISM-1755 ISM-1756			12.10		
VM-04	Vulnerability Management	Vulnerability Scans: Trend Analysis	Organization reviews vulnerability trends over time to include in risk assessments; high and moderate risk vulnerabilities are remediated in 30 and 90 days, respectively.			X	X							X	X	X		X			X					18.4	8.1.7.5								RA-05	RA-05	RA-05		ISM-0298 ISM-1643 ISM-1690 ISM-1694 ISM-1695 ISM-1696 ISM-1697			11.3, 11.3.1, 11.3.1.1, 11.3.1.2, 11.3.1.3, 11.3.2, 11.3.2.1		
VM-05	Vulnerability Management	Approved Scanning Vendor	At least quarterly, Organization engages an Approved Scanning Vendor to conduct external vulnerability scans.		X									X	X	X					X				COS-03 OPS-22										RA-05	RA-05	RA-05 CA-08 (01)					11.3., 11.3.2.1		
VM-06	Vulnerability Management	Application Penetration Testing	Organization conducts penetration tests periodically.		X	X				X				X	X	X	X		X	X	X		X		COM-03 OPS-18 OPS-19 OPS-20 PSS-02 OIS-05	16.13 18.1 18.2 18.5				4 27 28 29 88 89 90					CA-07 SI-03	CA-02 (01) CA-07 SI-03 CA-08	CA-02 (01) CA-07 SI-03 CA-08	164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(8)		14.2.9.4	13.2 13.3	11.4.1, 11.4.2, 11.4.3, 11.4.4, 11.4.5, 11.4.6, 11.4.7, A1.1.4, A3.2.4		CC4.1 CC7.1
VM-07	Vulnerability Management	Application Penetration Testing: Cardholder Data Environment	Organization conducts penetration tests against cardholder data environments (CDE) and includes the following requirements: • testing covers the entire CDE perimeter and critical data systems • testing verifies that CDE perimeter segmentation is operational • testing is performed from both inside and outside the CDE network • testing validates segmentation and scope-reduction controls (e.g., tokenization processes) • network layer penetration tests include components that support network functions as well as operating systems • at the application level, testing provides coverage, at a minimum, against the security testing requirements defined in VM-05-01 (01) • testing is performed with consideration of threats verified in the last 12 months from external alerts, directives, and advisories defined in VM-06-02 • testing is performed with consideration of vulnerabilities reported through Organization's PSIRT process within the last 12 months • risk ratings are assigned to discovered vulnerabilities, which are tracked through remediation													X					X																CA-08 (01)					6.4.1, A1.1.4		
VM-08	Vulnerability Management	Infrastructure Patch Management	Organization installs security-relevant patches, including software or firmware updates; identified end-of-life software must have a documented decommission plan in place.		X	X	X		X					X	X	X	X	X	X	X	X	X	X		OPS-22	7.3 7.4	8.1.4.4		Security Update Management						CA-07 SI-02	CA-07 SI-02	CA-07 SI-02 CM-08 (01)	164.312(c)(1)	ISM-1407 ISM-1744 ISM-1467 ISM-1483 ISM-1606 ISM-1143 ISM-0298 ISM-1643 ISM-1690 ISM-1691 ISM-1692 ISM-1693 ISM-1751 ISM-0300 ISM-1717	12.5.1.11 12.5.1.15	7.3 7.4 11.4	6.3.2, 6.3.3	8.1.4 8.1.5 8.3.1	CC7.1
VM-09	Vulnerability Management	Enterprise Antivirus	Organization has managed enterprise antivirus deployments to detect and respond to malicious activities.		X	X	X		X	X		X		X	X	X	X	X	X	X	X	X	X		OPS-04 OPS-05	9.7 10.1 10.2 10.3 10.4 10.6 10.7	8.1.10.7		Malware Protection	31		8.7			CA-07	CA-07	CA-07	164.308(a)(5)(ii)(B)	ISM-0917 ISM-1745 ISM-1417 ISM-1672 ISM-1288 ISM-0657	12.2.1.1 12.2.1.3 12.2.1.4 12.2.1.6 12.2.1.8 12.2.1.13	11.3	5.2, 5.2.1, 5.2.2, 5.2.3, 5.2.3.1	8.2.1	CC6.8
VM-10	Vulnerability Management	Enterprise Antivirus Tampering	Antivirus mechanisms cannot be disabled or altered by users unless specifically authorized by management.															X			X																		ISM-1672			5.3.5		
VM-11	Vulnerability Management	Enterprise Antivirus Scope	Vulnerability scans are periodically performed on systems that do not require anti-virus; management determines if anti-virus should be required on the system based on scan results and associated risk.						X												X								Malware Protection													5.2, 5.2.1, 5.2.2, 5.2.3, 5.2.3.1		
VM-12	Vulnerability Management	Maintenance Tools: Inspect Media	Organization checks media containing diagnostic and test programs for malicious code before the media are used in production systems.				X														X						8.1.10.7															6.2.3.1		
VM-13	Vulnerability Management	Code Security Check	Organization conducts periodic source code checks for vulnerabilities.			X				X		X		X	X	X		X	X		X					16.12				8 9 10 87		5.8 8.25 8.29			CA-07 SI-03	CA-07 SI-03	CA-07 SI-03		ISM-1460 ISM-1604	14.2.1.8 14.2.1.9		6.2.3.1		
VM-14	Vulnerability Management	Code Security Check: Cardholder Data Environment	Where applicable, security testing performed prior to releasing code into production includes the following: • code injection • buffer overflows • insecure cryptographic storage • insecure communications • improper error handling • high-risk vulnerabilities • cross-site scripting • improper access control • cross-site request forgery • broken authentication session management			X	X											X			X					16.12	8.1.9.7												ISM-1669 ISM-1542 ISM-0402 ISM-0971			6.2.4		
VM-15	Vulnerability Management	Third-Party Library Check	Organization scans third-party libraries for vulnerabilities according to the service risk rating assignment.			X															X					16.5																6.3.1		
VM-16	Vulnerability Management	Non-disclosure of Error Detail	Information systems are designed to ensure error messages generated provide adequate information for taking corrective action without revealing sensitive information.													X					X																SI-11					6.2.4		
VM-17	Vulnerability Management	Embedded Authenticators	Quality Engineering checks to ensure that static passwords are not embedded within application source code or access scripts, prior to deployment on the Organization network.															X			X																		ISM-1460 ISM-1604			6.2.3.1		
VM-18	Vulnerability Management	External Information Security Inquiries	Organization reviews information-security-related inquiries, complaints, and disputes.																		X																					6.3.1		
VM-19	Vulnerability Management	External Alerts and Advisories	Organization reviews alerts and advisories from management approved security forums and communicates verified threats to authorized personnel.		X					X		X			X			X			X				OIS-05					3 32 36 60		5.5 5.6				RA-05 (11)			ISM-0298 ISM-1643 ISM-1690 ISM-1691 ISM-1692 ISM-1693 ISM-1694 ISM-1695 ISM-1696 ISM-1697			6.3.1		
VM-20	Vulnerability Management	Third-Party Security Assessment	Organization engages qualified managed service providers to perform independent information security assessments.													X					X																CA-07 (01) SA-11 SA-11 (02)					6.3.1		
VM-21	Vulnerability Management	Security Testing Window	Security administrators notify relevant parties prior to executing technical security assessments; assessment details and results are documented in a ticket.													X																					SA-11							

VM-22	Vulnerability Management	Vulnerability Remediation	Organization assigns a risk rating to identified vulnerabilities and prioritizes remediation of legitimate vulnerabilities according to the assigned risk.			X				X					X	X	X			X		X	X				7.2 7.7 16.2 16.6 18.3				4 27 28 29 88 89 90					CA-07 RA-05	CA-07 RA-05	CA-07 RA-05			12.6.1.1		6.3.1	3.3.1	
VM-23	Vulnerability Management	Backlog Prioritization	Organization documents identified bugs, prioritize bug fixes according to risk, and tracks resolution as part of the product release cycle.			X	X															X					7.2 7.7 16.2	8.1.9.5															6.3.1		

CCF ID	Control Domain	Control Name	Control Description	Control Theme	Control Type	Policy/Standard	Control Implementation Guidance	Control Testing Procedure	Audit Artifacts
AM-01	Asset Management	Inventory Management	Organization maintains an inventory of information systems, which is reconciled on a periodic basis.	Process	Preventive	Asset Management Policy	1. Design and document a process for maintaining an inventory of information systems for management of assets within an organization. 2. Perform inventory reconciliation on a periodic basis. 3. Create and maintain periodic reconciliation documentation.	1. Inspect the policy and standard to determine whether requirements for maintaining and reconciling a system of inventory for information systems are defined. 2. Observe the inventory of system devices to determine whether the organization maintains the inventory in a system of record. 3. Inspect periodic reconciliation documentation to determine whether reconciliation was performed.	E-AM-01 E-AM-02 E-AM-03
AM-02	Asset Management	Inventory Management: Applications	Organization maintains an inventory of application assets, which is reconciled on a periodic basis.	Process	Preventive	Asset Management Policy	1. Design and document a process for maintaining an inventory of application assets for management of assets within an organization. 2. Perform inventory reconciliation on a periodic basis. 3. Create and maintain periodic reconciliation documentation.	1. Inspect the policy and standard to determine whether requirements for maintaining and reconciling a system of inventory for application assets are defined. 2. Observe the inventory of system devices to determine whether the organization maintains the inventory in a system of record. 3. Inspect periodic reconciliation documentation to determine whether reconciliation was performed.	E-AM-01 E-AM-02 E-AM-03
AM-03	Asset Management	Inventory Reconciliation: ARP Table	Organization reconciles network discovery scans against the established device inventory on a quarterly basis; non-inventoried devices are assigned an owner.	Process	Preventive	Asset Management Policy	1. Design and document a process for conducting network discovery scans on a periodic basis. 2. Ensure the results of the scans are reconciled with the system asset inventory at least quarterly. 3. Ensure necessary actions are taken to include non-inventoried assets in the inventory with appropriate ownership details.	1. Inspect network discovery scans result to ensure periodic scans were conducted. 2. Observe the reconciliation report of network discovery scans against the established device inventory to determine that the inventories are reconciled on a quarterly basis. 3. Inspect the device inventory to ensure non-inventoried devices have been added and have a designed owner.	E-AM-04 E-AM-03 E-AM-02
AM-04	Asset Management	Inventory Reconciliation: Logging	Organization reconciles the enterprise log repository against the established device inventory on a quarterly basis; non-inventoried devices are assigned an owner.	Process	Preventive	Asset Management Policy	1. Ensure logs from enterprise logging solutions are reconciled with the system device asset inventory on a quarterly basis. 2. Ensure necessary actions are taken to include non-inventoried assets in the inventory with appropriate ownership details	1. Inspect the reconciliation report of enterprise log repository against the established device inventory to determine that the inventories are reconciled on a quarterly basis. 2. Inspect the non-inventoried devices to determine that the assets have a designed owner.	E-AM-03 E-AM-02
AM-05	Asset Management	Inventory Labels	Organization assets are labeled and have designated owners.	Process	Preventive	Asset Management Policy	1. Ensure all assets in the system device asset inventory are assigned appropriate labels as per the organization's labelling procedures. 2. Ensure each asset has an assigned owner and accuracy is maintained.	1. Inspect documentation to determine whether requirements for asset labelling ownership assessment are defined. 2. Inspect the asset listings to determine whether the assets are labelled and have a designated owner. 3. For a sample of services, inspect the asset reports to determine asset are labelled and have a designated owner. 4. Observe and compare physical assets at an organization's data center to determine whether the assets were labelled according to in-scope asset listings.	E-AM-02 E-AM-01
AM-06	Asset Management	Media Marking	Where applicable, Organization marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information. Exemptions must be approved by management and remain in a specific controlled area.	Process	Preventive	Asset Management Policy	1. Ensure that a process is established and documented for media marking and handling, including distribution limitation. 2. Ensure that sensitive information containing media is marked as per the organization's media marking requirements as applicable. 3. Ensure that any exceptions are approved by management, documented and retained by authorized personnel.	1. Inspect information system media marking to indicate the distribution limitations, handling caveats, and applicable security markings (if any) of the information. 2. Inspect exemption cases to validate that it must be approved by management and remain in a specific area.	E-AM-01 E-AM-05

AM-07	Asset Management	Asset Transportation Authorization	Organization authorizes and records the entry and exit of systems at datacenter locations.	Process	Preventive	Asset Management Policy	1. Ensure a process is established and documented to control the transport of assets in and out of data center locations. 2. Ensure appropriate records and approvals are obtained and maintained against entry and exit of each asset.	1. Inspect the policy and/or standard to determine whether requirements have been established to authorize and record the entry and exit of systems at datacenter locations. 2. Inspect evidence of asset movement from a sample of data centers and colocations.	E-AM-01 E-AM-06
AM-08	Asset Management	Asset Transportation Documentation	Organization documents the transportation of physical media outside of datacenters. Physical media is packaged securely and transported in a secure, traceable manner.	Process	Preventive	Asset Management Policy	1. Ensure appropriate records and approvals are obtained and documented against entry and exit of each asset. 2. Ensure all assets being transported are secured as per the organization's policy and can be tracked when offsite.	1. Inspect the policy and/or standard to determine whether the transportation of physical media outside of datacenters are defined. 2. Inspect the logs of physical media evidence that have been transported to determine that physical media is packed securely and transported in a secure, traceable manner.	E-AM-01 E-AM-06
AM-09	Asset Management	Use of Portable Media	The use of portable media in Organization datacenters is prohibited unless explicitly authorized by management.	Process	Preventive	Asset Management Policy	1. Ensure policy and procedures are established and communicated prohibiting the use of portable media. 2. Ensure necessary controls are in place to detect the usage of portable media inside the organization's network. 3. Ensure any exceptions are documented based on business justification and need and are approved appropriately.	1. Inspect the policy and/or standard to determine that the use of portable media in the datacenters is prohibited unless explicitly authorized by management. 2. Inspect Configurations to detect the use of portable media.	E-AM-01 E-AM-07
AM-10	Asset Management	Maintenance of Assets	Equipment maintenance is documented and approved according to management requirements.	Process	Preventive	Asset Management Policy	1. Ensure a process is established and documented for maintenance of assets. 2. Ensure all maintenance is approved by the management and is carried out through approved vendors. 3. Ensure proper testing of equipment is conducted post maintenance before use.	1. Inspect the policy and/or standard to determine whether management requirements have been established for the documentation and approval of equipment maintenance. 2. Inspect equipment maintenance requests to determine whether equipment maintenance is documented and approved according to management requirements.	E-AM-01 E-AM-08
AM-11	Asset Management	Tampering of Payment Card Capture Devices	Devices that physically capture payment card data are inspected for evidence of tampering on a semi-annual basis.	Process	Detective	Asset Management Policy	1. Ensure all payment card devices are inspected on semiannual basis to check for tampering. 2. Ensure that appropriate documentation is maintained regarding maintenance activities of these devices	1. Inspect devices verification records for tampering check. 2. Inspect and validate whether these verification were done at least semi-annually.	E-AM-09
AM-12	Asset Management	Component Installation: Inspection and Approval	Prior to installation in a production network, hardware components are inspected for improper or unauthorized modifications.	Process	Preventive	Asset Management Policy	1. Ensure a process is established and documented for approval of hardware prior to installation on production. 2. Ensure each asset is inspected with agreed on procedures before being enabled on production.	1. Validate if a process exists for the approval and verification of hardware prior to production installation. 2. Inspect hardware components installation records in a production network to determine that modifications were validated before installation.	E-AM-01 E-AM-10
AM-13	Asset Management	Software bill of Material	Organization maintains a comprehensive software bill of materials	Process	Preventive	Asset Management Policy	1. Ensure a Software bill of material is established. 2. Ensure that a process has been established and documented for the addition, removal, and update of components from SBOM.	1. Inspect and validate that a Software bill of material is established. 2. Validate that a process has been established and documented for addition, removal, and update of components from SBOM.	E-AM-01 E-AM-11

BC-01	Business Continuity	Business Continuity Plan	Organization's business contingency plan is periodically reviewed, approved by management and communicated to relevant team members.	Process	Preventive	Business Continuity Policy	1. Design and document a process for Business Continuity and Disaster Recovery. 2. Define steps for recovery with all roles and responsibilities in the Business Continuity Plan. 3. Ensure that the Business Continuity Plan is approved by the process owners, and is communicated to all the relevant team members.	1. Inspect and validate whether the Business Continuity and Disaster Recovery Processes are designed and documented. 2. Inspect Organization's Business Continuity Plan ("BCP") to determine whether Organization has established recovery steps and phases, recovery capabilities, and identified personnel responsible to execute recovery procedures. 3. Inspect the most recent version of Organization's BCP to determine whether it is periodically reviewed and approved. 4. Inspect the corporate intranet to determine whether Organization's BCP is communicated to relevant team members.	E-BC-01 E-BC-02
BC-02	Business Continuity	Business Continuity Plan: Personal Health Information	Organization's Business Contingency Plan addresses how to access facilities and obtain data during an emergency.	Process	Corrective	Business Continuity Policy	1. Ensure that steps to be followed in case of an emergency are clearly mentioned in the Business Continuity Plan so that access to the facilities and data is facilitated during an emergency.	1. Inspect an organization's Business Contingency Plan to determine whether Organization has addresses how to access facilities and obtain data during an emergency.	E-BC-02
BC-03	Business Continuity	Business Continuity Plan: Roles and Responsibilities	Business contingency roles and responsibilities are assigned to individuals and their contact information is communicated to authorized personnel.	Process	Corrective	Business Continuity Policy	1. Check that roles and responsibilities are clearly defined in the Business Continuity Plan. There should be proper demarcation of responsibilities during each phase of the crisis. 2. Ensure that the contact information for all the stakeholders is defined within Business Continuity Plan and should be up to date, documented, and communicated to all authorized personnel. 3. Ensure that people with roles and responsibilities within Business Continuity Plans are well aware of their responsibilities.	1. Inspect documentation consisting of business contingency roles and responsibilities. . 2. Inspect whether the contact information of personnel with business continuity responsibilities are documented within the Business Continuity Plan. 3. Inspect evidence to check whether roles and responsibilities are communicated to all applicable stakeholders and audience	E-BC-02
BC-04	Business Continuity	Continuity Testing	Organization performs business contingency and disaster recovery tests on a periodic basis and ensures the following: • tests are executed with relevant contingency teams • test results are documented • corrective actions are taken for exceptions noted • plans are updated based on results	Process	Detective	Business Continuity Policy	1. Ensure that Business Continuity testing should be performed on a periodic basis as per the organization policy. 2. The business continuity testing should emulate the Business Continuity Plan and should check the coverage and efficiency of the plan. All the relevant team preparedness should be assessed in this testing. 3. Ensure that the test results are documented, and any exceptions are noted and appropriate corrective action is undertaken.	1. Inspect whether Business Continuity Testing was performed on a periodic basis as per the organization's policy. 2. Inspect the most recent BCP test and inspect DR tests results to determine whether tests were executed and results were documented. 3. Validate whether the results of the testing exercises were tracked to remediation.	E-BC-03
BC-05	Business Continuity	Business Impact Analysis	Organization identifies the business impact of relevant threats to assets, infrastructure, and resources that support critical business functions. Recovery objectives are established for critical business functions.	Process	Corrective	Business Continuity Policy	1. Design and document a process for conducting Business Impact Analysis to determine the criticality of business activities and associated resource requirements. 2. Ensure that BIA is conducted for all processes and assets to identify criticality.	1. Inspect and validate whether a documented process exists for conducting Business Impact Analysis. 2. Inspect Business Impact Analysis to determine whether the threats to assets, infrastructure, and resources are identified and the recovery objectives are established.	E-BC-01 E-BC-02
BC-06	Business Continuity	Capacity Forecasting	Budgets for infrastructure capacity are established based on analysis of historical business activity and growth projections; purchases are made against the	Process	Preventive	Infrastructure Management Policy	1. Ensure that capacity forecasts are created based on the business forecasts, growth projections and analysis of historic business activity.	1. Inspect and validate whether capacity planning was done and forecasts were created.	E-BC-05
BM-01	Backup Management	Backup Configuration	Organization configures redundant systems or performs periodic backups of data to resume system operations in the event of a system failure.	Process	Corrective	Backup Management Policy	1. Ensure that Backup and Restoration process is established, documented and communicated to all the relevant stakeholders. 2. Ensure that all the information systems have redundancy or should be backed up periodically. Periodicity of the backup should be defined basis the criticality of the information system and data. 3. Check the backup configuration for all the storage/database resources whether on-prem or on cloud. 4. Ensure that alert are in place for backup failures and all backup failures are handled appropriately.	1. Inspect documentation to determine whether requirements for the configuration of redundant systems or performance of periodic backups of data to resume system operations are defined. 2.Inspect redundancy or system backup configurations for production systems to determine type, frequency, and storage of backups. 3. Inspect sample alerts for failed backups and validate the remediation steps.	E-BM-01 E-BM-07

BM-02	Backup Management	Resilience Testing	Organization performs annual backup restoration or data replication tests to confirm the reliability and integrity of system backups or recovery operations.	Process	Detective	Backup Management Policy	1. Ensure that the requirement for backup restoration testing is defined and documented appropriately. 2. Ensure that backup restoration testing is performed on an annual basis and ensure that the integrity of backup restores are maintained.	1. Inspect relevant documentation to determine whether requirements for annual backup restoration or failover and failback tests have been defined. 2. Inspect annual backup restoration, or failover and failback tests to determine whether Organization has tested the reliability and integrity of system backups.	E-BM-01 E-BM-02
BM-03	Backup Management	Backup Failure Review	Failed backup jobs are periodically reviewed and resolved in a timely manner.	Process	Corrective	Backup Management Policy	1. Ensure that alert are sent to the system administrators in case of backup failures. 2. All backup failures should be handled appropriately and resolved in a timely manner.	1. Inspect whether failed backup jobs are being reviewed periodically. 2. Inspect alerts are configured to notify administrators if backup fails. 3. Inspect and validate the remediation process for failed backups.	E-BM-03 E-BM-06
BM-04	Backup Management	Alternate Storage	Organization backups are securely stored in an alternate location from source data.	Process	Corrective	Backup Management Policy	1. Ensure that the backups are stored in an alternate location than the source data.	1. Inspect whether backups are stored in a different location than the source data.	E-BM-04
BM-05	Backup Management	Alternate Telecommunication	Alternate telecommunication service agreements have been established to resume business when the primary service gets disrupted. Service agreements contain priority of service provisions.	Process	Preventive	Backup Management Policy	1. Ensure that alternate telecommunication service agreements are defined to resume business when the primary service gets disrupted. 2. The priority of the service provisions should be defined in the service agreements.	1. Inspect whether alternate telecommunication service agreements are defined to resume business when the primary service gets disrupted. 2. Inspect documentation to determine that the Service agreements contain priority of service provisions.	E-BM-05
CFM-01	Configuration Management	Baseline Configuration Standard	Organization ensures security hardening and baseline configuration standards have been established according to industry standards and are reviewed and updated periodically.	Process	Preventive	Infrastructure Management Policy	1. Prepare and maintain Security hardening and Baseline configuration standards shall be established. 2. Configuration of systems (systems can include AWS, Azure, GCP, and more) shall be configured with the baseline configuration. 3. Configure required permissions for the configuration management server. 4. Configuration of Security Groups, NACLs, and virtual firewall appliances shall be in place. 5. Configuration of VPC Firewall Rules and virtual firewall appliances to allow traffic from the configuration management server to the other system servers. 6. All production systems shall be able to demonstrate consistent system configurations via version control number, last update date, settings, or other. 7. Process shall be established to ensure that latest version patch (hardened as per industry practices) is applied wherever possible. 8. Ensure that security hardening and configuration baselines are	1. Validate whether Security hardening and Baseline configuration standards are established. 2. Inspect baseline configuration of systems (systems can include AWS, Azure, GCP, and more) shall be configured with the baseline configuration. 3. Validate whether the required permissions are present for the configuration management server. 4. Inspect Security Groups, NACLs, and virtual firewall appliances configurations. 5. Validate whether VPC Firewall Rules and virtual firewall appliances are configured to allow traffic from the configuration management server to the other system servers. 6. Inspect production systems to determine whether they demonstrate consistent system configurations via version control #, last update date, settings, or other. 7. For a sample of in scope servers validate whether latest version patch (hardened as per industry practices) is applied wherever possible.	Log Management E-CFM-01 E-CFM-02 E-CFM-03 E-CFM-04 E-CFM-05
CFM-02	Configuration Management	Default "Deny-all" Settings	Where applicable, the information system default access configurations are set to "deny-all."	Technology	Preventive	Infrastructure Management Policy	1. Prepare a list of in-scope network devices and production accounts and ensure that default deny-all rules are configured 2. Ensure that deny-all rule precedes all other applied rules in terms of priority.	1. For a list of in-scope network devices and production accounts, validate that default deny-all rules are configured 2. Validate that deny-all rule precedes all other applied rules in terms of priority.	E-AM-02 E-CFM-03
CFM-03	Configuration Management	Remote Access: Prohibited Protocols and Commands	Organization defines a listing of prohibited user commands and prohibited protocols that can be used in a remote session.	Process	Preventive	Infrastructure Management Policy	1. Prepare and maintain the listing of prohibited user commands and prohibited protocols that can be used in a remote session.	1. Inspect security hardening standard to determine the listing of prohibited user commands and prohibited protocols that can be used in a remote session.	E-CFM-06
CFM-04	Configuration Management	Data Execution Prevention	Organization ensures data execution prevention (DEP) security features are enabled on production hosts to restrict code execution within memory.	Technology	Preventive	Infrastructure Management Policy	1. Ensure that configuration setting includes data execution prevention (DEP) security features enabled on production hosts to restrict code execution within memory.	1. Check configuration setting to ensure data execution prevention (DEP) security features are enabled on production hosts to restrict code execution within memory.	E-CFM-02 E-CFM-03

CFM-05	Configuration Management	Client Run Time Technologies	Organization disables prohibited client run time technologies on information systems.	Technology	Preventive	Infrastructure Management Policy	1. Establish a process to ensure no prohibited application/software is installed on the machine.	1. Inspect Organization's software compliance dashboard, to ensure no prohibited application/software is installed on the machine.	E-CFM-07
CFM-06	Configuration Management	Prohibited Activity Monitoring	Organization information systems are configured to explicitly deny a predefined list of activities.	Technology	Detective	Infrastructure Management Policy	1. Prepare a list of activities that shall be denied on Information Systems, e.g., removable media restriction. 2. Ensure that the denied activities are enforced on the Information systems. 3. Ensure that the logs are being maintained for monitoring. 4. The list shall be reviewed periodically.	1. Validate whether a list is being maintained that has the activities that shall be denied on Information Systems. 2. Inspect the activity logs to validate whether the denied activities are enforced and monitored on the Information systems. 3. Validate whether the periodic review history documentation is present.	E-CFM-08 E-CFM-09 E-CFM-10
CFM-07	Configuration Management	Configuration Checks	Organization uses mechanisms to detect deviations from baseline configurations on production environments.	Technology	Detective	Infrastructure Management Policy	1. Ensure that security hardening and configuration baselines are being monitored for in-scope servers. 2. Deviations shall be generated for in-scope servers for which remediations shall be tracked to closure. 3. Design a process for security hardening and configuration baselines checks being accurate and updated at least annually.	1. Validate that security hardening and configuration baselines are being monitored for in-scope servers. 2. Validate that deviations are being generated for in-scope servers and remediations are tracked to closure. 3. Validate that the security hardening and configuration baselines checks are accurate and updated at least annually.	E-CFM-11 E-CFM-05
CFM-08	Configuration Management	Configuration Check Reconciliation: Logging	Organization reconciles the established device inventory against the enterprise log repository on a quarterly basis; devices which do not forward security configurations are remediated.	Process	Corrective	Infrastructure Management Policy	1. Prepare an asset register to ensure asset life cycle is maintained as per the defined policy and/or standard of asset management. 2. Establish a process through which the device configuration logs can be fetched and reconciled with asset register quarterly. 3. Ensure that a process is established that tracks the deviations to remediation.	1. Inspects Organization asset register to ensure asset life cycle is maintained as per the defined policy and/or standard of asset management. 2. Validate whether the device configuration logs are being reconciled with asset register quarterly. 3. Validate for a sample of deviations whether the remediation is done in a timely manner.	E-AM-02 E-CFM-12 with E-AM-02 E-CFM-05
CFM-09	Configuration Management	Time Clock Synchronization	Systems are configured to synchronize information system time clocks based on International Atomic Time or Coordinated Universal Time (UTC).	Technology	Preventive	Infrastructure Management Policy	1. Ensure that the inventory includes all the ICT devices such as firewalls, routers and servers. 2. Ensure that a process has been established to use only hardened images for the servers. 3. Ensure that the NTP configuration (primary & secondary NTP servers) for these devices is configured. 4. Ensure that the time sync is enabled and stratums are defined.	1. Obtain a list of in-scope ICT devices such as firewalls, routers and servers. 2. For servers, validate that security hardened images are used. 3. Obtain the NTP configuration for a sample of devices and check whether primary and secondary NTP servers are configured. 4. Validate whether time sync is enabled and stratums are defined and the time servers are working.	E-CFM-02 E-CFM-14 E-CFM-13 E-CFM-15
CFM-10	Configuration Management	Time Clock Configuration Access	Access to modify time data is restricted to authorized personnel.	Technology	Preventive	Infrastructure Management Policy	1. Ensure that the ability to modify time data is restricted to authorized personnel. 2. Ensure that access reviews of authorized users and all remediations are appropriately tracked	1. Obtain a list of all users who have the ability to modify time data. 2. Validate whether access reviews of these users were performed and all remediations are appropriately tracked	E-CFM-16 E-CFM-17
CFM-11	Configuration Management	Default Device Passwords	Vendor-supplied default passwords are changed according to Organization standards prior to device installation on the Organization network or immediately after software or operating system installation.	Technology	Preventive	Infrastructure Management Policy	1. Ensure that the security hardening and configuration baseline checks include enforcing disablement of default accounts. 2. Ensure that the security hardening and configuration baseline deviations are being tracked to resolution	1. Inspect security hardening and configuration baseline checks to determine whether they are configured to enforce disabling of default accounts. 2. Validate that the security hardening and configuration baseline deviations are being tracked to resolution.	E-CFM-02 E-CFM-05
CFM-12	Configuration Management	Process Isolation	Organization implements only one primary function per server within the production environment; the information system maintains a separate execution domain for each executing process.	Technology	Preventive	Infrastructure Management Policy	1. Ensure that the security hardening and configuration baseline checks include installing one primary function per server within the production environment and the information system maintains a separate execution domain for each executing process. 2. Ensure that the security hardening and configuration baseline deviations are being tracked to resolution.	1. Inspect security hardening and configuration baseline checks include installing one primary function per server within the production environment and the information system maintains a separate execution domain for each executing process. 2. Validate that the security hardening and configuration baseline deviations are being tracked to resolution.	E-CFM-02 E-CFM-18 E-CFM-05

CFM-13	Configuration Management	Collaborative Devices	Where applicable, collaborative computing devices used at Organization are configured to restrict remote activation and provide an explicit indication that they are in use.	Technology	Preventive	Infrastructure Management Policy	1. In case of collaborative computing devices, ensure that an explicit indication is documented confirming its use and requirement. 2. Ensure that the security hardening and configuration baseline checks are configured to restrict remote activation on collaborative computing devices. 3. Ensure that the security hardening and configuration baseline deviations are being tracked to resolution	1. Validate whether the use of collaborative computing devices is being flagged and justification of its use is documented. 2. Inspect security hardening and configuration baseline checks to determine whether collaborative computing devices are configured to restrict remote activation. 3. Validate that the security hardening and configuration baseline deviations are being tracked to resolution	E-CFM-02 E-CFM-19 E-CFM-05
CFM-14	Configuration Management	Software Installation	Installation of software or programs in the production environment is approved by authorized personnel.	Process	Preventive	Infrastructure Management Policy	1. Ensure Security hardening and Baseline configuration standards includes process established to determine whether the installation of software or programs in the production environment is approved by authorized personnel. 2. Prepare an authorized approval matrix for installation of software or programs in the production environment.	1. Inspect Security hardening and Baseline configuration standards to ensure that the installation of software or programs in the production environment is approved by authorized personnel is defined. 2. Inspect the authorized approval matrix for installation of software or programs in the production environment.	E-CFM-02 E-CFM-20
CFM-15	Configuration Management	Job Schedules	Schedule changes or the modifications of production jobs require: • documented approval from authorized personnel • documented monitoring details	Process	Preventive	Change Management Policy	1. Prepare, document, and periodically review Organization's change management standard. 2. Ensure that the change management process includes tracking to determine whether schedule changes or the modifications of production jobs require: • documented approval from authorized personnel • documented monitoring details	1. Obtain Organization's change management standard and validate whether it is periodically reviewed. 2. For a sample of change tickets, inspect change management process flow documentation (e.g., ticketing/tracking tools) to determine whether schedule changes or the modifications of production jobs require: • documented approval from authorized personnel • documented monitoring details	E-CFM-21 E-CFM-22 E-CFM-23 E-CFM-24
CHM-01	Change Management	Change Management Workflow	Change scope, change type, and roles and responsibilities are pre-established and documented in a change control workflow; notification and approval requirements are also pre-established based on risk associated with change scope and type.	Process	Preventive	Change Management Policy	1. Ensure that the change management process is established and well-documented, and should be approved by the management and communicated to all the relevant stakeholders. 2. Ensure that roles and responsibilities are defined for each activity and change scope, that change type is predefined. 3. Ensure that the change workflow has a mandatory approval and notification requirements incorporated based on risk and change type.	1. Inspect Organization's policy to determine whether: a. Change scope, change type, and roles and responsibilities are pre-established. b. Notification and approval requirements are pre-established based on the risk associated with change scope and type. 2. Inspect change management ticketing and tracking tools to determine whether the change control workflow is defined in accordance with the defined requirements.	E-CHM-01 E-CHM-03

CHM-02	Change Management	Change Approval	Prior to introducing changes into the production environment, approval from authorized personnel is required based on the following: • change description • impact of change • test results • back-out plan	Process	Preventive	Change Management Policy	1. Ensure that all the changes to the production environment are tracked in a Change Management tracking tool. All the change details should be documented. Some of the mandatory details for each change are: a. Change Description b. Change Impact c. Test Details d. Roll-out and Roll-back Plan e. Change Approval f. Change date and time 2. All the changes in the production environment should be approved by the authorized personnel prior to implementation. Make sure that the approver is independent of the change requestor and change implementor. If not, check that there a secondary approver to ensure segregation of duty is maintained. 3. Make sure that the deployment and change logs are retained as per organization's policy.	1. Inspect Change Management tracking tool to determine that requirements prior to introducing changes into the production environment, approval from appropriate personnel is documented including the following: a. Change description b. Impact of change c. Test results d. Back-out procedures 2. For a sample of changes, inspect corresponding change tickets, and verify if it includes the following information: a. Change Description b. Impact of changes c. Roll back plan d. Evidence of successful testing documentation e. Approval of change prior to implementation 3. For the sampled changes, validate that the change was approved by a person independent of the person who requested or made the change. Alternatively, ensure that there is a second level of approval to ensure that segregation of duties is being maintained. 4. Inspect whether the change logs are retained as per the organization's policy.	E-CHM-02 E-CHM-03
CHM-03	Change Management	Segregation of Duties	Changes to the production environment are implemented by authorized personnel.	Process	Preventive	Change Management Policy	1. Ensure that the permission to implement changes to the production is limited to few authorized personnels. 2. Ensure that the change implementor is not the change approver.	1. Inspect Change Management tracking tool and for a sample of changes, inspect that change tickets were launched and appropriately approved.	E-CHM-02 E-CHM-03
CHM-04	Change Management	Communication of Maintenance and Downtime	Customer-impacting product and system changes are publicly communicated on the company website.	Process	Preventive	Change Management Policy	1. Ensure that all the changes that impact the customers and customer product or services should be communicated to the customers on the company website. 2. In cases of any planned downtime due to a change, it should be communicated to the customers in advance on the website.	1. Inspect the company website to determine whether customer-impacting product and system changes are publicly communicated.	E-CHM-04
CMS-01	Customer Managed Security	Customer Administrative Access	For products that enable customers to manage their end users, privileged user roles exist with the capability to manage end user access to the relevant applications.	Technology	Preventive	Access Control Policy	1. In cases where customers can manage the access of their end users, ensure that ability to configure privileged user roles exist. 2. Ensure that the customer's privileged user roles can manage end user access to the relevant applications.	1. Validate whether the customers can configure privileged user roles. 2. Inspect whether the customer defined privileged user roles can manage end user access to relevant applications.	E-CMS-01 E-CMS-05
CMS-02	Customer Managed Security	Customer Authentication	Authentication to organization customer-facing applications are performed through secure log-on procedures.	Technology	Preventive	Access Control Policy	1. Ensure that authentication to organization customer-facing applications are performed through secure log-on procedures.	1. Inspect whether the authentication to organization customer-facing applications are performed through secure log-on procedures.	E-CMS-02
CMS-03	Customer Managed Security	Customer Systems Monitoring	As necessary, event logs are made available to customers.	Technology	Preventive	Logging & Monitoring Standard	1. Establish a process for the customers to access event logs as needed.	1. Inspect the customer console to determine how the event logs are made available to the customer.	E-CMS-03
CMS-04	Customer Managed Security	Customer Security Engagements	Organization supports customer-requested security inquiries, questionnaires, and audits: • in accordance with customer contracts and agreements • to facilitate due diligence prior to licensing organization products	Process	Corrective	Customer Authentication Standard	1. Establish a documented process to support customer-requested security inquiries, questionnaires, and audits: • in accordance with customer contracts and agreements • to facilitate due diligence prior to licensing organization products	1. Validate whether a process in place to support customer-requested security inquiries, questionnaires, and audits: • in accordance with customer contracts and agreements • to facilitate due diligence prior to licensing organization products 2. Inspect a sample customer inquiry, questionnaire, or audit.	E-CMS-02 E-CMS-04

CRY-01	Cryptography	Encryption Key Maintenance	Cryptographic keys are invalidated when compromised or at the end of their defined lifecycle period.	Process	Preventive	Cryptographic Management Policy	1. Establish a process to ensure that organization approved key storage solutions are used. 2. Ensure that access to the cryptographic key stores is limited to authorized personnel. 3. Establish a process to periodically review the users access list for the keys and document the confirmation that these are authorized users. 4. Establish a process to ensure that the keys are rotated during either of the below events: a) Suspicion that the key has been compromised b) End of key life cycle 7. In case of termination or transfer of an individual with access to the key, establish a process for access review and key rotation.	1. Inspect the process and location of where Encryption keys are stored. 2. Obtain details of the process to ensure that access to the cryptographic key stores is limited to authorized personnel. 3. Review the users access list for the keys and confirmation that these are authorized users. 4. Obtain confirmation of key rotation at the occurence of either of the below events during last quarter: a) Suspicion that the key has been compromised b) End of key life cycle 7. For a sample of termination or transfer of an individual with access to the key, and review the process of key rotation.	E-CRY-01 E-CRY-02 E-CRY-03
CRY-02	Cryptography	Encryption Key Distribution	Organization prohibits the distribution of cryptographic keys in clear text.	Process	Preventive	Key Management Policy	1. Ensure that the Key management policy hass a prohibition on the distribution of cryptographic keys in clear text.	1. Inspect the Key management policy that shows that there is a prohibition on the distribution of cryptographic keys in clear text.	E-CRY-04
CRY-03	Cryptography	Encryption Key Storage	Encryption keys are securely stored in an approved encryption platform.	Process	Preventive	Key Management Policy	1. Ensure that key management standard includes management operations using one of the listed options below, for encrypting and decrypting cardholder data: -Key-encrypting key is at least as strong as the data-encrypting key and is stored separately from the data-encrypting key -Stored within a cryptographic device -Keys are stored as at least two full-length key components or key shares	1. Inspect and review the key management standard, to ensure that the management operations are using one of the listed options below, for encrypting and decrypting cardholder data: -Key-encrypting key is at least as strong as the data-encrypting key and is stored separately from the data-encrypting key -Stored within a cryptographic device -Keys are stored as at least two full-length key components or key shares 2. Inspect the process and validate that one of the above methods are being used to protect the keys.	E-CRY-04
CRY-04	Cryptography	Clear Text Key Management	If applicable, manual clear-text cryptographic key-management operations must be managed using split knowledge and dual control.	Process	Preventive	Cryptographic Management Policy	1. Ensure that the key management standard includes guidance on management operations being managed using split knowledge and dual controls. 2. Establish a key custodian acknowledgement form. 3. Ensure that when split knowledge is in place, both key components are 2 full keys, not 1 key split into 2 components.	1. Inspect and review the key management standard, to ensure that the management operations are managed using split knowledge and dual controls. 2. Observe and confirm a sample key custodian acknowledgement form. 3. Inspect that if split knowledge is in place both key components are 2 full keys, not 1 key split into 2 components.	E-CRY-04 E-CRY-05
CRY-05	Cryptography	Encryption of Data in Transit	Organization restricted data that is transmitted over public networks is encrypted.	Technology	Preventive	Cryptographic Management Policy	1. Ensure that Organization's Data Classification and Handling Standard and Data Encryption Standard includes requirements for encrypting data at rest.	1. Inspect Organization's Data Classification and Handling Standard and Data Encryption Standard to determine whether requirements for encrypting data at rest were defined.	E-CRY-06 E-CRY-07

CRY-06	Cryptography	Encryption of Data at Rest	Organization restricted data at rest is encrypted.	Technology	Preventive	Cryptographic Management Policy	1. Ensure that Organization's Data Classification and Handling Standard and Data Encryption Standard includes requirements for encrypting data at rest. 2. Where data at rest shall be encrypted as per Data Classification and Handling Standard, ensure the following: a. Ensure encryption is enabled along with type of encryption algorithm being used as applicable (e.g. for AWS S3 - AWS SSE-KMSetc., full disk encryption for on prem databases). b. Ensure that only strong encryption algorithms mandated by Organization Cryptography standard are in use where applicable. c. Establish a process to periodically check the list of all cloud storage resources and determine whether encryption was appropriately applied as applicable.	1. Inspect Organization's Data Classification and Handling Standard and Cryptography Standard to determine whether requirements for encrypting restricted data at rest have been defined. 2. Obtain confirmation from teams that storage of data is in place. For services storing restricted data at rest, obtain and inspect the following: a. List of all databases/storage locations (AWS/Azure Databases, On prem databases, etc.) where data is stored at rest. b. For all the above locations, obtain evidence showing that encryption is enabled along with the type of encryption algorithm being used as applicable (e.g. for AWS S3 - AWS SSE-KMSetc., full disk encryption for on prem databases) to ensure that only strong encryption algorithms mandated by Organization Cryptography standard are in use where applicable. c. Obtain the list of all cloud storage resources and determine whether encryption was appropriately applied as applicable.	E-CRY-06 E-CRY-07 E-CRY-14 E-CRY-16 E-CRY-15
CRY-07	Cryptography	Approved Cryptographic Technology	Where applicable, strong industry standard cryptographic ciphers and keys with an effective strength greater than 112 bits are required for cryptographic security operations.	Process	Preventive	Cryptographic Management Policy	1. Ensure that the encryption is enabled along with type of encryption algorithm being used as applicable (e.g. for AWS S3 - AWS SSE-KMSetc., full disk encryption for on prem databases). 2. Ensure that strong industry standard cryptographic ciphers and keys with an effective strength greater than 112 bits are required for cryptographic security operations.	1. Validate evidence showing that encryption is enabled along with type of encryption algorithm being used as applicable (e.g. for AWS S3 - AWS SSE-KMSetc., full disk encryption for on prem databases) to ensure that only strong encryption algorithms mandated by Organization Cryptography standard are in use where applicable. 2. Validate whether the keys have a strength greater than 112 bits for cryptographic security operations.	E-CRY-06 E-CRY-07
CRY-08	Cryptography	Key Repository Access	Access to the cryptographic keystores is limited to authorized personnel.	Process	Preventive	Cryptographic Management Policy	1. Ensure that the access lists of the key repositories have authorized users and reviewed periodically.	1. Inspect the access lists of the key repositories and ensure that the users listed are authorized and reviewed previously.	E-CRY-17
CRY-09	Cryptography	Key Store Review	Management reviews and authorizes key store locations.	Process	Detective	Key Management Policy	1. Establish a process to review key management services to ensure that they are still authorized key stores. 2. The list of authorized key stores shall be reviewed periodically.	1. Inspect and review key management services to ensure that they are still authorized key stores. 2. Review the list of authorized key stores and their last date of review.	E-CRY-18
CRY-10	Cryptography	Full Disk Encryption Access	Where full disk encryption is used, logical access must be managed independently of operating system authentication; decryption keys must not be associated with user accounts.	Process	Preventive	Access Management Procedure	1. Ensure that the decryption keys are stored in a Trusted Platform Module (TPM). 2. Ensure that the decryption keys are not stored as plain text in insecure storage locations.	1. Confirm that the decryption keys are stored in a Trusted Platform Module (TPM). 2. Confirm that the decryption keys are not stored as plain text in insecure storage locations.	E-CRY-19
CRY-11	Cryptography	Key Custodians Agreement	Cryptographic Key Custodians and Cryptographic Materials Custodians (CMC) acknowledge in writing or electronically that they understand and accept their cryptographic-key-custodian responsibilities.	Process	Preventive	Cryptographic Management Policy	1. Ensure that Key Custodian Acknowledgements are signed by cryptographic key custodians, which will provide assurance of appropriate acknowledgement to the key custodian responsibilities.	1. Obtain and inspect a sample of signed Key Custodian Acknowledgements to validate that cryptographic key custodians have appropriately acknowledged their key custodian responsibilities.	E-CRY-20
CRY-12	Cryptography	Approved Certificate Authorities	Organization restricts the use of digital certificates to those that are signed by approved certificate authorities; a certification path to an accepted trust anchor is established.	Technology	Preventive	Key Management Policy	1. Establish a process for executing periodic SSL tests to ensure that only digital certificates that are signed by approved certificate authorities are accepted.	1. Observe a sample of servers and review their SSL test. 2. Observe the SSL test and confirm that only digital certificates that are signed by approved certificate authorities are accepted.	E-CRY-21

CRY-13	Cryptography	Installation of Software: Certificate Verification	Digital Certificates are verified by information system components prior to installation on the production network.	Technology	Preventive	Key Management Policy	1. Establish a process for executing periodic SSL tests and configuration files to ensure that digital certificates are verified prior to installation on production networks.	1. Observe a sample of servers and review their SSL test. 2. Observe the SSL test and configuration files and ensure that digital certificates are verified prior to installation on production networks.	E-CRY-21 E-CRY-22
CRY-14	Cryptography	Public Key Infrastructure-based Authentication	Information systems are configured to follow an established certification path to an accepted trust anchor; in the case of network failure, a local cache of revocation data is maintained to support validation.	Technology	Preventive	Key Management Policy	1. Establish a process for executing periodic SSL tests to ensure that the identified Certificate authority is authorized to act as a trust anchor.	1. Observe a sample of servers and domains and review their SSL test. 2. Observe the Certificate authority and ensure that it is an authorized to act as a trust anchor.	E-CRY-21
CRY-15	Cryptography	Software Signing	Organization uses a software signing infrastructure to restrict access to organization's code signing private keys used to sign organization authorized software builds.	Technology	Preventive	Secure Development Lifecycle Policy	1. Ensure that a process is defined and documented for software signing. 2. Ensure that the private keys used for software signing are accessible only to a restricted set of personnel.	1. Inspect and validate that a process is defined and documented for software signing. 2. Validate whether the private keys used for software signing are accessible only to a restricted set of personnel. 3. Validate that periodic access reviews are performed for these keys.	E-CRY-23 E-CRY-24
DM-01	Data Management	Data Classification Criteria	Organization's data classification criteria are periodically reviewed, approved by management, and communicated to authorized personnel; the data security management team determines the treatment of data according to its designated data classification level.	Process	Preventive	Data Management Policy	1. Ensure that a Data Classification Criteria is defined and documented. 2. Ensure that this criteria is reviewed and approved periodically and appropriate documentation for the review is retained. 3. Ensure that a process is defined and implemented to ensure data is treated according to its data classification level.	1. Inspect Organization's policy and/or standard to determine whether Organization's data classification criteria is defined. 2. Inspect whether the criteria is periodically reviewed and approved by the management. 3. Validate using sample testing that data is categorized and treated according to its data classification level and defined controls.	E-DM-01 E-DM-02 E-DM-03
DM-02	Data Management	Data Inventory	Organization should identify, label and classify Data based on the Data Classification Criteria.	Process	Preventive	Data Management Policy	1. Ensure that a process for identifying data is defined and documented in the organization. 2. Ensure that the data is labelled and classified as per the Data Classification criteria.	1. Inspect and validate in the Organization's policy and/or standard whether a process for identifying data is defined in the organization. 2. Validate for a sample of data, that it is labelled and classified as per the Data Classification criteria.	E-DM-01 E-DM-03
DM-03	Data Management	Terms of Service	Consent is obtained for Organization's Terms of Service (ToS) prior to collecting personal information and when the ToS is updated.	Process	Preventive	Data Management Policy	1. Ensure that organizations Terms of Service are defined and documented. 2. Ensure that a process is defined for updating the Terms of Service which includes recapturing of consent. 3. Ensure that the consent is taken for the Terms of Service prior to collecting personal information.	1. Inspect and validate whether Terms of Service are defined and documented for the organization. 2. Inspect whether the Terms of Service are updated periodically and ensure that consent is recaptured after updates. 3. For sample of customers validate whether consent was obtained before collection of personal information.	E-DM-04 E-DM-05 E-DM-06

DM-04	Data Management	Personal Information Access Requests	In accordance with Organization policy, upon request, authenticated individuals are provided with a copy of their personal information or disclosures of their personal information in an understandable form and within the defined timeframe.	Process	Preventive	Privacy Policy	1. Ensure that a process is defined, documented, and communicated for requesting a copy of personal information. 2. Ensure that on request a copy of personal information is provided to authenticated individuals as per the policy. 3. Ensure that the information is provided in an understandable form and in a timely manner as per the policy	1. Inspect and validate whether a documented process is defined, and communicated for requesting a copy of personal information. 2. Validate whether on request a copy of personal information was provided to authenticated individuals. 3. Validate that the information was provided in an understandable form and in a timely manner.	E-PRIV-01 E-DM-07
DM-05	Data Management	Personal Information Deletion Requests	In accordance with Organization policy, Organization processes requests for the deletion of personal information.	Process	Preventive	Privacy Policy	1. Ensure that a process is defined, documented, and communicated for requesting deletion of personal information. 2. Ensure that on request personal information is deleted as per the policy.	1. Inspect and validate whether a documented process is defined, and communicated for requesting deletion of personal information. 2. Validate whether on request personal information was deleted as per organization's policy.	E-PRIV-01 E-DM-08
DM-06	Data Management	External Privacy Inquiries	In compliance with Organization policy, Organization reviews privacy-related inquiries, complaints, and disputes.	Process	Preventive	Privacy Policy	1. Ensure that a process is defined, documented and communicated for review of privacy-related inquiries, complaints, and disputes. 2. Ensure that these inquiries, complaints, and disputes are addressed in a timely and well communicated manner.	1. Inspect and validate whether a documented process is defined, and communicated for review of privacy-related inquiries, complaints, and disputes. 2. Validate for a sample whether these inquiries, complaints, and disputes are addressed in a timely and well communicated manner.	E-PRIV-01 E-DM-09
DM-07	Data Management	Test Data Sanitization	Restricted data is redacted prior to use in a non-production environment.	Process	Preventive	Secure Development Lifecycle Policy	1. Ensure that a process is defined, documented, and communicated for redacting or not using production data in test environments. 2. Ensure that sufficient tools and processes exists for creation of dummy test data for testing purposes.	1. Inspect and validate whether a documented process is defined, and communicated for redacting or not using production data in test environments. 2. Validate for a sample, whether any production data is used in test environments. 3. Validate how test data is generated and used for testing.	E-VM-15 E-DM-10
DM-08	Data Management	Personal Information Updates	Organization allows authenticated users to review and update their personal information.	Process	Preventive	Data Management Policy	1. Ensure that a process is defined, documented, and communicated regarding access and update to personal information. 2. Ensure that appropriate justifications are provided for any denied access or update requests. 3. Ensure that a process is defined, documented, and communicated for appealing the denial of access or update request.	1. Inspect and validate whether a documented process exists regarding access and update to personal information. 2. Validate that for any denied access or update requests, appropriate justifications were provided. 3. Inspect and validate whether a documented process exists for appealing the denial of access or update request. 4. Ensure that the access or update request process is well communicated.	E-DM-11 E-DM-12
DM-09	Data Management	Credit Card Data Restrictions	Organization does not store full track credit card data, credit card authentication information, credit card verification code, or credit personal identification number (PIN) which Organization processes for payment.	Technology	Preventive	Data Management Policy	1. Ensure that a process is defined and documented for redaction of credit card data. 2. Ensure that the organization does not store full track credit card data, credit card authentication information, credit card verification code, or personal identification number (PIN).	1. Validate that full credit card track data and sensitive authentication data is not stored in the databases of the Organization.	E-DM-13
DM-10	Data Management	Primary Account Number Data Restrictions	Organization restricts primary account number (PAN) data such that only the first six and last four digits are displayed; authorized users with a legitimate business need may be provided the full PAN.	Technology	Preventive	Data Management Policy	1. Ensure that a process is defined and documented for redaction of credit card data. 2. Ensure that the organization restricts primary account number (PAN) data such that only the first six and last four digits are displayed. 3. Ensure that a process is defined to provide full PAN to authorized users with a legitimate business need.	1. Inspect and validate whether a documented process exists for redaction of credit card data. 2. Validate that primary account number is stored such that only the first six and last four digits are displayed. 3. Inspect and validate whether a documented process exists to provide full PAN to authorized users with a legitimate business need.	E-DM-01 E-DM-13 E-DM-14
DM-11	Data Management	Personal Information Inventory	Organization maintains a documented inventory of media containing personal information.	Process	Preventive	Data Management Policy	1. Ensure that an inventory of media containing personal information is documented, approved, and communicated to appropriate stakeholders. 2. Ensure that this inventory is reviewed and update periodically.	1. Inspect and validate whether an inventory of media containing personal information is formally documented. 2. Ensure that a process is defined to review and update the inventory periodically.	E-DM-01 E-DM-15

DM-12	Data Management	Changes to Data at Rest	Organization uses mechanisms to detect direct changes to the integrity of customer data and personal information; Organization takes action to resolve confirmed unauthorized changes to data.	Technology	Detective	Data Management Policy	1. Ensure that a process is defined and documented to detect unauthorized changed to customer data. 2. Ensure that appropriate alerts are sent and actions are taken to resolve unauthorized changes.	1. Inspect and validate that a process is defined and documented to detect unauthorized changed to customer data. 2. Validate whether alerts are sent and actions were taken to resolve unauthorized changes.	E-DM-01 E-DM-16
DM-13	Data Management	Data Processing Integrity	System checks are in place to ensure both complete and accurate capture of data in process.	Technology	Detective	Data Management Policy	1. Ensure that a process is defined and documented for ensuring data integrity in transit and at rest 2. Ensure appropriate tests are used to check checksums or hashes to ensure data integrity.	1. Inspect and validate that a process for ensuring data integrity in transit and at rest is defined and documented. 2. Validate and inspect the tests used to check checksums or hashes to ensure data integrity	E-DM-01 E-DM-16
DM-14	Data Management	Secure Disposal of Media	Organization securely erases media containing decommissioned restricted data and obtains a certificate or log of erasure; media pending erasure are stored within a secured facility.	Process	Preventive	Data Management Policy	1. Ensure that requirements for destroying media containing decommissioned restricted data are defined and documented. 2. Ensure that the requirements for maintaining a log of such activities is defined. 3. Ensure that appropriate records are maintained for such activities. 4. Ensure a security facility is designated to store such media prior to erasure. 5. Ensure a certificate of erasure is obtained for such media post erasure completion.	1. Inspect and validate whether requirements for destroying media containing decommissioned restricted data are defined and documented. 2. Inspect and validate that the requirements for maintaining a log of such activities is defined. 3. Validate that appropriate records are maintained for such activities. 4. For a sample of records, validate that a certificate of erasure was obtained for such media post erasure completion.	E-DM-01 E-DM-17
DM-15	Data Management	Customer Data Retention and Deletion	Organization purges or archives data according to customer requests or legal and regulatory mandates.	Process	Preventive	Privacy Policy	1. Ensure that a process is defined, documented, and communicated for requesting deletion or archival of personal information. 2. Ensure that on customer's request or as per legal/regulatory mandates, personal information is deleted/archived as per the policy.	1. Inspect and validate whether a documented process is defined & communicated for requesting deletion/archival of personal information. 2. Validate whether on customer's request or as per legal/regulatory mandates personal information is deleted/archived as per the policy.	E-PRIV-01 E-DM-08
DM-16	Data Management	Removal of PHI from Media	Organization removes electronic protected health information from electronic media if the media is made available for re-use.	Process	Preventive	Data Management Policy	1. Ensure that a process is defined and documented for removal of Protected Health Information from electronic media if the media is made available for reuse. 2. Ensure that validation is done to ensure that no protected health information exists on the media before reuse.	1. Inspect and validate that a process is defined and documented for removal of Protected Health Information from electronic media if the media is made available for reuse. 2. Inspect whether validation is done to ensure that no protected health information exists on the media before reuse.	E-DM-01
DM-17	Data Management	Secure Disposal of Media: Testing	Organization tests sanitization procedures and equipment annually for effectiveness.	Process	Detective	Data Management Policy	1. Ensure that a process is defined and documented for testing of sanitization procedures. 2. Ensure that the sanitization procedures are tested annually and appropriate records are maintained.	1. Inspect and validate that a process is defined and documented for testing of sanitization procedures. 2. Validate whether the sanitization procedures were tested annually.	E-DM-01 E-DM-18
DM-18	Data Management	Personal Information Retention and Deletion	Organization retains and deletes personal information from Organization and service provider systems in accordance with Organization policy.	Process	Preventive	Data Management Policy	1. Ensure that a process is defined and documented for retention and deletion of personal information. 2. Ensure that the personal information is retained and deleted as per the process from organization and service provider systems.	1. Inspect and validate that a process is defined and documented for retention and deletion of personal information. 2. Validate whether the personal information was retained and deleted as per the process.	E-DM-01 E-DM-19
DM-19	Data Management	Temporary Storage of Personal Information	Temporary files and documents containing personal information are deleted in accordance with a timeframe consistent with Organization policy.	Process	Preventive	Data Management Policy	1. Ensure that a process is defined and documented for deletion of temporary files. 2. Ensure that temporary files are deleted within a defined timeframe as per the process.	1. Inspect and validate that a process is defined and documented for deletion of temporary files. 2. Validate the configuration for deletion of temporary files and ensure that the timeframe is as per the process.	E-DM-01 E-DM-20
DM-20	Data Management	Social Media	Sharing Organization restricted data via messaging technologies, social media, and public websites is prohibited.	Process	Preventive	Data Management Policy	1. Ensure that a process is defined, documented, and communicated which prohibits sharing of restricted data via messaging technologies, social media, and public websites. 2. Ensure that appropriate mechanisms are in place to detect such activities.	1. Inspect and validate whether a process is defined, documented and communicated which prohibits sharing of restricted data via messaging technologies, social media, and public websites. 2. Validate whether appropriate mechanisms are in place to detect such activities and alerts are generated.	E-DM-01 E-DM-21

DM-21	Data Management	Publicly Accessible Content	Organization protects its public information system presence with the following processes: only authorized and trained individuals may post public information, content is reviewed prior to publishing, information on public systems is reviewed periodically, and non-public information is removed from public systems upon discovery.	Process	Preventive	Data Management Policy	1. Ensure that a process is defined, documented, and communicated regarding publishing of information on public websites. 2. Ensure public information is reviewed periodically. 3. Ensure appropriate process is defined for removing non-public information from public websites. 4. Ensure appropriate access control exists for posting information on public websites.	1. Inspect and validate whether a process is defined, documented, and communicated regarding publishing of information on public websites. 2. Validate whether public information is reviewed periodically. 3. Validate the process for removing non-public information from public websites. 4. Validate that appropriate access control exists for posting information on public websites.	E-DM-01 E-DM-23
DM-22	Data Management	Data Loss Prevention	Data loss prevention capabilities are implemented to protect sensitive information as it is stored, transmitted, and processed.	Technology	Preventive	Logging & Monitoring Standard	1. Ensure that Data Loss Prevention solution is enabled on systems to protect sensitive data as it is stored, transmitted, and processed. 2. Ensure appropriate alerts are sent and actions are taken to remediate any deviations.	1. Validate whether that Data Loss Prevention solution is enabled on a sample system. 2. Validate whether appropriate alerts are sent and actions are taken to remediate any deviations.	E-DM-22 E-DM-21
EM-01	Entity Management	Board of Directors Structure and Purpose	The Board of Directors provides corporate oversight, strategic direction, and review of management for Organization. The Board of Directors meets at least quarterly and has 3 sub-committees: • Audit Committee • Executive Compensation and Nominating Committee • Governance Committee	Process	Preventive	Information Systems Operations Policy	1. Document the Board of Directors responsibilities and members within a charter. 2. Ensure Board of Directors meet at least quarterly, and document meeting minutes of each meeting. 3. Ensure Board of directors have at least 3 sub-committees defined and formed, audit committee, executive compensation and nominating committee, and governance committee.	1. Inspect that the board of directors information in the form of Charter is available on the Organization governance website. 2. Validate that board of directors meet at least quarterly to provide corporate oversight and have at least 3 sub-committees defined: audit committee, executive compensation and nominating committee, and governance committee.	E-EM-01 E-EM-02
EM-02	Entity Management	Audit Committee	The Audit Committee is governed by a Charter, is independent from Organization Management, composed of outside directors (Industry Experts), and meets quarterly. The Audit Committee oversees: •Financial Statement Quality •Enterprise Risk Management •Regulatory & Legal Compliance •Internal Audit Functions •Information Security Functions •External Audit Functions	People	Preventive	Information Systems Operations Policy	1. Ensure documented information on the Audit Committee and Audit Committee Charter is created. 2. Ensure that the audit committee is independent and meets quarterly as defined within the charter. Document the most recent meeting in the form of an audit committee minutes. 3. Ensure that the audit committee includes outside directors (industry experts). 4. Ensure audit committee reviews financial statement quality, enterprise risk management, regulatory & legal compliance, internal and external audit function, and information security functions. 5. Follow up on any open items from previous audit committee meetings to ensure they are being worked on and closed out.	1. Inspect the Charter of the Audit Committee of the Board of Directors and meeting minutes to determine whether the Audit Committee is independent from management, and is composed of outside directors. 2. Validate that the audit committee is independent and meets quarterly as defined within the charter. 3. Inspect the minutes of meeting audit committee. 4. Validate meeting minutes to ensure that financial statement quality, enterprise risk management, regulatory & legal compliance, internal and external audit function, and information security functions were reviewed.	E-EM-03 E-EM-04 E-EM-05 E-EM-06
EM-03	Entity Management	Organizational Structure	Organization Management ensures that its organization is aligned with the corporate strategy by assigning key managers with responsibilities to execute the corporate strategy.	Process	Preventive	Information Systems Operations Policy	1. Ensure the organization has defined and documented a corporate strategy including the responsibilities for key managers. 2. Ensure the strategy is available to the respective stakeholder and is communicated effectively.	1. Validate and ensure that the organization has established and documented the strategy with the responsibilities for key managers. 2. Inspect whether the strategy is available to the respective stakeholder and is communicated effectively.	E-EM-07
EM-04	Entity Management	Operating Plans	Annual operating plans are aligned with Corporate Objectives, which are established on an annual basis during the Company's planning process. Priorities are set and plans are communicated appropriately.	Process	Preventive	Information Systems Operations Policy	1. Ensure that operating plans are established. 2. Ensure that these plans are updated and approved on an annual basis. 3. Ensure priorities are set and plans are communicated to the respective stakeholders.	1. Inspect the process of operating plans creation and update. 2. Validate that the corporate strategy is an input to operating plans update process. 3. Validate whether the plans are updated and approved at least annually and communicated to the stakeholders.	E-EM-08 E-EM-09
EM-05	Entity Management	Cyber Security Insurance	Organization purchases cyber security insurance to mitigate risk of material financial impact that could result from a cyber security event.	Process	Corrective	Information Systems Operations Policy	1. Ensure cyber security insurance is being purchased by the organization and is active for the audit period. 2. Ensure that a process is created for renewal of Cyber Security Insurance.	1. Obtain and inspect the latest cyber security insurance to verify that the insurance policy is active for the audit period.	E-EM-10

EM-06	Entity Management	Internal Audit Function	Quarterly, the Chief Audit Executive meets with the Audit Committee to review key risk issues. The Audit Committee approves the annual Internal Audit Plan. Results of quarterly audits and subsequent issue tracking summaries are presented to the Audit Committee.	Process	Corrective	Information Systems Operations Policy	1. Ensure key risk issues shall be reviewed at least quarterly by the audit committee and document the issues identified along with the plan of action for risk remediation. 2. Ensure the Internal audit plan is annually approved by the audit committee. 3. Ensure results of quarterly audits and issues identified as a part of audit are presented to the Audit Committee.	1. Inspect Minutes of audit committee meeting and validate that it highlights the key risks identified, plan of action along with the timeline. 2. Check internal audit plan to ensure it was approved by the audit committee. 3. Inspect and validate whether results of quarterly audits are presented to the audit committee.	E-EM-11 E-EM-12 E-EM-13
EM-07	Entity Management	Financial Control Review	Internal financial control assessment results are reported to the Audit Committee by the Chief Audit Executive on a quarterly basis and support the CEO/CFO 302/404 certifications.	Process	Preventive	Information Systems Operations Policy	1. Ensure Chief Audit committee shall report the internal financial control assessment results to the Audit Committee on a quarterly basis.	1. Inspect Minutes of the audit committee meeting to ensure internal financial control assessment results are discussed and reported on a quarterly basis.	E-EM-14
EM-08	Entity Management	Information Security Function	Quarterly, the Chief Security Officer meets with the Audit Committee to review key Information Security issues. Results of continuous monitoring activities and current security compliance status are presented to the Audit Committee and the Board of Directors.	Process	Preventive	Information Systems Operations Policy	1. Ensure audit committee reviews the Information security issues at least quarterly and document the issues identified along with the plan of action for risk remediation. 2. Ensure Minutes of Meetings to be documented stating the compliance status. 3. Ensure results of continuous compliance activities and current compliance status are reported to the Audit Committee and the Board of Directors in the form of PowerPoints, documents, etc.	1. Validate whether information security issues are reviewed at least quarterly by the audit committee along with remediation plans. 2. Inspect minutes of audit committee meeting with chief security officer to ensure security compliance status along with the continuous monitoring of action plan is discussed.	E-EM-15
EM-09	Entity Management	Information Security Compliance Review	Information Security compliance results are reported to the Audit Committee by the Chief Security Officer on a quarterly basis and support information security compliance certifications	Process	Preventive	Information Systems Operations Policy	1. Ensure Minutes of Meetings to be documented stating the compliance results on a quarterly basis. 2. Ensure results of current security compliance status and issues identified as a part of audit are reported to the Audit Committee in the form of PowerPoints, documents, etc.	1. Obtain and inspect evidence that quarterly Information Security compliance results were reported to the Audit Committee.	E-EM-16
EM-10	Entity Management	Common Controls Framework	Organization maintains a Common Control Framework (CCF) that is used in the implementation of control measures as a risk mitigation strategy to support organization operations, technology infrastructure, and security management activities.	Process	Preventive	Information Security Management Standard	1. Ensure that a control set is created to govern the organization's information security program. 2. Document the control set and ensure it is communicated with relevant stakeholders.	1. Validate whether a control framework exists for managing the organization's information security program. 2. Ensure that this control set is documented and available to relevant stakeholders.	E-EM-17
EM-11	Entity Management	Service Agreement	When customers sign-up for Organization's product and services, the customer is required to acknowledge a service agreement which includes considerations for protecting security, availability, confidentiality and indicates the responsibilities of the users and organization's responsibilities and commitments.	Process	Preventive	Third-Party Service Agreement	1. Ensure that the customers acknowledge a service agreement including considerations for protecting security, availability, confidentiality. 2. Ensure that the service agreement contains responsibilities of users and the organization.	1. Validate whether customers acknowledge a service agreement. 2. Validate whether the agreement contains considerations for protecting security, availability, confidentiality. 3. Validate whether the agreement contains users and organizations responsibilities.	E-EM-18
IAM-01	Identity and Access Management	Logical Access Provisioning	Logical access provisioning to information systems requires approval from appropriate personnel.	Process	Preventive	Access Management Procedure	1. Design and document a process for Logical Access and requirements for access provisioning. 2. Ensure access approval logic is mandated in the access management portal accordingly. 3. Ensure that the access management portal is updated with the relevant approvers.	1. Inspect Organization Logical Access Policy and/or Standard to determine that the requirements for access provisioning were defined. 2. Inspect evidence of the workflow from access management portal showing access requires approval and is provisioned upon approval. 3. Inspect the system generated list of identity and access groups which are in-scope and associated workgroups with approvers from access management portal. 4. Inspect access provisioning system logs for a selection of users who were granted access to production systems.	E-IAM-01 E-IAM-02 E-IAM-03

IAM-02	Identity and Access Management	Change of Access Notification	Changes made to system access trigger a notification that is sent to designated personnel.	Technology	Detective	Access Management Procedure	1. Design and document a process for Logical Access and requirements for access modification. 2. Ensure that any change made to access triggers a notification in the access management portal accordingly.	1. Inspect Organization Logical Access Policy and/or Standard to determine the requirements for access provisioning were defined. 2. Validate for a sample access change, that a notification in the access management portal was triggered to the management.	E-IAM-01 E-IAM-04 E-IAM-05
IAM-03	Identity and Access Management	Logical Access De-provisioning	Logical access that is no longer required in the event of a termination is documented, communicated to management, and revoked.	Process	Preventive	Access Management Procedure	1. Design and document a process for Logical Access and requirements for access de-provisioning. 2. Ensure access termination logic is mandated in the access management portal accordingly.	1. Inspect Organization's Logical Access Account Standard to determine whether the requirements for access de-provisioning or terminations were defined. 2. Inspect the list of system generated population of terminated full-time and temporary employees and contractors from the HR system. 3. Inspect configurations to determine that user accounts are disabled after they are no longer required.. 4. Inspect removals from the access management tool for a selection of terminations.	E-IAM-01 E-IAM-02 E-IAM-07
IAM-04	Identity and Access Management	Logical Access De-provisioning: Notification	The People Resources system sends a notification to relevant personnel in the event of a termination of an information system user.	Technology	Preventive	Access Management Procedure	1. Ensure that on access termination, the access management portal triggers a notification to the relevant personnel.	1. Inspect resource management portal to check if the relevant stakeholders are informed upon an employee's termination of an information system user.	E-IAM-02 E-IAM-06
IAM-05	Identity and Access Management	Logical Access Review	Organization performs account and access reviews on a quarterly basis; corrective action is taken where applicable.	Process	Detective	Access Management Procedure	1. Design and document a process for Logical Access and requirements for access reviews. 2. Ensure access reviews are performed as per defined frequency. 3. Ensure that the necessary corrective action has been taken, if required.	1. Inspect Organization's Logical Access Account Standard to determine whether the requirements for access reviews were defined. 2. Inspect the access reviews reconciliation report on a quarterly basis. 3. For a sample of services, inspect the access review for the selected quarters. 4. In case of any discrepancy, ensure that corrective action has been taken and appropriate approval is obtained from the authorized personnel.	E-IAM-01 E-IAM-08 E-IAM-09
IAM-06	Identity and Access Management	Role Change: Access De-provisioning	Upon notification of an employee reassignment or transfer, management reviews the employee's access for appropriateness. Access that is no longer required is revoked and documented.	Process	Preventive	Access Management Procedure	1. Design and document a process for Logical Access and requirements for access modification in case of transfer or reassignment. 2. Ensure access reviews are performed appropriately. 3. Ensure that the necessary corrective action has been taken, if required.	1. Inspect Organization's Logical Access Account Standard to determine whether the requirements for access modifications were defined and includes the case of employee reassignment or transfer. 2. Inspect the user access reconciliation report to ensure that the user access reviews are completed appropriately. 3. In case of any discrepancy, ensure that corrective action has been taken inspect the list of terminated users from the audit period. 4. For a sample of terminated users, validate that access was terminated in a timely and appropriate manner.	E-IAM-01 E-IAM-08 E-IAM-09
IAM-07	Identity and Access Management	Shared Logical Accounts	Organization restricts the use of shared and group authentication credentials. Authentication credentials for shared and group accounts are reset every 90 days.	Process	Preventive	Access Management Procedure	1. Design and document a process for Logical Access and requirements for rotation of shared credentials. 2. Ensure that shared secrets were rotated as per the defined policy.	1. Inspect the Logical Access Account Standard to determine whether Organization requires the restriction of shared and group authentication credentials, and that authentication credentials are rotated 2. For a sample of services validate that shared secrets were rotated as per the defined policy and appropriate evidences are available.	E-IAM-01 E-IAM-10

IAM-08	Identity and Access Management	Shared Logical Accounts: Group Member	Passwords for shared and group accounts are reset when a member of the shared group leaves.	Process	Preventive	Access Management Procedure	1. Design and document a process for Password Policy and requirements for changing password of shared and group accounts. 2. Ensure that the password is changed if a member of the shared group leaves.	1. Inspect Organization's password policy and check requirement for changing the password for shared and group accounts are clearly defined. 2. Inspect shared credential storage tools to check the operational effectiveness and ensure passwords are changed when a member of the shared group leaves.	E-IAM-16 E-IAM-11
IAM-09	Identity and Access Management	Shared Account Restrictions	Where applicable, the use of generic and shared accounts to administer systems or perform critical functions is prohibited; generic user IDs are disabled or removed.	Process	Preventive	Access Management Procedure	1. Ensure that there are no generic or shared accounts used. 2. Ensure that production access is controlled and does not use generic or shared accounts.	1. Review and ensure that there are no generic or shared accounts. 2. Validate for a sample of services that production access is controlled and is configured to use unique user accounts and that a generic or shared ID is not used..	E-IAM-12 E-IAM-13
IAM-10	Identity and Access Management	Role Change: People Resources Notification	The People Resources system sends a notification to relevant management and relevant information system administrators in the event of an employee reassignment or transfer of an information system user.	Technology	Preventive	Access Management Procedure	1. Design and document a process for Logical Access and requirements for access modification in case of transfer or reassignment. 2. Ensure access management portal sends a notification to concerned personnel.	1. Inspect resource management portal to check if the relevant stakeholders are informed upon an event of an employee reassignment or transfer of an information system user.	E-IAM-01 E-IAM-02 E-IAM-04 E-IAM-15
IAM-11	Identity and Access Management	Temporary Account Termination	Temporary and emergency accounts are automatically terminated 90 days from the date they are generated.	Technology	Preventive	Access Management Procedure	1. Design and document a process for Access control and requirements for automatic termination of temporary and emergency accounts. 2. Ensure that the access management portal is configured to terminate temporary and emergency accounts within 90 days.	1. Inspect Organization's access control policy to check policy pertaining to temporary and emergency accounts are automatically terminated 90 days from the date they are generated, is clearly defined. 2. Check the access management tool to ensure the effectiveness of termination of temporary and emergency accounts within 90 days..	E-IAM-01 E-IAM-14
IAM-12	Identity and Access Management	Unique Identifiers	Organization requires unique identifiers for user accounts and prevents identifier reuse.	Process	Preventive	Access Management Procedure	1. Ensure unique identifiers are used for user accounts.	1. Inspect Organization's Authentication Standard to determine whether unique identifier requirements are documented. 2. Perform a walkthrough of user account creation of an existing user to determine whether identifier reuse is prevented. 3. Obtain a complete list of existing users with identifiers to determine whether same identifier is not used for any two users.	E-IAM-16 E-IAM-02 E-IAM-17
IAM-13	Identity and Access Management	Password Authentication	User and device authentication to privileged information systems is protected by passwords that meet Organization's password complexity requirements.	Technology	Preventive	Access Management Procedure	1. Ensure that user and device authentication to privileged information systems is protected by passwords that meet Organization's password complexity requirements.	1. Inspect Organization's Authentication Standard to determine whether the policies contain requirements for the creation, allocation, change, distribution, and safeguarding of passwords. 2. Inspect the accessmanagement tool setting to determine password complexity, consecutive re-use, and change frequency requirements of passwords is in accordance with organization password complexity requirements.	E-IAM-16 E-IAM-18
IAM-14	Identity and Access Management	Multifactor Authentication	Multi-factor authentication is required for: • remote VPN sessions • access to trusted data environments	Technology	Preventive	Access Management Procedure	1. Ensure remote connection to the corporate network is invoked via VPN and VPN in turn invokes Multi-factor authentication	1. Inspect Organization's Remote Access Standard to determine whether requirements for remotely connecting to the corporate network are defined. 2. Observe a user remotely connect to the Organization Corporate Network via VPN. 3. Inspect system configuration of VPN software to determine whether Multi-factor authentication is required. 4. Perform a walkthrough of system connecting to Organization network remotely via vpn software to determine whether Multi- factor authentication is required for remote VPN session.	E-IAM-19 E-IAM-20 E-IAM-21

IAM-15	Identity and Access Management	Authentication Credential Maintenance	Authorized personnel verify the identity of users before modifying authentication credentials on their behalf.	Process	Preventive	Access Management Procedure	1. Document and validate the process of modifying credentials. 2. Ensure that verification is done before modification	1. Validate the process with the IT Helpdesk at least on an annual basis. 2. Inspect whether necessary and updated documentation is available on the process.	E-IAM-22
IAM-16	Identity and Access Management	Session Timeout	Information systems are configured to terminate inactive sessions after 15 minutes or when the user terminates the session.	Technology	Preventive	Access Management Procedure	1. Ensure that information systems are configured to terminate inactive sessions after 15 minutes or when the user terminates the session.	1. Inspect Organization's Logical Access Account Standard to determine whether the requirements for access reviews were defined. 2. Inspect the server samples from the service team. 3. Select the sample from the listing and inspect session timeout configuration	E-IAM-01 E-IAM-23
IAM-17	Identity and Access Management	Session Limit	Information systems are configured to limit concurrent login sessions and the inactive user interface is not displayed when the session is terminated.	Technology	Preventive	Access Management Procedure	1. Ensure that the systems are configured to limit concurrent login sessions. 2. Ensure that inactive user interface is not displayed when the session is terminated.	1. Inspect Organization's access control policy to check clauses pertaining to limited concurrent login sessions and the inactive user interface is not displayed when the session is terminated are clearly defined. 2. Check logical access systems to ensure the effectiveness for the same.	E-IAM-24 E-IAM-25
IAM-18	Identity and Access Management	Account Lockout: Cardholder Data Environments	Users are locked out of information systems after 6 invalid attempts for a minimum of 30 minutes, or until an administrator enables the user ID.	Technology	Preventive	Access Management Procedure	1. Ensure that user lock out parameters are defined and implemented to lockout after 6 invalid attempts for minimum 30 minutes.	1. Inspect Organization's Authentication Standard to determine whether the policies contain requirements for the account lockout post failed login attempts. 2. Inspect the logical access systems setting to determine that account lockout policy is configured with Organization password requirements to lock a user's account after 6 failed attempts for a minimum of 30 minutes or until it is reset by a System Administrator	E-IAM-16 E-IAM-26
IAM-19	Identity and Access Management	Account Lockout	Users are locked out of information systems after multiple, consecutive invalid attempts within a defined period; accounts remain locked for a defined period.	Technology	Preventive	Access Management Procedure	1. Ensure that user lock out parameters are defined and implemented	1. Inspect Organization's access control policy to check clauses pertaining to accessing system by multiple failed attempts are clearly defined. 2. Check check logical access systems to ensure the effectiveness for the same.	E-IAM-16 E-IAM-26
IAM-20	Identity and Access Management	Login Banner	Systems leveraged by the U.S. Federal Government present a login screen that displays the following language: • users are accessing a U.S. Government information system • system usage may be monitored, recorded, and subject to audit • unauthorized use of the system is prohibited and subject to criminal and civil penalties • use of the system indicates consent to monitoring and recording	Technology	Preventive	Access Management Procedure	1. Ensure that the Systems leveraged by the U.S. Federal Government present a login screen that displays the following language: • users are accessing a U.S. Government information system • system usage may be monitored, recorded, and subject to audit • unauthorized use of the system is prohibited and subject to criminal and civil penalties • use of the system indicates consent to monitoring and recording	1. Inspect and validate for a sample system that Systems leveraged by the U.S. Federal Government present a login screen that displays the following language: • users are accessing a U.S. Government information system • system usage may be monitored, recorded, and subject to audit • unauthorized use of the system is prohibited and subject to criminal and civil penalties • use of the system indicates consent to monitoring and recording	E-IAM-27
IAM-21	Identity and Access Management	Credentials Validation	Organization systems utilize Federal Identity, Credential, and Access Management (FICAM) components and conform to FICAM-issued profiles; systems verify and accept the following external credentials: • personal Identity Verification (PIV) credentials from federal agencies, and • FICAM-approved credentials from non-federal third-parties	Technology	Preventive	Access Management Procedure	1. Ensure that the organization uses Federal Identity, Credential, and Access Management (FICAM) components and conform to FICAM-issued profiles for Federal Systems. 2. Ensure that the organization accepts personal Identity Verification (PIV) credentials from federal agencies and FICAM-approved credentials from non-federal third-parties	1. Inspect and validate whether the organization uses Federal Identity, Credential, and Access Management (FICAM) components and conform to FICAM-issued profiles for Federal Systems. 2. Validate that the organization accepts personal Identity Verification (PIV) credentials from federal agencies and FICAM-approved credentials from non-federal third-parties	E-IAM-27

IAM-22	Identity and Access Management	Password Authentication Standard: Federal Systems	Organization information systems obscure feedback of authentication information during the authentication process (e.g., the system does not disclose error information such as "'user1' is not a valid username") and have the following password requirements: • minimum of 12 characters • contains at least one upper-case letter, lower-case letter, number, and a special character • at least one of the characters is changed when the new passwords are created. • the password life span is between 1 to 60 days • password reuse is prohibited for 24 generations • only allow the use of temporary password system logons with an immediate change to a permanent password	Technology	Preventive	Access Management Procedure	1. Ensure that failed authentication notes do not contain any error information. 2. Ensure that the password policy in the logical access system is defined as below: -Minimum 12 character length -Password complexity has one upper-case, lower-case, and a special character -Temporary Passwords are immediately changed to a permanent password -Passwords cannot be the same as the last 24 passwords -Passwords must be rotated at least every 60 days	1. Inspect that failed authentication notes do not contain any error information. 2. Inspect that the password policy in the logical access system and ensure that it is defined as below: -Minimum 12 character length -Password complexity has one upper-case, lower-case, and a special character -Temporary Passwords are immediately changed to a permanent password -Passwords cannot be the same as the last 24 passwords -Passwords must be rotated at least every 60 days	E-IAM-28 E-IAM-18
IAM-23	Identity and Access Management	Privileged Session Management	Privileged logical access to trusted data environments is enabled through an authorized session manager; session user activity is recorded and tunnelling to untrusted data environments is restricted.	Process	Preventive	Access Management Procedure	1. Ensure Privileged logical access to trusted data environments is enabled through an authorized session manager. 2. Ensure session user activity is recorded and documented. 3. Tunnelling to untrusted data environments is restricted.	1. Observe user access management process for managing privileged access to trusted data environments in accordance with organization policies and verify the following: • Creation and allocation of privileged user accounts/IDs on the information systems is controlled through a formal authorization process. • Privilege access to trusted data environments are enabled through an authorized session manager • Privileged access rights are allocated to users on a time bound need-to-use basis and on an event-by-event basis in line with the access control policy, i.e. based on the minimum requirement for their functional roles and shall be revoked post that defined time period; • All session user activities are recorded and tunnelling to untrusted data environments is restricted 2. Inspect list of users that have privileged logical access to trusted data environments. 3. For a sample of user, inspect evidence of screenshot showing privilege access to trusted data environments is granted by authorized session manager. 4. Inspect configuration showing that session recording for user activity is recorded.	E-IAM-01 E-IAM-29 E-IAM-30 E-IAM-31 E-IAM-32
IAM-24	Identity and Access Management	Zero Trust Enterprise Network	Organization users are authenticated against a Zero Trust model prior to gaining access to organization resources.	Technology	Preventive	Access Control Policy	1. Ensure that a process is defined and documented for the organization's zero trust architecture. 2. Ensure that a zero trust access authorization infrastructure is effectively operating for accessing organization's resources.	1. Inspect and validate that a process is defined and documented for the organization's zero trust architecture. 2. Validate whether all access to organization's resources are via a zero trust method.	E-IAM-24 E-IAM-33
IAM-25	Identity and Access Management	Logical Access Role Permission Authorization	Initial permission definitions, and changes to permissions, associated with logical access roles are approved by authorized personnel.	Process	Preventive	Access Management Procedure	1. Ensure that access to systems is granted after appropriate approvals. 2. Ensure that production access is controlled via authentication methods.	1. Observe and validate for a sample user, that the access to the systems was approved by the appropriate party based on the business need. 2. Validate for a sample of services, that production access is controlled via appropriate authentication methods and is configured to use appropriate logical access lists.	E-IAM-12 E-IAM-34 E-IAM-35

IAM-26	Identity and Access Management	Source Code Security	Access to modify source code is restricted to authorized personnel.	Process	Preventive	Access Management Procedure	1. Ensure that access to modify source code is restricted to authorized personnel.	1. Observe and validate the change management process for code development process. 2. Observe configurations in code source management tools showing that only authorized users are able to make changes to source code. 3. Observe a sample of code change tickets, to show that only authorized personnel were able to make the appropriate change necessary.	E-IAM-36 E-IAM-37
IAM-27	Identity and Access Management	Service Account Restrictions	Individual user or administrator use of service accounts for O/S, applications, and databases is prohibited.	Process	Preventive	Access Management Procedure	1. Ensure that Individual user or administrator use of service accounts for O/S, applications, and databases is prohibited.	1. Review all interactive service accounts used within the environment and confirm that they are disabled or removed. 2. If interactive service accounts are in use these accounts should be stored in a shared credential management tool., and access to these accounts need to be tied back to an individual user.	E-IAM-38 E-IAM-39
IAM-28	Identity and Access Management	PCI Account Restrictions	Organization clients with access to the cardholder data environment (CDE), as users or processes, are assigned unique accounts that cannot modify shared binaries or access data, server resources, or scripts owned by another CDE or Organization; application processes are restricted from operating in privileged-mode.	Technology	Preventive	Access Management Procedure	1. Ensure that in cases of multi-tenant environments one organization or user cannot effect the security or integrity of another organizations resources. 2. Ensure that users are restricted from using privileged-mode.	1. Review the network architecture diagram and confirm that in cases of multi-tenant environments that one organization or user cannot effect the security or integrity of another organizations resources. 2. Observe the application processes showing that they are restricted from using privileged-mode.	E-IAM-24 E-IAM-40 E-IAM- 42
IAM-29	Identity and Access Management	Least Privilege	Role-based access is defined and deployed to restrict privileged access to information resources based on the concept of least privilege.	Process	Preventive	Access Management Procedure	1. Design and document the process for assigning least privilege access. 2. Ensure access is granted as per required approvals.	1. Inspect logical access policy and validate that each role is assigned the correct level of access. 2. Inspect the logical access systems and review how the access levels are granted for types of roles (Developers, SWE, SRE). 3. For a sample of employees, inspect the level of access available and correlate to the job role and confirm that they are congruent.	E-IAM-01 E-IAM-41
IAM-30	Identity and Access Management	Virtual Private Network	Remote connections to the corporate network are accessed via VPN through managed gateways.	Technology	Preventive	Remote Access Procedure	1. Design and document process for requirements of remote connection to corporate network. 2. Ensure all remote connections are via VPN.	1. Inspect Remote Access Standard to determine whether requirements for remotely connecting to the corporate network were defined. 2. Inspect a user remotely connect to the Corporate Network via VPN.	E-IAM-19 E-IAM-43
IAM-31	Identity and Access Management	Virtual Private Network: Restrict Split-Tunneling	VPN configurations restrict split-tunneling capabilities.	Technology	Preventive	Remote Access Procedure	1. Ensure split tunneling is not enabled.	1. Inspect the VPN configurations and ensure that split tunneling is not enabled.	E-IAM-43
IAM-32	Identity and Access Management	Ability to Disable Remote Sessions	Organization has a defined process and mechanisms in place to expeditiously disable or disconnect remote access to information systems within a defined time frame based on business need.	Process	Preventive	Remote Access Procedure	1. Ensure that the server configuration for idle-session timeout is set to 15 minutes. 2. Ensure that access credentials expiry configuration is present. 3. Ensure remote connection tools such as (VPN or Management consoles) have session expirations enabled.	1. Inspect the server configuration showing that idle-session timeout is set to 15 minutes. 2. Validate that access credentials expiry configuration is present. 3. Inspect that remote connection tools such as (VPN or Management consoles) have session expirations enabled.	E-IAM-44 E-IAM-45 E-IAM-46
IAM-33	Identity and Access Management	Remote Maintenance: Authentication Sessions	Vendor accounts used for remote access are enabled only during the time period needed, disabled when not in use, and monitored while in use.	Technology	Preventive	Remote Access Procedure	1. Ensure that vendor accounts that are used for remote access, have the following configurations: -Enabled only for the time period needed -Disabled when not in use -Monitored when in use	1. Validate that vendor accounts that are used for remote access, have the following configurations: -Enabled only for the time period needed -Disabled when not in use -Monitored when in use	E-IAM-47
IAM-34	Identity and Access Management	Remote Maintenance: Unique Authentication Credentials for each Customer	Where applicable, Service providers with remote access to customer premises (e.g., for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.	Process	Preventive	Remote Access Procedure	1. Ensure that remote access to customer premises are using unique individual credentials, and that there is no shared administrative access.	1. Inspect that remote access to customer premises are using unique individual credentials, and that there is no shared administrative access.	E-IAM-48

IAM-35	Identity and Access Management	Remote Maintenance: Authentication	Remote maintenance and diagnostic tool utilization are restricted to the minimum required level, strong authentication is required, and remote sessions are recorded.	Technology	Preventive	Remote Access Procedure	1. Ensure remote maintenance and diagnostic tools have the following configurations: -Restricted to the minimum required level -Strong authentication -Remote sessions are recorded	1. Inspect remote maintenance and diagnostic tools and ensure that they have the following configurations: -Restricted to the minimum required level -Strong authentication -Remote sessions are recorded	E-IAM-47
IAM-36	Identity and Access Management	Remote Maintenance: Audit	Organization documents and maintains records for vendor remote maintenance, diagnostic activities, and permissions granted. A listing of vendor remote maintenance connections is documented as well.	Process	Preventive	Remote Access Procedure	1.Ensure vendor remote access is documented and that they include: -Maintenance activities -Diagnostic activities -Permissions granted 2. Ensure that there is no unauthorized access be vendor or third parties.	1. Inspect documents and records for vendor remote access. 2. Review the records and ensure that they include: -Maintenance activities -Diagnostic activities -Permissions granted 3. Review the list of vendor remote connections and ensure that there is no unauthorized access.	E-IAM-49
IAM-37	Identity and Access Management	End-user Environment Segmentation	Where applicable, processes that run as part of an Organization shared hosting platform will run under unique credentials that permit access to only one customer environment.	Technology	Preventive	Customer Authentication Standard	1. Where applicable, ensure that the platform will run under unique credentials that permit access to only one customer environment.	1. Inspect application processes and validate that, where applicable, the platform will run under unique credentials that are permitted to access only one customer environment.	E-IAM-50
IAM-38	Identity and Access Management	End-user Access to Applications and Data	Organization applications secure user data and maintain confidentiality by default or according to permissions set by the individual; Organization authenticates individuals with unique identifiers and passwords prior to enabling access to: • use the application • view or modify their own data	Technology	Preventive	Customer Authentication Standard	1. Ensure that individuals are given unique identifiers and passwords prior to enabling access. 2. Ensure that passwords used by the consumer are protected using proper encryption in transmission and storage.	1. Inspect the authentication method for consumers, and confirm that individuals are given unique identifiers and passwords prior to enabling access. 2. Ensure that passwords used by the consumer are protected using proper encryption in transmission and storage.	E-IAM-51 E-IAM-52 E-IAM-53
IAM-39	Identity and Access Management	Hardware Tokens	Where applicable, hardware token-based authentication is facilitated only by approved organizations.	Process	Preventive	Access Management Procedure	1. Design the process for hardware token-based authentication. 2. Ensure that the hardware tokens are assigned to the corresponding users.	1. Inspect the process by which hardware token-based authentication is distributed, used, and collected. 2. For a sample of users, inspect the inventory of the hardware tokens and ensure that they are assigned to the corresponding users.	E-IAM-54 E-IAM-55
IR-01	Incident Response	Incident Response Plan	Organization defines the types of incidents that need to be managed, tracked and reported, including: • procedures for the identification and management of incidents • procedures for the resolution of confirmed incidents • key incident response systems • incident coordination and communication strategy • contact method for internal parties to report incidents • support team contact information • notification to relevant management in the event of a security breach • provisions for updating and communicating the plan • provisions for training of support team • preservation of incident information • management review and approval, annually, or when major changes to the organization occur	Process	Preventive	Incident Management Policy	1. Prepare, document, and communicate the Incident Response Plan and Incident Management Policy and ensure that the following are documented: a. Procedures for the assignment of Roles and Responsibilities for the design implementation, maintenance and execution of the incident response plan b. Procedures for the identification and management of incidents c. Procedures for the resolution of confirmed incidents d. Procedures for the restoration of data and business operation e. Incident coordination and communication strategy f. Notification to relevant management in the event of a security breach g. Provisions for updating and communicating the plan h. Provisions for evaluating the effectiveness of incident response i. Post incident resolution including post mortem analysis and lessons learned 2. Ensure that a process exists to periodically review the changes which displays revision history of the Incident Response Plan.	1. Inspect the Incident Response Plan and Incident Management Policy to determine whether the following are documented: a. Procedures for the assignment of Roles and Responsibilities for the design implementation, maintenance and execution of the incident response plan b. Procedures for the identification and management of incidents c. Procedures for the resolution of confirmed incidents d. Procedures for the restoration of data and business operation e. Incident coordination and communication strategy f. Notification to relevant management in the event of a security breach g. Provisions for updating and communicating the plan h. Provisions for evaluating the effectiveness of incident response i. Post incident resolution including post mortem analysis and lessons learned 2. Review the changes which displays revision history of the Incident Response Plan.	E-IR-01 E-IR-02 E-IR-03
IR-02	Incident Response	Incident Response Testing	Organization tests incident response processes on an annual basis. Results from the tests are documented.	Process	Detective	Incident Management Policy	1. Ensure that a process exists to test the incident response process on an annual basis. 2. Ensure that Incident Response Standard is updated at least annually. 3. Establish a process for conducting the trainings such as table top exercise and ensure that all necessary personnel attended the training.	1. Validate with the Incident response team of the completion of the training and its documentation. 2. Validate that Incident Response Standard is updated at least annually. 3. Review elements of the training such as table top exercise and confirm that all necessary personnel attended the training.	E-IR-01 E-IR-04 E-IR-05

IR-03	Incident Response	Incident Response	Confirmed incidents are assigned a priority level and managed to resolution. If applicable, Organization coordinates the incident response with business contingency activities.	Process	Preventive	Incident Management Policy	1. Prepare, document, and communicate the Security Incident Management Policy within the organization. 2. Ensure that priority level are assigned to a sample of incidents and that they are tracked to resolution. 3. For any crisis declared incidents, validate that business contingency activities are performed.	1. Inspect the Organization Security Incident Management Policy. 2. Validate that priority level are assigned to a sample of incidents and ensure that they are tracked to resolution. 3. Validate that for any crisis declared incidents, that business contingency activities were performed.	E-IR-02 E-IR-06
IR-04	Incident Response	External Communication of Incidents	Organization defines external communication requirements for incidents, including: • information about external party dependencies • criteria for notification to external parties as required by Organization policy in the event of a security breach • contact information for authorities (e.g., law enforcement, regulatory bodies, etc.) • provisions for updating and communicating external communication requirement changes	Process	Preventive	Incident Management Policy	1. Ensure that following details are documented in Incident Response Plan and Standard: • information about external party dependencies • criteria for notification to external parties as required by policy in the event of a security breach • contact information for authorities (e.g., law enforcement, regulatory bodies, etc.) • provisions for updating and communicating external communication requirement changes 2. Establish a process that flags the alerts as the defined escalation metrics.	1. Inspect the Incident Response Plan and Standard to determine whether the following are documented: • information about external party dependencies • criteria for notification to external parties as required by policy in the event of a security breach • contact information for authorities (e.g., law enforcement, regulatory bodies, etc.) • provisions for updating and communicating external communication requirement changes 2. Review the procedure for alert escalation	E-IR-01 E-IR-02
IR-05	Incident Response	Incident Reporting Contact Information	Organization provides a contact method to: • submit complaints and inquiries • report incidents	Process	Preventive	Incident Management Policy	1. Define a communication channel on the company public website which shall include a contact method for external parties to submit complaints, inquiries, and report incidents.	1. Review public website to determine whether the company provides a contact method for external parties to submit complaints, inquiries, and report incidents.	E-IR-08
IR-06	Incident Response	Incident External Communication	Organization communicates a response to external stakeholders as required by the Incident Response Plan.	Process	Preventive	Incident Management Policy	1. Ensure that the Incident Response Plan and the Incident Legal Communications Requirements Standard include a process for communicating a response to external stakeholders is required. 2. Design a process to maintain the list of confirmed incidents which involved external stakeholders. 3. Establish a process which sends out communications to external stakeholders per the Incident Response Plan.	1. Inspect the Incident Response Plan and the Incident Legal Communications Requirements Standard to determine whether communicating a response to external stakeholders is required. 2. Obtain a list of confirmed incidents which involved external stakeholders. 3. Inspect a sample of confirmed incidents tickets to determine whether communications required a response to external stakeholders per the Incident Response Plan.	E-IR-01 E-IR-09 E-IR-06
IR-07	Incident Response	External Communication of Incidents: Protected Health Information	Organization communicates the discovery and status of the breach of Protected Health Information (PHI) to the covered entity within 60 days or as required by the Business Associates Agreement (BAA) and provides the following information if available: • description of the Event • description of the Information that was compromised • identification of the Individuals whose PHI were compromised • steps Required to Protect Individuals • investigation Plan • contact Information	Process	Preventive	Incident Management Policy	1. Design the process to validate whether an incident includes Personal Health information. 2. Ensure that all incidents where there has been a breach have been communicated to the covered entity within 60 days, or following the covered entity's Business Associates Agreement. 3. Ensure that within the communication all the listed information was provided to the covered entity: • description of the Event • description of the Information that was Compromised • identification of the Individuals whose PHI were Compromised • steps Required to Protect Individuals • investigation Plan • contact Information	1. Validate all incidents have included Personal Health information. 2. Inspect whether all the incidents where there has been a breach have been communicated to the covered entity within 60 days, or following the covered entity's Business Associates Agreement. 3. Validate whether the communication was sent to the covered entity and included all the listed information: • description of the Event • description of the Information that was Compromised • identification of the Individuals whose PHI were Compromised • steps Required to Protect Individuals • investigation Plan • contact Information	E-IR-10 E-IR-11
IR-08	Incident Response	Problem Management	Organization resolves customer support inquiries.	Process	Corrective	Incident Management Policy	1. Establish a process to support customer inquires and ensure that they have been resolved and documented.	1. Review a sample of customer support inquires and ensure that they have been resolved.	E-IR-12
MDM-01	Mobile Device Management	Mobile Device Enrollment	Mobile devices (i.e., laptops, smartphones, tablets) must be configured with the appropriate Mobile Device Management (MDM) profile when used as a medium to access Organization internal resources.	Process	Preventive	Mobile Device Policy	1. Ensure that a Mobile device management process is defined and documented. 2. Ensure that all mobile devices are registered and configured within the appropriate Mobile Device Management (MDM) to access the internal resources.	1. Inspect the Mobile device Policy to ensure that a Mobile Device management process is defined. 2. Inspect the list of mobile devices to verify that the devices are registered within the Mobile Device Management (MDM) tool. 3. For a sample of devices, validate that the devices are configured with the MDM tool and that it cannot be disabled from the end user device.	E-MDM-01 E-MDM-02 E-MDM-03.

MDM-02	Mobile Device Management	Mobile Device Encryption	Mobile devices (i.e., laptops, smartphones, tablets) that are used to access data from Organization internal resources are encrypted.	Process	Preventive	Mobile Device Policy	1. Ensure that mobile devices are encrypted and is configured with the Mobile Device Management (MDM) tool.	1. Review the Mobile Device Management (MDM) tool and ensure that a device encryption tool is enabled for all registered devices. 2. Review a sample of mobile devices and verify that device encryption tools are enabled on devices and cannot be disabled by the end user.	E-MDM-02 E-MDM-04
MDM-03	Mobile Device Management	Configuration Management: Mobile Devices	Organization Mobile devices (i.e., laptops, smartphones, tablets) are configured to ensure unnecessary hardware capabilities and functionalities are disabled, and management defined security features are enabled.	Technology	Preventive	Mobile Device Policy	1. Ensure that mobile devices are configured to ensure unnecessary hardware capabilities and functionalities are disabled. 2. Ensure security features defined by the management shall be enabled within the MDM tool.	1. Review the Mobile Device Management (MDM) tool and confirm that there is a policy implemented that restricts the use of unnecessary hardware capabilities and functionalities are disabled. 2. For a sample of mobile devices, verify security features are enabled in the MDM tool. 3 Review a sample of user devices and verify that the end user cannot use hardware capabilities and functionalities that have been disabled by the MDM tool per its policy and that these functionalities are not able to be re-activated by the end user.	E-MDM-02 E-MDM-05
MDM-04	Mobile Device Management	Configuration Management: High Risk Travel Locations	Organization has a documented list of travel locations considered high risk for the use of mobile devices (i.e., laptops, smartphones, tablets). Employees procure alternate equipment before traveling to these locations.	Process	Preventive	Mobile Device Policy	1. Ensure that a process is defined and documented for handling travel to high-risk locations. 2. Ensure that a documented list of travel locations considered to be high risk for the use of mobile devices is maintained. 3. Ensure alternate equipment is provided to employees before traveling to these locations.	1. Inspect and validate that a process is defined and documented for handling travel to high-risk locations. 2. Validate the list of travel locations considered to be high risk for the use of mobile devices 3. Validate the process for providing alternate equipment to employees before traveling to these locations.	E-MDM-06 E-MDM-03
NO-01	Network Operations	Network Policy Enforcement Points	Network traffic to and from untrusted networks passes through a policy enforcement point; firewall rules are established in accordance with identified security requirements and business justifications.	Technology	Preventive	Network Security Standard	1. Ensure that necessary process and documentation are established for network traffic management. 2. Ensure necessary requirements are defined for managing network traffic to and from untrusted networks in the policy. 3. Ensure firewall rules are established to determine specific configuration requirements have been documented for network devices within the policy.	1. Inspect Network Security Policy and/or Standard to determine whether requirements have been defined for managing network traffic to and from untrusted networks. 2. Review firewall rules to ensure they are defined according to the requirements of the organization.	E-NO-01 E-NO-02
NO-02	Network Operations	Inbound and Outbound Network Traffic: DMZ Requirements	Network traffic to and from untrusted networks passes through a Demilitarized Zone (DMZ).	Technology	Preventive	Network Security Standard	1. Ensure necessary requirements are defined which outlines the use of a DMZ and firewalls must be used wherever necessary to enforce perimeter security between separate networks in the policy. 2. Ensure DMZ is enabled and configured within the network traffic.	1. Inspect Network Security Policy and/or Standard documents to determine whether requirements have been defined that outlines the use of a DMZ and firewalls must be used wherever necessary to enforce perimeter security between separate networks. 2. Observe a sample of network security rules or firewall rulesets and confirm that the DMZ or DMZ equivalents are operating in the rulesets.	E-NO-01 E-NO-03
NO-03	Network Operations	Ingress and Egress Points	Organization maintains an inventory of ingress and egress points on the production network and performs the following for each: • inventory is reduced to the minimum possible level • permitted ports, protocols and services are inventoried and validated • documents security features that are implemented for insecure protocols	Process	Preventive	Network Security Standard	1. Ensure a process is maintained for inventory of ingress and egress points on the production network 2. Ensure network security rules are defined and established with the following: • permitted ports, protocols and services are inventoried and validated • documented security features that are implemented for insecure protocols	1. Observe the inventory of ingress and egress points on the production network. 2. Observe network security rules and validate to ensure no insecure ports, protocols, and services are present. 3. If applicable, for any insecure ports, protocols, and services, ensure that additional security features are in place.	E-NO-04 E-NO-05
NO-04	Network Operations	Non-disclosure of Routing Information	Organization does not disclose private IP addresses and routing information to unauthorized parties.	Technology	Preventive	Network Security Standard	1. Ensure necessary requirements are defined that prohibits the disclosure of private IP addresses and routing information to unauthorized parties in the policy.	1. Inspect Network Security Policy and/or Standard documents to determine whether requirements have been defined that prohibits the disclosure of private IP addresses and routing information to unauthorized parties. 2. Review the configuration to determine the non-disclosure of private IP Addresses and Network Address Translation.	E-NO-01 E-NO-07

NO-05	Network Operations	Dynamic Packet Filtering	Where applicable, Organization enables dynamic packet filtering on the network.	Technology	Preventive	Network Security Standard	1. Ensure that Network Security Policy/Standard specifies when to use dynamic packet filtering on the network. 2.Ensure dynamic packet filtering is turned on applicable systems.	1. Inspect Network Security Policy and/or Standard documents to determine whether requirements have been defined that outlines that dynamic packet filtering on the network should be enabled when applicable. 2. For a sample of applicable systems review the configurations for the devices and ensure that dynamic packet filtering has been enabled.	E-NO-01 E-NO-06
NO-06	Network Operations	Firewall Rule Set Review	Network infrastructure rule sets are reviewed every 6 months.	Process	Detective	Network Security Standard	1. Ensure that a process is defined and documented for performing Network Infrastructure rules every six months. 2. Ensure network infrastructure rules are reviewed and appropriate documentation is maintained for this review.	1 Observe the Network infrastructure rules review documentation and verify that it was last reviewed within the last 6 months.	E-NO-08
NO-07	Network Operations	Ingress and Egress Points: Fail Secure	The information system fails securely in the event of an operational failure of a boundary protection device.	Technology	Preventive	Network Security Standard	1. Ensure that appropriate fail safe procedures are defined for network boundary protection devices. 2. Ensure all network systems are configured to fail securely in the event of an operational failure.	1. Inspect Network Security Policy/Standard to determine whether requirements have been defined that outlines that in the event of an operation failure that information systems fail securely. 2. For a sample of applicable systems review the configurations for the devices and confirm that in the event of failure that the systems will fail securely.	E-NO-01 E-NO-09
NO-08	Network Operations	Traffic Flow: Managed Proxy	Organization requires egress traffic initiated from within the Organization network to pass through a managed proxy.	Technology	Preventive	Network Security Standard	1. Ensure that a process is defined and documented so that all egress traffic from within the organization passes through a proxy. 2.Ensure that proxy servers have been deployed on application systems for the filtering of traffic.	1. Inspect documentation to determine whether requirements have been defined that outlines that all egress traffic initiated from within the Organization's network passes through a managed proxy. 2. For a sample of applicable systems review the architecture and ensure that all egress traffic from within the network is passed through the managed proxy.	E-NO-01 E-NO-10
NO-09	Network Operations	Domain Name Services Security Extensions (DNSSec)	Organization establishes a DNSSec implementation standard and uses mechanisms to verify the DNS infrastructure for compliance.	Process	Preventive	Network Security Standard	1. Ensure that a process is defined and documented for a DNSSec implementation. 2. Ensure appropriate mechanism are in place to validate DNS infrastructure for compliance.	1. Inspect documentation to determine whether requirements have been defined that outlines a DNSSec implementation. 2. Review a sample of DNS infrastructure used and ensure that they are following the DNSSec implementation requirements.	E-NO-01 E-NO-11
NO-10	Network Operations	Email Spam Protection	Organization has documented procedures and protection mechanisms in place to protect its information and information systems from spam and ensures that signature definitions are updated whenever new releases are available.	Process	Preventive	Network Security Standard	1. Ensure that a process is defined and documented to ensure spam protection on emails. 2. Ensure that appropriate controls are deployed to prevent spam from emails. 3. Ensure that spam signature definitions are updated when new releases are available.	1. Inspect the documentation to ensure a process is defined for spam protection. 2. For a sample of applicable systems such as mail servers ensure that anti-spam filters are enabled and are updated to the most recent version possible.	E-NO-01 E-NO-12
NO-11	Network Operations	Denial of Service (DOS)	Organization implements a Denial of Service (DOS) protection plan, identifies threatening DOS attacks, and configures boundary protection devices according to the DOS plan.	Process	Preventive	Network Security Standard	1. Ensure a process is defined and documented to prevent from Denial of Service (DoS) attacks. 2. Ensure that boundary protection devices are configured as per the process to enable Denial of Service Attack Protection.	1. Inspect documentation to determine whether requirements have been defined that outlines that a Denial of Service (DoS) protection plan. 2. For a sample of applicable system ensure that configuration aligns with the Denial of Service Protection Plan.	E-NO-01 E-NO-23
NO-12	Network Operations	Trusted Connections	All trusted connections are documented and approved by authorized personnel; management ensures the following documentation is in place prior to approval: • agreement with vendor • security requirements • nature of transmitted information	Process	Preventive	Network Security Standard	1. Ensure that a process is defined and documented for managing trusted connections. 2. Ensure that all trusted connections are documented and approved by authorized personnel. 3. Ensure that appropriate agreements with vendors exist before establishing trusted connection.	1. Inspect and validate whether a process is defined and documented for managing trusted connections. 2. Validate for a sample trusted connections that it was documented and approved by authorized personnel. 3. Validate whether appropriate agreement with vendors existed before establishing trusted connection.	E-NO-01 E-NO-13

NO-13	Network Operations	Network Segmentation	Production environments are logically segregated from non-production environments.	Technology	Preventive	Network Security Standard	1. Ensure that a process is defined and documented to ensure that production and non-production environments are logically segregated. 2. Ensure that for all systems production and non-production environments are logically segregated and this is reflected via appropriate architecture diagrams.	1. Inspect and validate whether a process is defined and documented to ensure that production and non-production environments are logically segregated. 2. Validate for a sample system whether production and non-production environments are logically segregated.	E-NO-14 E-NO-16
NO-14	Network Operations	Card Processing Environment Segmentation	Where applicable, Organization segregates the Primary Account Number (PAN) infrastructure including payment card collection devices; Organization limits access to the segregated environment to authorized personnel.	Process	Preventive	Network Security Standard	1. Ensure that a process is defined and documented for segregating PCI Environment from non-PCI environment. 2. Ensure that network segmentation testing is performed on a semi-annual basis. 3. Ensure that the Data flow and architecture diagram is updated periodically and reviewed by required officials.	1. Inspect and validate whether a process is defined and documented for segregating PCI Environment from non-PCI environment. 2. Validate whether network segmentation testing was performed on a semi annual basis. 3. Validate whether the Data flow and architecture diagram were updated periodically and were approved.	E-NO-01 E-NO-15 E-NO-17 E-NO-14
NO-15	Network Operations	Traffic Flow	Organization documents the approved traffic flow at each managed interface and configures the managed interface accordingly. Exceptions to traffic flow are documented, reviewed periodically, and removed when there is no longer a business requirement.	Process	Preventive	Network Security Standard	1. Ensure a process is defined and documented for managing traffic flow at each interface. 2. Ensure all managed interfaces are configured as per the approved traffic flow. 3. Ensure all exceptions are documented, reviewed periodically, and removed when there is no longer a business requirement.	1. Inspect and validate whether a process is defined and documented for managing traffic flow at each interface. 2. Validate for a sample of managed interface that it is configured as per the approved traffic flow. 3. Validate for a sample of exceptions whether they were documented, reviewed periodically, and removed when there was no longer a business requirement.	E-NO-01 E-NO-18 E-SG-04
NO-16	Network Operations	Disable Rogue Wireless Access Points	Organization employs mechanisms to detect and disable the use of unauthorized wireless access points.	Technology	Detective	Network Security Standard	1. Ensure a process is defined and documented to detect unauthorized wireless access points. 2. Ensure network monitoring software is in place to identify unauthorized wireless access points send alerts to the appropriate personnel. 3. Ensure that alerts are regularly reviewed, and if necessary, actions are taken to fix any issues.	1. Inspect and validate that a process is defined and documented to detect unauthorized wireless access points. 2. Validate the configuration of network monitoring software to check if it detects unauthorized wireless access points send alerts to the appropriate personnel. 3. Validate sample alerts and inspect whether they were reviewed, and if necessary, actions were taken to fix any issues.	E-NO-01 E-NO-19 E-NO-20
NO-17	Network Operations	Wireless Access Points	Organization maintains an inventory of authorized wireless access points including a documented business justification.	Process	Preventive	Network Security Standard	1. Ensure that a formal inventory of authorized wireless access points is documented which includes information of the function of the wireless point and its business justification.	1. Inspect and validate that an inventory of authorized wireless points is maintained. 2. Validate that the inventory contains the business need and the function of each wireless access point	E-NO-01 E-NO-21
NO-18	Network Operations	Authentication: Wireless Access Points	Organization restricts access to network services via wireless access points to authenticated users and services; approved wireless encryption protocols are required for wireless connections.	Technology	Preventive	Network Security Standard	1. Ensure that a process is defined and documented to restrict access to network services via wireless access points to authenticated users and services 2. Ensure Approved wireless encryption protocols are required for wireless connections.	1. Inspect and validate that a process is defined and documented to restrict access to network services via wireless access points to authenticated users and services 2. Validate whether approved wireless encryption protocols are required for wireless connections.	E-NO-01 E-NO-22
PR-01	People Resources	Background Checks	New hires are required to pass a background check as a condition of their employment.	Process	Preventive	Human Resource Policy	1. Ensure that a process is defined and documented to conduct background checks for new hires. 2. Ensure that a background check is completed prior to the hire date for all new hires.	1. Inspect documentation to validate whether requirements for background checks have been defined. 2 For a sample of new hires, validate that background checks defined in the policy were performed prior to their hire date.	E-PR-01 E-PR-02
PR-02	People Resources	Performance Management	Organization has established a check-in performance management process for on-going dialogue between managers and employees. Quarterly reminders are sent to managers to perform their regular check-in conversation.	Process	Preventive	Human Resource Policy	1. Document and maintain a check-in performance management process for on-going dialogue between managers and employees. 2. Ensure reminders are sent to managers on a quarterly basis for performing regular check-in.	1. Inspect relevant documentation to validate whether a process regarding check-in performance management has been defined. 2. For a sample of quarters, inspect the mail communication to determine whether quarterly reminders are sent to managers to perform their regular check-in conversation.	E-PR-01 E-PR-03

PR-03	People Resources	Hiring Process	Job candidates apply for roles that are listed on the Organization career portal; candidates are interviewed to determine their knowledge and competence for their prospective roles and compatibility with Organization values.	Process	Preventive	Human Resource Policy	1. Ensure that a process is defined and documented that outlines the requirements for hiring of employees. 2. Ensure all job roles are posted on career portal for application. 3. Ensure appropriate hiring process is followed to determine competence before hiring.	1. Inspect and validate that a process is defined and documented that outlines the requirements for hiring of employees. 2. Validate sample job roles and check if they are posted on career portal for application. 3. For sample employees validate the hiring process followed and evaluate whether it was according to the policy.	E-PR-01 E-PR-04 E-PR-05
PR-04	People Resources	Organization Property Collection	Upon employee termination, management is notified to collect Organization property from the terminated employee.	Process	Preventive	Human Resource Policy	1. Ensure a process is defined and documented to notify the management in case of employee termination and collect organization property. 2. Ensure termination procedures are followed to collect organization property from the employee.	1. Inspect the relevant documentation to determine whether a process is defined and documented to notify the management in case of employee termination and collect organization property. 2. For a sample of terminated employees, validate that termination procedures were followed to collect organization property.	E-PR-01 E-PR-06
PR-05	People Resources	Exit Interviews	Upon employee termination, management conducts exit interviews for the terminated employee.	Process	Preventive	Human Resource Policy	1. Ensure a process is defined and documented to notify the management in case of employee termination and conduct exit interviews 2. Ensure exit interviews are conducted once a user is terminated in HR Management System and relevant stakeholders are involved. 3. Ensure that a record of the interview is retained.	1. Inspect the relevant documentation to determine whether a process is defined and documented to notify the management in case of employee termination and conduct exit interviews 2. Inspect records of the exit interview for terminated employees. 3. For a sample of terminated employees, validate that termination procedures were followed including the performance of an exit interview.	E-PR-01 E-PR-07
PR-06	People Resources	Disciplinary Process	Employees that fail to comply with Organization policies are subject to a disciplinary process.	Process	Corrective	Human Resource Policy	1. Ensure that a disciplinary process is defined and documented and is appropriately communicated. 2. Ensure that the disciplinary process is followed for all employees violating organizational policies.	1. Inspect relevant documentation to validate that a disciplinary process is defined and appropriately communicated. 2. Validate that disciplinary process was followed for all employees violating organizational policies.	E-PR-01 E-PR-08
PR-07	People Resources	Code of Ethics	Organization has a Code of Ethics for Senior Officers. The Senior Officers and CEO certify that they understand the Code on an annual basis.	Process	Preventive	Human Resource Policy	1. Ensure that a Code of Ethics has been established for senior officers and the CEO. 2. Ensure all senior officers and CEO have documented certification of Code of Ethics on an annual basis.	1. Inspect and validate that a Code of ethics is defined and documented for senior officers and CEO. 2. Validate that all senior officers and CEO have documented certification of code of ethics at least annually.	E-PR-09 E-PR-10
PR-08	People Resources	Business Ethics Hotline	Organization has a business ethics hotline for employees and external parties to report ethical misconduct. Allegations are investigated and Organization will take appropriate action for confirmed violations. Hotline reports are reported to the Audit Committee on a quarterly basis.	Process	Preventive	Human Resource Policy	1. Ensure that a process has been defined and documented for reporting ethical misconduct. 2. Ensure that allegations made through the hotline are investigated and appropriate action is taken. 3. Ensure Hotline reports are reported to the Audit Committee on a quarterly basis.	1. Inspect the relevant documentation to validate that a process has been defined and documented for reporting ethical misconduct. 2. Validate that the allegations made through the hotline are investigated and appropriate action is taken for a sample of reports. 3. Validate whether the hotline reports are reported to the Audit Committee on a quarterly basis.	E-PR-01 E-PR-11 E-PR-12

PR-09	People Resources	National Security Clearance	Organization conducts screening and rescreening of authorized personnel for roles that require national security clearances. For national security clearances; a reinvestigation is required during the 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance. In addition, for law enforcement and high impact public trust level, a reinvestigation is required during the 5th year.	Process	Preventive	Human Resource Policy	1. Document and maintain a process on screening/rescreening or vetting of employees that need national security clearances. 2. Ensure list of roles requiring national security clearances is reviewed and kept up-to-date. 3. Ensure that screening and rescreening of authorized personnel are conducted for roles that require national security clearances. 4. For national security clearances, ensure that rescreening is conducted for the following: • 5th year for top secret security clearance • 10th year for secret security clearance • 15th year for confidential security clearance 5. For law enforcement an high impact public trust level, ensure that an	1. Inspect relevant documentation and validate that a process on screening/rescreening or vetting of employees that need national security clearances is established. 2. Validate whether a list of roles requiring national security clearances is reviewed and kept up-to-date. 3. Validate for a sample employee requiring National Security Clearance that screening and rescreening was conducted. 4. For sample national security clearances, validate that rescreening was conducted for the following: • 5th year for top secret security clearance • 10th year for secret security clearance • 15th year for confidential security clearance	E-PR-13 E-PR-14 E-PR-15 E-PR-16
PR-10	People Resources	Code of Business Conduct	Organization has documented the Code of Business Conduct and Business Partner Code of Conduct, which are reviewed, updated if applicable, and approved by senior management annually.	Process	Preventive	Human Resource Policy	1. Ensure that a Code of Business Conduct and Business Partner Code of Conduct is defined, documented, and approved by senior management. 2. Ensure that these documents are reviewed, updated, and approved at least on an annual basis.	1. Inspect and validate that a Code of Business Conduct and Business Partner Code of Conduct is defined, documented, and approved by senior management. 2. Validate that these documents are reviewed, updated, and approved at least on an annual basis.	E-PR-17 E-PR-18
PRIV-01	Privacy	Privacy Program	Organization privacy policies for individuals, including relevant updates, are communicated on the public company website or on the internal corporate network.	Process	Preventive	Privacy Policy	1. Ensure the organization has created a privacy policy. 2. Ensure the policy is updated and approved on regular intervals. 3. Ensure the policy is communicated and is available for employees and relevant stakeholders.	1. Inspect privacy policies and confirm that the policy is updated. 2. Confirm that anytime the privacy policy is updated, these updates are present on the intranet or public website.	E-PRIV-01
PRIV-02	Privacy	Privacy Program Review	On an annual basis, Organization performs a review of privacy practices to ensure the following: • consent is obtained for users whose personal information (PI) is managed by Organization • PI inventory integrity and accuracy • data access request response template is understandable • standard agreement templates are up-to-date • requests to delete, access or update PI are processed accurately and within a timeframe consistent with Organization policy • compliance with Organization's privacy commitments • known privacy issues are remediated • opt-in and opt-out compliance with applicable law • Organization privacy documentation and practices are relevant to applicable law • compliance with relevant industry Codes of Conduct (e.g., EDAA) • if applicable, joint controller responsibilities are clearly defined and communicated to both data controllers and the data subject	Process	Preventive	Privacy Policy	1. Ensure that the organization has established a privacy program. 2. Ensure that the program is reviewed on at least an annual basis. 3. Ensure that the privacy program contains controls regarding consent, data access requests, modification requests, SLAs, privacy issues, roles and responsibilities. 4. Ensure that agreement templates are reviewed and updated.	1. Collect and inspect the organization's annual privacy review. 2. Validated that the annual privacy review covers all components.	E-PRIV-02

PRIV-03	Privacy	Privacy Readiness Review	Organization performs privacy readiness reviews to identify high-risk processing activities that impact personal data; identified non-compliance with Organization privacy practices is tracked through remediation.	Process	Corrective	Privacy Policy	1. Ensure that a process has been established for privacy readiness reviews. 2. Ensure privacy readiness reviews are conducted for high-risk processing activities. 3. Ensure necessary actions are taken for the remediation of findings from privacy readiness reviews.	1. Inspect privacy readiness reviews and ensure that remediation activities were launched for any non-compliant actions. 2. Validate that remediation activates were resolved and remediated.	E-PRIV-03
PRIV-04	Privacy	Privacy Notice	Individuals are given appropriate notice and an opportunity to consent or decline to Organization privacy practices such as accessing, collecting, processing, transferring, or storing personal information.	Process	Preventive	Data Management Policy	1. Ensure that a consent notice is established for users regarding privacy guidelines. 2. Ensure that the users have an option to accept or decline the consent.	1. Inspect Data Protection Policy and procedure documents to ensure individuals are given appropriate notice and an opportunity to consent or decline to organization privacy practices such as accessing, collecting, processing, transferring, or storing personal information.	E-PRIV-04
PRIV-05	Privacy	Personal Information Notice and Consent: Additional Processing Activities	Where appropriate, Organization obtains individual consent for processing activities for which consent has not been previously obtained.	Process	Preventive	Data Management Policy	1. Ensure that consent is obtained for processing user data. 2. Ensure that any change in processing activities is followed by an update of consent.	1. Inspect Data Protection Policy and procedure documents to determine whether organization obtains individual consent for processing activities for which consent has not been previously obtained.	E-PRIV-04
PRIV-06	Privacy	Notice of Personal Information Disclosure	In accordance with Organization policy, Organization provides notice to individuals regarding legally-required disclosures of personal information.	Process	Detective	Data Management Policy	1. Ensure that a process is established for disclosing user data in case of legal enquiries. 2. Ensure appropriate notice is provided to the users regarding disclosure of their data.	1. Inspect Organization policy related to disclosure of personal information to determine whether process of providing notice to individuals regarding legally required disclosures of personal information is documented.	E-PRIV-05
PRIV-07	Privacy	PII Processing Agreements	Personal information is handled and processed in accordance with contractual requirements.	Process	Preventive	Privacy Policy	1. Ensure that appropriate agreements are established to define PII processing requirements. 2. Ensure all customers sign PII processing agreements. 3. Ensure all PII is handled and processed as per contractual requirements.	1. Inspect and validate that appropriate agreements are established and documented that define PII processing requirements. 2. For a sample customer validate that PII processing agreement has been signed. 3. Validate that all PII is handled and processed as per contractual requirements and the employees are briefed of these requirements.	E-PRIV-06 E-PRIV-07
PRIV-08	Privacy	Record of Processing Activity	Organization documents, reviews, and approves a record of processing activities related to personal information.	Process	Preventive	Privacy Policy	1. Ensure appropriate process has been established to document and record all processing activities related to Personal Information. 2. Ensure the records of PII processing activities are reviewed periodically as per contractual requirements. 3. Ensure that the record is approved by appropriate personnel.	1. Inspect a sample of reviews related to processing of personal information and validate that it is approved by the authorized personnel.	E-PRIV-08
PRIV-09	Privacy	Document Management Standard: HIPAA	Documentation that impacts personal health information, including policies, procedures, and the documentation of actions, activities, or assessments, are retained for 6 years from the date of its creation, or the date when it last was in effect, whichever is later.	Process	Preventive	Privacy Policy	1. Ensure that a process is defined and documented for retaining documentation related to personal health information. 2. Ensure that this documentation is retained at least for 6 years from the date of creation or when it was last effective. 3. Ensure this documentation consists of polices and procedures of actions, activities and/or assessments.	1. Validate documented retention configuration is set to at least 6 years for policies, procedures, and assessment for the documents that impacts personal health information. 2. Inspect a sample of documentation going back to the earliest document or at least 6 years.	E-PRIV-09

PRIV-10	Privacy	Law Enforcement Requests	Law enforcement agencies may submit requests for evidence; submitted requests are reviewed and tracked to resolution.	Process	Preventive	Incident Management Policy	1. Ensure a process is defined, documented, and approved for law enforcement agencies to submit evidence requests for investigation. 2. Ensure these requests are appropriately tracked and resolved as per contractual and legal requirements. 3. Ensure any evidence sharing is done via secure methods to avoid unauthorized access to data. 4. Ensure only customer data relevant to the investigation is segregated and submitted if needed.	1. Inspect and validate that a process is defined, documented, and approved for law enforcement agencies to submit evidence requests for investigation. 2. Validate for a sample of requests that they are appropriately tracked and resolved as per contractual and legal requirements. 3. Validate for a sample request whether the evidence sharing was done via secure methods to avoid unauthorized access to data. 4. Validate how customer data relevant to the investigation was segregated and submitted.	E-PRIV-10 E-PRIV-11 E-PRIV-12
PS-01	Proactive Security	Endpoint Detection and Response	Endpoint Detection and Response (EDR) software is deployed to continuously monitor, detect, and respond to cyber threats and patterns of malicious behavior and activity.	Technology	Preventive	Network Security Standard	1. Deploy Endpoint Detection and Response (EDR) software to continuously monitor, detect, and respond to cyber threats and patterns of malicious behavior and activity. 2. Ensure that the EDR configurations are periodically reviewed.	1. For a sample of endpoints, validate whether Endpoint Detection and Response (EDR) software is installed and continuously monitor, detect, and respond to cyber threats and patterns of malicious behavior and activity. 2. Inspect whether the EDR configurations are reviewed periodically.	E-NO-01 E-PS-01
PS-02	Proactive Security	Threat Hunting	Organization performs threat hunting to identify, track, and disrupt threats that evade existing security controls.	Process	Preventive	Incident Management Policy	1. Conduct cyber threat hunting activities according to an organization-defined frequency and/or organization-defined event to detect, track, and disrupt threats that evade existing controls. 2. Establish a threat hunting methodology in accordance with the organization's security objectives. 3. Define threat indicator information and effective mitigations.	1. Inspect whether cyber threat hunting activities are performed as per defined frequency to detect, track, and disrupt threats that evade existing controls. 2. Validate whether a threat hunting methodology exists in accordance with the organization's security objectives. 3. Inspect the threat indicator information and effective mitigations.	E-PS-02 E-PS-03
PS-03	Proactive Security	Threat Modeling	Organization performs periodic threat modeling to ensure that potential threats are identified and assessed.	Process	Preventive	System Architecture and Design Documentation Standard	1. Ensure that an organization performs periodic threat modeling to ensure that potential threats are identified and assessed.	1. Validate whether an organization performs threat modeling periodically to identify and assess potential threats.	E-PS-04
PS-04	Proactive Security	Adversary Intelligence	Organization gathers intelligence on adversary personas to assist in the prioritization of security activities.	Process	Preventive	Incident Management Policy	1. Establish a process through which an organization gathers intelligence on adversary personas to assist in the prioritization of security activities.	1. Validate whether a process exists through which an organization gathers intelligence on adversary personas to assist in the prioritization of security activities.	E-PS-05
RM-01	Risk Management	Service Risk Rating Assignment	Annually, Organization prioritizes the frequency of vulnerability discovery activities based on an assigned service risk rating.	Process	Detective	Risk Management Standard	1. Ensure Risk management standard is in place and documented which defines the frequency of vulnerability discovery activities based on an assigned service risk rating. 2. Ensure all the identified vulnerabilities are remediated based on the risk rating.	1. Validate that the organization has a defined vulnerability management standard. 2. For a sample of vulnerabilities, test that it was remediated based on risk ranking.	E-RM-01 E-RM-02
RM-02	Risk Management	Risk Assessment	Organization management performs an annual risk assessment. Results from risk assessment activities are reviewed to prioritize mitigation of identified risks.	Process	Detective	Risk Management Standard	1. Ensure Risk Management Standard shall be in place which RM-01 defines the requirements for annual risk assessment. 2. Ensure that the results of risk assessment are reviewed and mitigation is performed on priority. 3. Any identified issues should have a corresponding risk treatment plan or corrective action plan in place. Each issue shall be tracked to completion.	1. Validate that Risk Management Standard is in place and defines the requirements for annual risk assessment. 2. Validate evidence for the review of results of risk assessment and mitigation of risks. 3. Validate that any identified issues were tracked to completion, according to its corresponding risk treatment plan or corrective action plan.	E-RM-03 E-RM-04 E-RM-05

RM-03	Risk Management	Risk Assessment: HIPAA Criteria	Organization's periodic risk assessment for systems that process, transmit or store Protected Health Information (PHI) includes the following: • identify and classify assets • identify threats • identify vulnerabilities • identify controls • perform threat likelihood analysis • perform threat impact analysis • identify residual risk • identify appropriate safeguards	Process	Detective	Risk Management Standard	1. Ensure risk assessment for systems that process, transmit or store Protected Health Information (PHI) shall be in place and includes the information listed below: • identify and classify assets • identify threats • identify vulnerabilities • identify controls • perform threat likelihood analysis • perform threat impact analysis • identify residual risk • identify appropriate safeguards	1. Review Risk Assessment for a sample system that process, transmit or store Protected Health Information (PHI) and validate whether it includes the following: • identify and classify assets • identify threats • identify vulnerabilities • identify controls • perform threat likelihood analysis • perform threat impact analysis • identify residual risk • identify appropriate safeguards	E-RM-06
RM-04	Risk Management	Continuous Monitoring	The design and operating effectiveness of internal controls are continuously evaluated against the established Common Controls Framework by Organization. Corrective actions related to identified deficiencies are tracked to resolution.	Process	Detective	Risk Management Standard	1. Ensure that a process is defined and documented for the continuous monitoring of internal controls against the common controls framework. 2. Ensure any gaps identified are remediated as per the organization's policy.	1. Validate that a process is defined and documented for the continuous monitoring of internal controls against the common controls framework. 2. For sample gaps validate that they were remediated as per the organization's policy.	E-RM-07 E-RM-08
RM-05	Risk Management	Self-Assessments: PCI	On a quarterly basis, reviews shall be performed with approved documented specification to confirm personnel are following security policies and operational procedures pertaining to: • daily log reviews • firewall rule-set reviews • applying configuration standards to new systems • responding to security alerts • change management processes	Process	Preventive	Risk Management Standard	1. Establish a quarterly process to ensure that the following policies and operational procedures are being reviewed and approved by authorized personnel: • daily log reviews • firewall rule-set reviews • applying configuration standards to new systems • responding to security alerts • change management processes	1. Inspect whether a process exists for reviewing the following on a quarterly basis: • daily log reviews • firewall rule-set reviews • applying configuration standards to new systems • responding to security alerts • change management processes 2. Validate using the last review whether any deviations were noted and if applicable, were tracked till resolution	E-RM-03 E-RM-09
RM-06	Risk Management	Internal Audits	Organization establishes internal audit requirements based on the Common Controls Framework by Organization and executes audits on information systems and processes at planned intervals.	Process	Detective	Risk Management Standard	1. Ensure that the organization sets audit rules based on its Common Controls Framework and conducts audits on its information systems and processes at scheduled times	1. Inspect internal and external audit results.	E-RM-10 E-RM-11
RM-07	Risk Management	ISMS Internal Audit Requirements	Internal audit establishes and executes a plan to evaluate applicable controls in the Information Security Management System (ISMS) at least once every 3 years.	Process	Detective	Risk Management Standard	1. Ensure that the organization possesses an audit program document that enumerates the particular controls slated for testing within its Information Security Management System (ISMS). 2. Ensure that the outcomes of internal audit for ISMS controls is reviewed on a periodic basis.	1. Inspect audit program document that lists out specific controls to be tested in the ISMS. 2. Inspect the results of internal audit of ISMS controls and note the cadence of such audits.	E-RM-12 E-RM-13 E-RM-11
RM-08	Risk Management	Remediation Tracking	Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Process	Corrective	Risk Management Standard	1. Ensure that there is a well-defined and documented remediation plan in place to address and resolve any findings from risk assessment activities. 2. Ensure that the findings identified are resolved within the agreed timeframe.	1. Inspect documentation of remediation plan for any risk assessment activities. 2. Validate whether the findings created are remediated in the defined timeframe.	E-RM-14 E-RM-03 E-RM-15
RM-09	Risk Management	ISMS Corrective Action Plans	Management prepares a Corrective Action Plan (CAP) to manage the resolution of nonconformities identified in independent audits.	Process	Corrective	Risk Management Standard	1. Ensure that there is an audit finding document generated following an external, independent audit and used as a basis for implementing necessary improvements and corrective actions.	1. Inspect audit finding document prepared after external, independent audit. 2. For a sample of findings, examine evidence of resolution or a plan of action for audit findings.	E-RM-15 E-RM-16

RM-10	Risk Management	Statement of Applicability	Management prepares a statement of applicability that includes control objectives, implemented controls, and business justification for excluded controls. Management aligns the statement of applicability with the results of the annual risk assessment.	Process	Preventive	Risk Management Standard	1. Ensure that the statement of applicability (SOA) is approved by the management and in alignment with the outcomes of the annual risk assessment to ensure consistency and relevance.	1. Inspect the organization's statement of applicability (SOA) and compares it with the result of the annual risk assessment. 2. Validate whether the statement of applicability is approved by management.	E-RM-17
SDD-01	System Design Documentation	System Documentation	Documentation of system boundaries and key aspects of their functionality are published to authorized Organization personnel on the Organization intranet.	Process	Preventive	System Architecture and Design Documentation Standard	1. Ensure that appropriate documentation is established for system boundaries and key aspects of functionality. 2. Ensure that these diagrams are available to authorized personnel through intranet.	1. Inspect and validate that appropriate documentation is established for system boundaries and key aspects of functionality. 2. Validate that these diagrams are available to authorized personnel through intranet.	E-SDD-01
SDD-02	System Design Documentation	Whitepapers	Organization publishes whitepapers to its public website that describe the purpose, design and boundaries of the system and system components.	Process	Preventive	Information Security Management Standard	1. Ensure that the organization's public website have published whitepapers describing the purpose, design, and boundaries of the in-scope services and system components. 2. Ensure that these whitepapers are reviewed periodically for accuracy and approved by relevant personnel prior to publishing.	1. Inspect the organization's public website to determine whether whitepapers for in-scope services are published.	E-SDD-02
SG-01	Security Governance	Policy and Standard Review	Organization's policies and standards are periodically reviewed, approved by management, and communicated to Organization personnel.	Process	Preventive	Information Security Management Standard	1. Ensure that the organization's policies and standards are well-defined, documented and communicated with relevant personnel. 2. Ensure that these policies and standards are reviewed periodically and are approved by the management.	1. Inspect organization's Policy to determine whether requirements for periodic reviews, management approval, and communication of policies and standards are defined. 2. Inspect a sample of organization's policies and standards to determine whether they are documented, periodically reviewed, and approved by management 3. Inspect the corporate intranet or email communication sent to employee that validates these policies are communicated within the organization.	E-SG-01 E-SG-02 E-SG-03
SG-02	Security Governance	Exception Management	Organization reviews exceptions to policies, standards and procedures; exceptions are documented and approved based on business need and removed when no longer required.	Process	Detective	Information Security Management Standard	1. Ensure that a process for the handling of exceptions is well defined and documented. 2. Ensure exceptions observed have thorough documentation, approval from higher management, and are promptly removed when no longer needed.	1. Inspect organization's policy and/or standards to determine whether requirements to review, approve, and document exceptions to policies, standards, and procedures are defined. 2. Inspect a sample of exceptions to determine whether each exception is reviewed, approved, and documented based on business need and removed when no longer required.	E-SG-01 E-SG-04
SG-03	Security Governance	Document Control	Organization's document management criteria is periodically reviewed, approved by management, and communicated to authorized personnel; management determines the treatment and retention of documentation according to legal and regulatory requirements.	Process	Preventive	Information Security Management Standard	1. Ensure that the organization has a well defined and documented document management criteria. 2. Ensure that the criteria is reviewed and approved by the management periodically. 3. Ensure that the criteria is communicated to authorized personnel. 4. Ensure that the documentation is treated and retained according to legal and regulatory requirements.	1. Inspect the organization's policy and/or standard to validate that the organization has a well defined and documented document management criteria. 2. Validate that the criteria is reviewed and approved by the management periodically. 3. Validate whether the criteria is communicated to authorized personnel. 4. Validate for a sample documentation that it is treated and retained according to legal and regulatory requirements.	E-SG-01 E-SG-05 E-SG-06
SG-04	Security Governance	Information Security Program Content	The Chief Security Officer conducts a periodic staff meeting to communicate and align on relevant security threats, program performance, and resource prioritization.	Process	Preventive	Information Security Management Standard	1. Ensure that a process is defined and documented for conducting periodic staff meetings with the Chief Security Officer. 2.Ensure that the meeting agenda consists of security threats, Information Security Management Program Performance and Resource Prioritization.	1. Inspect and validate that a process is defined and documented for conducting periodic staff meetings with the Chief Security Officer. 2. Validate that the meeting agenda consists of security threats, Information Security Management Program Performance and Resource Prioritization for sample quarters.	E-SG-01 E-SG-15

SG-05	Security Governance	Procedures	Organization's key control capabilities are supported by documented procedures that are communicated to authorized personnel.	Process	Preventive	Information Security Management Standard	1. Ensure that a process is defined and documented so that all key control capabilities are supported by documented procedures. 2. Ensure that these procedures are communicated to authorized personnel.	1. Inspect and validate that a process is defined and documented so that all key control capabilities are supported by documented procedures. 2. Validate that these procedures are communicated to authorized personnel.	E-SG-01
SG-06	Security Governance	Proprietary Rights Agreement	Organization regular employees consent to a proprietary rights agreement.	Process	Preventive	Human Resource Policy	1. Ensure that all employees are required to sign a proprietary rights agreement prior to joining the organization. 2. Ensure that appropriate records are maintained for retaining this information.	1. Inspect the procedure for employees to sign proprietary rights agreement. 2. Inspect a sample of employee's proprietary rights agreement.	E-SG-07
SG-07	Security Governance	Review of Confidentiality Agreements	The Organization Proprietary Rights Agreement and Organization Network Access Agreement are reviewed on a periodic basis.	Process	Preventive	Human Resource Policy	1. Ensure all employees sign the organization's proprietary rights agreement and network access agreement prior to joining the organization. 2. Ensure these agreements are updated on a need-to-know basis and communicated to stakeholders.	1. Inspect organization's proprietary rights agreement and network access agreement and check for periodic review.	E-SG-07
SG-08	Security Governance	Information Security Program	Organization has an established security leadership team including key stakeholders in the Organization Information Security Program; goals and milestones for deployment of the information security program are established and communicated to the company through the periodic security all-hands meeting.	Process	Preventive	Information Security Management Standard	1. Ensure there is a dedicated information security management standard which consists of requirements pertaining to security leadership team and the establishment and communication of security goals and milestones. 2. Ensure the organization's information security management standard is uploaded on corporate intranet and made available to all employees. 3. Ensure, ISMS steering committee is conducting monthly meetings whose, minutes are documented and communicated to relevant stakeholders.	1. Inspect Information Security Management Standard to determine whether requirements for a security leadership team and the establishment and communication of security goals and milestones are defined. 2. Observe organization's corporate intranet to determine whether the Information Security Management Standard is communicated to the company. 3. Inspect the most recent ISMS Steering minutes to determine the participation from the security leadership team, and the establishment and communication of security goals and milestones.	E-SG-01 E-SG-08 E-SG-09
SG-09	Security Governance	Accessibility Program	Organization has an established accessibility leadership team including key stakeholders; goals and milestones for deployment of the accessibility program are established and communicated to the company.	Process	Preventive	Information Security Management Standard	1. Prepare a list of accessibility key stakeholders and objectives of accessibility program. 2. Review ISMS standard to ensure that it includes the information related to accessibility program and made available to the employees of the organization.	1. Validate that the ISMS standard lists key stakeholders and objectives of the accessibility program. 2. Observed how the ISMS standard includes information about the accessibility program and whether it is readability available to employees of the organization.	E-SG-01
SG-10	Security Governance	Information Security Management System Scope	Information Security Management System (ISMS) boundaries are formally defined in an ISMS scoping document.	Process	Preventive	Information Security Management Standard	1. Ensure a process has been defined and documented to create an ISMS scoping document. 2. Ensure that this document is appropriately reviewed and updated to refelct accurate boundaries for the information security management system.	1. Inspect and validate whether a process has been defined and documented to create an ISMS scoping document. 2. Validate whether this document was appropriately reviewed and updated.	E-SG-10
SG-11	Security Governance	Security Roles and Responsibilities	Roles and responsibilities for the governance of Information Security within Organization are formally documented within the Information Security Management Standard and communicated on the Organization intranet.	Process	Preventive	Information Security Management Standard	1. Ensure organization's information security standard consists of roles and responsibilities for the governance of information security within organization and uploaded on the corporate intranet and made available to all employees. 2. Ensure, ISMS steering committee is conducting monthly meetings whose, minutes are documented and communicated to relevant stakeholders.	1. Inspect Organization's Information Security Management Standard to determine whether it was communicated and defined information security roles and responsibilities for the governance of information security within Organization. 2. Observed Organization's corporate intranet to determine whether the Information Security Management Standard is communicated to the company. 3. Inspect the most recent ISMS Steering Committee Meeting minutes to determine the participation from the security leadership team, and establishment and communication of security goals and milestones.	E-SG-10
SG-12	Security Governance	Security Roles and Responsibilities: Risk Designations	Organization defined security roles and responsibilities are assigned risk designations and reviewed at least once every three years.	Process	Preventive	Information Security Management Standard	1. Ensure there is a risk management policy, and risk matrix (which consists of risk severity, risk treatment, risk mitigation plan, and compensatory control) which are updated once in every 3 years or on a need-to-know basis.	1. Inspect Organization's Risk Management policy and risk control matrix and ensure they are updated once in every 3 years or on a need-to-know basis.	E-SG-11 E-SG-12

SG-13	Security Governance	Security Roles and Responsibilities: PCI Compliance	Roles and responsibilities and a program charter for the governance of PCI DSS compliance within Organization are formally documented and communicated by management.	Process	Preventive	Information Security Management Standard	1. Define roles and responsibilities for PCI DSS governances which is approved by the organization's management and documented well in PCI Charter.	1. Inspect Organization's PCI Charter and organization chart to determine that roles and responsibilities for PCI DSS governances are appropriately documented and disseminated by Organization Management.	E-SG-13
SG-14	Security Governance	Information Security Resources	Information systems security implementation and management are included as part of the budget required to support the Organization Security Program.	Process	Preventive	Information Security Management Standard	1. Allocate resources as per the Organization's Security program and the defined budget. 2. Ensure management meets monthly or on a need-to-know basis to discuss the critical security requirements across organization based on multiple factors as well as justifications basis which budget is allocated for management of Organization's security program and corresponding records are maintained. 3. Each department spend and allocate resources as per the defined budget and security program which aligns with the business objectives. 4. Ensure budget is approved by top management for spending to be aligned with business justification.	1. Inspect all the security requirements for which budget is required as a part of Organization's Security program and corresponding business justification are identified, documented and maintained. 2. Ensure that as a part of regular periodic management review meetings identified critical security requirements across organization are reviewed as well as analyzed and based on multiple factors as well as justifications basis which budget is allocated for management of Organization's security program and corresponding records are maintained. 3. Inspect documentation around representation from all the key departments to ensure allocation of budget for security program is aligned with business objectives. 4. Inspect the approval obtained by top management for spending of allocated budget to be aligned with business justification.	E-SG-14 E-SG-15
SG-15	Security Governance	Management Review	The Information Security Management System (ISMS) steering committee conducts a formal management review of ISMS scope, risk assessment activities, control implementation, and audit results on an annual basis.	Process	Corrective	Information Security Management Standard	1. Conduct ISMS steering committee meeting on monthly basis or on a need-to-know basis to discuss and review the current scope (products included), audit progress, ISMS scope, risk assessment activities, control implementation, and audit results. 2. Document the attendance of each member.	1. Validate that ISMS Steering committee meet at least annually, and inspect meeting minutes from each meeting. 2. Inspect attendees of the steering committee meeting shall be documented, and members of the information steering committee shall include relevant members from the offering's organization. 3. Each meeting shall include an discussion and review of current scope (products included), audit progress, ISMS scope, risk assessment activities, control implementation, and audit results. Included shall be action items for any audit findings.	E-SG-09
SG-16	Security Governance	Enterprise Data Catalog	Organization maintains an enterprise data catalog that encompasses key organizational data, environment metadata, and product information to facilitate continuous monitoring of the internal control environment. The enterprise data catalog is updated as part of the continuous monitoring process and upon the introduction of new service offerings and acquisitions.	Process	Preventive	Information Security Management Standard	1. Ensure there is a documented enterprise data catalogue which consists of details that include but not limited to: key organizational data, environment metadata, and product information to facilitate continuous monitoring of the internal control environment. 2. Ensure that the documented enterprise data catalogue is reviewed and updated annually or as in when required.	1. Inspect the Enterprise Data Catalog to determine that it includes key organizational data, environment metadata, and product information to facilitate continuous monitoring of the internal control environment. 2. Inspect that the data catalog is reviewed and updated periodically and further, upon the introduction of new service offerings and acquisitions.	E-SG-16

SG-17	Security Governance	Software Usage Restrictions	Organization maintains software license contracts and monitors its compliance with usage restrictions.	Process	Detective	Information Security Management Standard	1. Ensure there is a formal documented software license agreement/policy which defines the criteria for the installation of software. 2. Ensure software license agreement/policy is reviewed and updated on annual basis or when required. 3. Continuous monitoring of installed software to ensure the compliance posture as per the defined criteria.	1. Identify and document the inventory of software license contracts corresponding to different software. 2. Inspect management approved procedures for license maintenance and usage are in place and maintained. 3. Ensure that monitoring is in place to check the compliance effectiveness with usage restrictions defined as part of software license maintenance as well as usage contracts. 4. Ensure monitoring records of period review/audits are maintained to ensure adherence to the requirements of the software license contracts and usage restrictions. 5. Licenses and contracts are reviewed as needed, and increased supply of licenses and contracts are obtained if needed to meet use/demand.	E-SG-17 E-SG-18
SLC-01	Service Lifecycle	Service Lifecycle Workflow	Major software releases are subject to the Service Life Cycle, which requires acceptance via Concept Accept and Project Plan Commit phases prior to implementation.	Process	Preventive	Secure Development Lifecycle Policy	1. Ensure there is a documented standard for organization product lifecycle and secure product lifecycle which consists requirements for acceptance via concept accept and project plan commit phases prior to implementation. 2. Ensure the standard for organization product lifecycle and secure product lifecycle are reviewed and updated as required. 3. Implement a procedure to document the acceptance via concept accept and project plan commit phases prior to implementation for each and every major release.	1. Inspect Organization's Product Lifecycle Standard and Secure Product Lifecycle Standard to determine whether requirements for acceptance via Concept Accept and Project Plan Commit phases prior to implementation are defined. 2. Inspect documentation for a selection of major releases to determine whether it includes documentation of acceptance via Concept Accept and Project Plan Commit phases prior to implementation.	E-SLC-01 E-SLC-02
SLC-02	Service Lifecycle	Source Code Management	Source code is managed with Organization-approved version control mechanisms.	Process	Preventive	Secure Development Lifecycle Policy	1. Ensure there is a documented organization's source code security standard and it is updated on need to know basis. 2. Ensure source code repositories used by service team as per the approved version control mechanisms/systems.	1. Inspect Organization's Source Code Security Standard to determine whether requirements for Organization-approved version control software are in place. 2. For a sample of services, inspect source code repository used by services to determine that source code is managed with Organization-approved version control mechanisms/systems.	E-SLC-03 E-SLC-04
SLC-03	Service Lifecycle	Secrets in Code	Organization manages source code secrets in a centralized repository; secrets are rotated at least annually and immediately if the security of secrets is compromised.	Process	Preventive	Secure Development Lifecycle Policy	1. Each service should have a central source code repository where all secrets are managed. 2. Secrets of the service are rotated once every year and in cases where the securiy of secrets is compromised. Logs for the same are maintained and documented.	1. For a sample of services, inspect the Organization's centralized repository to determine that source code secrets are managed in a centralized repository. 2. Obtain evidence to validate secrets are rotated at least annually and immediately if the security of secrets is compromised.	E-SLC-05 E-SLC-06
SLC-04	Service Lifecycle	Project Budget Approval	Approval for project initiation and budget is obtained from IT management and business owners.	Process	Preventive	Secure Development Lifecycle Policy	1. Prepare a project management plan that includes but not limited to project initiation guidelines and budget from IT management and business owners.	1. Obtain evidence of approval for project initiation and budget from IT management and business owners.	E-SLC-07 E-SLC-08
SLC-05	Service Lifecycle	Project Scope Change	Changes to finalized project scope and requirements require the review and approval from the business team and project manager.	Process	Preventive	Secure Development Lifecycle Policy	1. Prepare a project management plan that outlines the project scope, and requirements. 2. Project Management plan is approved by business team.	1. Review the changes that have been modified and finalized for project scope and requirements. 2. Obtain evidence of approval from the business team and project management for finalization of project scope and requirements.	E-SLC-07 E-SLC-08

SLC-06	Service Lifecycle	Information System Operation Authorization	Senior management authorizes the operation of new information systems, based on security and business requirements, prior to implementation. The information system authorization is refreshed every 3 years or when significant change occurs.	Process	Preventive	Secure Development Lifecycle Policy	1. Ensure there is documented service lifecycle program which is updated on a need-to-know basis 2. Ensure there is a documented information system operation authorization which is approved by the senior management and updated once in every 3 years or on a need-to-know basis.	1. Inspect the approval matrix for Service Lifecycle Program Management. 2. Inspect the approval matrix for Information System Operation Authorization by the authorized senior management to determine the operation of new information systems 3. Review the information system authorization is updated every 3 years or when significant changes occurs.	E-SLC-09 E-SLC-10
SLC-07	Service Lifecycle	System Acquisition Approval	Information system acquisitions require approval from authorized personnel based on verification of the following documented evidence: • security function, strength, and assurance requirements • requirements for protecting security-related documentation • system development and test requirements • acceptance criteria for releases • enumeration of Security controls • security control implementation and monitoring requirements • components are FIPS-201 approved	Process	Preventive	Secure Development Lifecycle Policy	1. Define and implement a procedure for the formal approval from an authorized personnel Information system acquisitions based on verification of the following documented evidence: • security function, strength, and assurance requirements • requirements for protecting security-related documentation • system development and test requirements • acceptance criteria for releases • enumeration of Security controls • security control implementation and monitoring requirements • components are FIPS-201 approved	1. Obtain evidence of approval from authorized personnel for Information system acquisitions based on verification of the following documented evidence: • security function, strength, and assurance requirements • requirements for protecting security-related documentation • system development and test requirements • acceptance criteria for releases • enumeration of Security controls • security control implementation and monitoring requirements • components are FIPS-201 approved	E-SLC-11
SM-01	Systems Monitoring	Audit Logging	Organization logs critical information system activity.	Technology	Detective	Logging & Monitoring Standard	1. Ensure that the Organization's Logging Standard includes logging requirements for critical system activity. 2. Ensure that the following system logging configurations (at the least, but not limited to) for a selection of production systems to determine the following: a. Log aggregation tool is configured for the service. b. Whether the below logs are being sent to the log aggregation tool: i. System OS logs ii. AWS Config (configuration monitoring resource in AWS) iii. Cloud Trail (All account level activity including API calls, IAM role/user) iv. VPC Flow Logs (Showing all network connections to and from a VPC) v. Guard Duty (AWS provided threat detection service) c. PCI Specific - Whether critical information system activity is logged such as the following:	1. Inspect Organization's Logging Standard to determine whether logging requirements are defined for critical system activity. 2. Inspect system logging configurations for a sample of production systems to determine the following: a. Log aggregation tool is configured for the service. b. Whether the below logs are being sent to the log aggregation tool: i. System OS logs ii. AWS Config (configuration monitoring resource in AWS) iii. Cloud Trail (All account level activity including API calls, IAM role/user) iv. VPC Flow Logs (Showing all network connections to and from a VPC) v. Guard Duty (AWS provided threat detection service) c. PCI Specific - Whether critical information system activity is logged such as the following:	E-SM-01 E-SM-02 E-SM-03
SM-02	Systems Monitoring	Secure Audit Logging	Organization logs critical information system activity to a secure repository. Organization disables administrators ability to delete or modify enterprise audit logs; the number of administrators with access to audit logs is limited.	Process	Detective	Logging & Monitoring Standard	1. Ensure that Organization's Logging Standard includes logging requirements for critical system activity to mandate log forwarding and storage in a central repository. 2. Establish a process for periodic review of appropriate access of the administrators to SIEM tool. 3.Ensure that only a defined list of users are allowed to delete/modified SIEM logs.	1. Inspect Organization's Logging Standard to determine whether logging requirements are defined for critical system activity to mandate log forwarding and storage in a central repository. 2. Inspect the list of SIEM tool Administrators and validate that their access is appropriate. 3. Validate the list of users allowed to delete/modified SIEM tool logs and ensure it is restricted.	E-SM-01 E-SM-04

SM-03	Systems Monitoring	Audit Logging: Cardholder Data Environment Activity	Organization logs the following activity for cardholder data environments: • individual user access to cardholder data • administrative actions • access to logging servers • failed logins • modifications to authentication mechanisms and user privileges • initialization, stopping, or pausing of the audit logs • creation and deletion of system-level objects • security events • logs of all system components that store, process, transmit, or could impact the security of cardholder data (CHD) and/or sensitive authentication data (SAD) • logs of all critical system components • logs of all servers and system components that perform security functions (e.g., firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)	Technology	Detective	Logging & Monitoring Standard	1. Ensure that the following activity types are being logged in SIEM tool: a. individual user access to cardholder data b. administrative actions c. access to logging servers d. failed logins e. modifications to authentication mechanisms and user privileges f. initialization, stopping, or pausing of the audit logs g. creation and deletion of system-level objects h. security events i. logs of all system components that store, process, transmit, or could impact the security of cardholder data (CHD) and/or sensitive authentication data (SAD) j. logs of all critical system components	1. Inspect SIEM Logs for a sample of in-scope production servers to validate that the below activity types are being logged: a. individual user access to cardholder data b. administrative actions c. access to logging servers d. failed logins e. modifications to authentication mechanisms and user privileges f. initialization, stopping, or pausing of the audit logs g. creation and deletion of system-level objects h. security events i. logs of all system components that store, process, transmit, or could impact the security of cardholder data (CHD) and/or sensitive authentication data (SAD) j. logs of all critical system components	E-SM-01 E-SM-03
SM-04	Systems Monitoring	Audit Logging: Cardholder Data Environment Event Information	Organization records the following information for confirmed events in the cardholder data environment: • user identification • type of event • date and time • event success or failure indication • origination of the event • identification of affected data, system component, or resource	Technology	Detective	Logging & Monitoring Standard	1. Ensure that the below information is being logged for all critical security events: a. user identification b. type of event c. date and time d. event success or failure indication e. origination of the event f. identification of affected data, system component, or resource	1. Inspect SIEM Logs for a sample of in-scope production servers to validate that the below information is being logged for all critical security events: a. user identification b. type of event c. date and time d. event success or failure indication e. origination of the event f. identification of affected data, system component, or resource	E-SM-01 E-SM-03
SM-05	Systems Monitoring	Audit Logging: Service Provider Logging Requirements	Organization establishes unique logging and audit trails for each entity's cardholder data environment and complies with the following: • logs are enabled for third-party applications • logs are active by default • logs are available for review by and communicated to the owning entity	Technology	Detective	Logging & Monitoring Standard	1. Establish a process that ensures that Organization's audit trails/audit logs: • each and every third-party application for every entity. • logs are active by default 2. Establish a process in the Organization's logging and monitoring mechanism which ensures that logs are reviewed periodically and on a need-to-do basis. Additionally, the same shall be communicated to the concerned stakeholders.	1. Inspect Organization's audit trails/audit logs for: • each and every third-party application for every entity. • logs are active by default 2. Inspect Organization's logging and monitoring mechanism to ensure that logs are reviewed periodically and on a need-to-do basis. Additionally, validate whether the same is being communicated to the concerned stakeholders.	E-SM-01 E-SM-03
SM-06	Systems Monitoring	Configuration Management: Remote Logging	Where applicable, devices are configured to send audit log data to a remote server	Technology	Preventive	Logging & Monitoring Standard	1. Establish a data flow mechanism to ensure that the devices are configured to send audit log data to a remote server.	1. Inspect Organization's data flow mechanisms to ensure that the devices are configured to send audit log data to a remote server.	E-NO-17 E-SM-01 E-SM-03
SM-07	Systems Monitoring	Chain of Accountability	Organization implements audit trails to link authentication events to individuals users in production systems.	Technology	Detective	Logging & Monitoring Standard	1. Establish organization's logging and monitoring process. 2. Ensure logs contain identifiers to establish audit trails to systems and users.	1. Validate the organizations logging and monitoring process. 2. Validate whether the logs contain identifiers to establish audit trails to systems and users.	E-SM-01 E-SM-03

SM-08	Systems Monitoring	Audit Record Time Stamps	Organization records time stamps for audit records that can be mapped to a centralized time source.	Technology	Detective	Logging & Monitoring Standard	1. Ensure that the time sync is enabled, stratums are defined, and the time servers are working.	1. Validate whether time sync is enabled, stratums are defined, and the time servers are working. 2. For a sample of audit records, review time stamps to determine whether time stamps for audit records can be mapped to a centralized time source.	E-SM-05
SM-09	Systems Monitoring	Log Reconciliation: CMDB	Organization reconciles the established device inventory against the enterprise log repository on a quarterly basis; devices which do not forward log data are remediated.	Process	Corrective	Infrastructure Management Policy	1. Design a process to prepare a quarterly Log reconciliation report which includes reconciliation of the established device inventory against the enterprise log repository. 2. Wherever deviation is identified from the reconciliation, ensure that the actions are taken for remediation of the devices which do not forward log data.	1. Inspect Organization's Log reconciliation report to determine that the established device inventory against the enterprise log repository is reconciled on a quarterly basis. 2. Inspect the actions taken for remediation of the devices which do not forward log data.	E-SM-06 E-SM-07
SM-10	Systems Monitoring	Audit Log Capacity and Retention	Organization allocates audit record storage capacity in accordance with logging storage and retention requirements; Audit logs are retained for 1 year with 90 days of data immediately available for analysis.	Process	Corrective	Logging & Monitoring Standard	1. Document Organization's Logging Standard which includes logging retention requirements for critical system activity to mandate logs be available for a minimum for 1 year. 2. Implement SIEM tool configuration to retrieve the relevant logs for a minimum period of 1 year with 90 days of logs be available for immediate analysis.	1. Inspect Organization's Logging Standard to determine whether logging retention requirements are defined for critical system activity to mandate logs being available for a minimum for 1 year 2. Inspect sample logs for in-scope services to validate that the SIEM tool stores relevant logs for a minimum period of 1 year with 90 days of logs being available for immediate analysis. 3. Evaluate the SIEM tool configuration to validate the retention settings for 1 year.	E-SM-01 E-SM-02 E-SM-03
SM-11	Systems Monitoring	Enterprise Antivirus Logging	If applicable, Organization's managed enterprise antivirus deployments generate audit logs which are retained for 1 year with 90 days of data immediately available for analysis.	Technology	Detective	Logging & Monitoring Standard	1. Enable configurations for Enterprise Antivirus solutions to ensure that antivirus logs are being forwarded to the SIEM 2. Ensure that relevant logs are stored for a minimum period of 1 year with 90 days of logs being available for immediate analysis.	1. Inspect configurations for Enterprise Antivirus solutions to validate that antivirus logs are being forwarded to SIEM. 2. Inspect sample antivirus logs for in-scope services to validate that relevant logs are stored for a minimum period of 1 year with 90 days of logs being available for immediate analysis.	E-SM-08 E-SM-09
SM-12	Systems Monitoring	Security Monitoring Alert Criteria	Organization defines security monitoring alert criteria, how alert criteria will be flagged, and identifies authorized personnel for flagged system alerts.	Process	Detective	Logging & Monitoring Standard	1. Document Organization's Security Monitoring Standard to include requirements for security monitoring alert criteria. 2. Establish a process to periodically review and maintain a list of security monitoring rules.	1. Inspect Organization's Security Monitoring Standard to determine whether requirements for security monitoring alert criteria are defined. 2. Obtain list of security monitoring rules that are defined. 3. For a sample of alert rules from a sample of services, inspect the monitoring tool configuration to determine that rules are implemented to flag events, and notify authorized personnel.	E-SM-10 E-SM-11 E-SM-12
SM-13	Systems Monitoring	Security Monitoring Alert Criteria Review	Organization reviews security monitoring alert on an annual basis.	Process	Detective	Logging & Monitoring Standard	1. Document Organization's Security Monitoring Standard to include requirements for security monitoring alert criteria. 2. Establish a process to ensure that the monitoring tool is configured to review the security alerts on an annual basis by the authorized personnel.	1. Inspect Organization's Security Monitoring Standard to determine whether requirements for security monitoring alert criteria are defined. 2. For a sample of alert rules from a sample of services, inspect the monitoring tool configuration to determine that security alerts are reviewed on an annual basis by the authorized personnel.	E-SM-10 E-SM-11 E-SM-12

SM-14	Systems Monitoring	Log-tampering Detection	Organization monitors and flags tampering to the audit logging and monitoring tools in the production environment.	Technology	Detective	Logging & Monitoring Standard	1. Ensure Organization's Security Monitoring Standard to include requirements for monitoring and flagging, tampering to the audit logging and monitoring tools in the production environment. 2. Ensure specific mechanisms to monitor and flag tampering to the audit logging and monitoring tools in the production environment are defined and documented. 3. Ensure appropriate mechanisms are implemented for protecting integrity of logs and to prevent/detect logs from being modified/tampered at the storage location. Additionally, ensure such activities are recorded and controlled. 4. Restrict and control administrative permissions to manage and modify audit logs to authorized personnel only. 5. Ensure all administrative and operational activities are logged and events are captured to trace back to a particular user in case of any modifications/tampering performed. 6. Replicate and store all applicable logs on a centralized server and restrict access to only authorized personnel.	1. Obtain relevant organizational policy/standard and ensure defined process regarding enabling audit logging and monitoring are adhered to. 2. Validate specific mechanisms to monitor and flag tampering to the audit logging and monitoring tools in the production environment are defined and documented. 3. Validate whether appropriate mechanisms are implemented to protect the integrity of logs and to prevent/detect logs from being modified/tampered at the storage location. Additionally, ensure such activities are recorded and controlled. 4. Inspect whether administrative permissions to manage and modify audit logs are restricted to authorized personnel only. 5. For a sample of events, inspect whether all administrative and operational activities are logged and events are captured to trace back to a particular user in case of any modifications/tampering performed. 6. Validate whether all applicable logs are replicated and stored on a centralized server and access is restricted to only authorized personnel,	E-SM-10 E-SM-11 E-SM-13 E-SM-04
SM-15	Systems Monitoring	Unauthorized Devices Addition	Unauthorized devices connected to the Organization Network are: • detected within a maximum of five minutes, and • the unauthorized device is disabled, or a notification is sent to authorized Organization personnel	Technology	Detective	Logging & Monitoring Standard	1. Enable Organization's monitoring tool configurations to ensure that unauthorized devices are: • detected within a maximum of five minutes, and • the unauthorized device is disabled, or a notification is sent to authorized Organization personnel	1. Inspect Organization's monitoring tool configurations to ensure that the following: • detected within a maximum of five minutes, and • the unauthorized device is disabled, or a notification is sent to authorized Organization personnel	E-SM-14
SM-16	Systems Monitoring	Security Monitoring Alert Criteria: Guest, Anonymous and Temp Accounts	Organization defines security monitoring alert criteria for the use of guest, anonymous, and temporary accounts on Organization's network.	Process	Detective	Logging & Monitoring Standard	1. Ensure that Organization's Security Monitoring Standard includes requirements for security monitoring alert criteria for the use of guest, anonymous, and temporary accounts on Organization's network. 2. Ensure that the security monitoring rules are defined, enabled and alert applicable personnel on the use of guest, anonymous, and temporary accounts on Organization's network. 3. Ensure that alerts are being generated and sent to the SOC team to support remediation.	1. Inspect Organization's Security Monitoring Standard to determine whether requirements for security monitoring alert criteria for the use of guest, anonymous, and temporary accounts on Organization's network are defined. 2. Inspect a sample of security monitoring rules, to validate that the rules are defined to look for and alert applicable personnel on the use of guest, anonymous, and temporary accounts on Organization's network. 3. Validate that alerts being generated are sent to the SOC team to support remediation.	E-SM-10
SM-17	Systems Monitoring	Security Monitoring Alert Criteria: VoIP Usage	Organization defines security monitoring alert criteria to detect deviations from Voice over IP (VoIP) activity standards.	Process	Detective	Logging & Monitoring Standard	1. Ensure that Organization's Security Monitoring Standard includes requirements for security monitoring alert criteria to detect deviations from Voice over IP (VoIP) activity standards are defined. 2. Ensure that the security monitoring rules are defined, enabled and alert applicable personnel on deviations from Voice over IP (VoIP) activity standards. 3. Ensure that alerts are being generated and sent to the SOC team to support remediation.	1. Inspect Organization's Security Monitoring Standard to determine requirements for security monitoring alert criteria to detect deviations from Voice over IP (VoIP) activity standards are defined. 2. Inspect a sample of security monitoring rules, to validate that the rules are defined to look for and alert applicable personnel on deviations from Voice over IP (VoIP) activity standards. 3. Validate that alerts being generated are sent to the SOC team to support remediation.	E-SM-10
SM-18	Systems Monitoring	Prohibited Activity Monitoring: Remote Access	Remote sessions are monitored for prohibited activity.	Technology	Detective	Logging & Monitoring Standard	1. Ensure that the monitoring reports or evidence of logs from remote sessions are reviewed for prohibited activity.	1. Review the monitoring reports or evidence of logs from remote sessions to determine that the remote sessions are reviewed for prohibited activity.	E-SM-15

SM-19	Systems Monitoring	Prohibited Activity Monitoring: Client Run Time Technologies	Organization monitors and flags the use of prohibited client run time technologies on information systems.	Technology	Detective	Logging & Monitoring Standard	1. Ensure that the monitoring software are installed on information systems. 2. Enable the alerting criteria to ensure it monitors prohibited execution.	1. Validate and inspect if monitoring software are installed on information systems. 2. Inspect the alerting criteria to ensure it monitors prohibited execution.	E-SM-16 E-SM-17
SM-20	Systems Monitoring	Security Monitoring Alert Criteria: Wireless Access Point	Organization defines security monitoring alert criteria for attack attempts against wireless access points.	Process	Detective	Logging & Monitoring Standard	1. Ensure that Organization's Security Monitoring Standard includes requirements for security monitoring alert criteria for attack attempts against wireless access points. 2. Ensure that the security monitoring rules are defined, enabled and alert applicable personnel on potential failed login attempts. 3. Ensure that alerts are being generated and sent to the SOC team to support remediation.	1. Inspect Organization's Security Monitoring Standard to determine whether requirements for security monitoring alert criteria for attack attempts against wireless access points are defined. 2. Obtain list of security monitoring rules that are defined.	E-SM-10 E-SM-11
SM-21	Systems Monitoring	Security Monitoring Alert Criteria: Failed Logins	Organization defines security monitoring alert criteria for failed login attempts on Organization's network.	Process	Detective	Logging & Monitoring Standard	1. Ensure that Organization's Security Monitoring Standard includes requirements for security monitoring alert criteria for failed login attempts on Organization's network. 2. Ensure a sample of security monitoring rules, to validate that the rules are defined to look for and alert applicable personnel on potential failed login attempts. 3. Ensure that alerts being generated are sent to the SOC team to support remediation.	1. Inspect Organization's Security Monitoring Standard to determine whether requirements for security monitoring alert criteria for failed login attempts on Organization's network. 2. Inspect a sample of security monitoring rules, to validate that the rules are defined to look for and alert applicable personnel on potential failed login attempts. 3. Validate that alerts being generated are sent to the SOC team to support remediation.	E-SM-18 E-SM-19
SM-22	Systems Monitoring	Security Monitoring Alert Criteria: Privileged Functions	Organization defines security monitoring alert criteria for privileged functions executed by both authorized and unauthorized users.	Process	Detective	Logging & Monitoring Standard	1. Ensure that Organization's Security Monitoring Standard includes requirements for security monitoring alert criteria for privileged functions executed by both authorized and unauthorized users. 2. Ensure that the security monitoring rules are defined, enabled and alert applicable personnel on privileged functions executed by both authorized and unauthorized users. 3. Ensure that alerts are being generated and sent to the SOC team to support remediation.	1. Inspect Organization's Security Monitoring Standard to determine whether requirements for privileged functions executed by both authorized and unauthorized users. 2. Inspect a sample of security monitoring rules, to validate that the rules are defined to look for and alert applicable personnel on privileged functions executed by both authorized and unauthorized users. 3. Validate that alerts being generated are sent to the SOC team to support remediation.	E-SM-18 E-SM-19
SM-23	Systems Monitoring	Security Monitoring Alert Criteria: Audit Log Integrity	Organization defines security monitoring alert criteria for changes to the integrity of audit logs.	Process	Detective	Logging & Monitoring Standard	1. Ensure that Organization's Security Monitoring Standard includes requirements for security monitoring alert criteria for changes to the integrity of audit logs. 2. Ensure that the security monitoring rules are defined, enabled and alert applicable personnel on changes to the integrity of audit logs. 3. Ensure that alerts are being generated and sent to the SOC team to support remediation.	1. Inspect Organization's Security Monitoring Standard to determine whether requirements for changes to the integrity of audit logs. 2. Inspect a sample of security monitoring rules, to validate that the rules are defined to look for and alert applicable personnel on changes to the integrity of audit logs. 3. Validate that alerts being generated are sent to the SOC team to support remediation.	E-SM-18 E-SM-19
SM-24	Systems Monitoring	Security Monitoring Alert Criteria: Cardholder System Components	Organization defines security monitoring alert criteria for system components that store, process, transmit, or could impact the security of cardholder data and/or sensitive authentication data.	Process	Detective	Logging & Monitoring Standard	1. Ensure that Organization's Security Monitoring Standard includes requirements for security monitoring alert criteria for system components that store, process, transmit, or could impact the security of cardholder data and/or sensitive authentication data. 2. Ensure that the security monitoring rules are defined, enabled, and alert applicable personnel on checks for any impact to the CDE. 3. Ensure that alerts are being generated and sent to the SOC team to support remediation.	1. Inspect whether the security logs from various sources are sent to the monitoring tool. 2. Inspect a sample of security monitoring rules, to validate that the rules are defined to look for and alert applicable personnel on checks for any impact to the CDE. 3. Validate that alerts being generated are sent to the SOC team to support remediation.	E-SM-18 E-SM-19

SM-25	Systems Monitoring	System Security Monitoring	Critical systems are monitored in accordance with predefined security criteria and alerts are sent to authorized personnel. Confirmed incidents are tracked to resolution.	Process	Detective	Logging & Monitoring Standard	1. Ensure that Organization's Security Monitoring Standard includes requirements for responding to flagged system alerts and confirmed incidents. 2. Configure security monitoring tool to ensure that critical information system activity is monitored. 3. Ensure that the events are triaged and resolved by authorized personnel as applicable.	1. Inspect Organization's Security Monitoring Standard to determine whether requirements are defined for responding to flagged system alerts and confirmed incidents. 2. For a sample of services, inspect security monitoring tool to determine whether critical information system activity is monitored. 3. Inspect a sample of security events to determine whether the events are triaged and resolved by authorized personnel as applicable.	E-SM-10 E-SM-19
SM-26	Systems Monitoring	Intrusion Detection Systems	Organization has an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) deployment(s) and ensures the following: • signature definitions are updated including the removal of false positive signatures • non-signature based attacks are defined • IDS/IPS are configured to capture malicious (both signature and non-signature based) traffic • alerts are reviewed and resolved by authorized personnel when malicious traffic is detected	Technology	Detective	Information Systems Operations Policy	1. Ensure that the Organization has a policy or standard that covers the use and management of intrusion detection system (IDS) or intrusion prevention system (IPS) tools on its in-scope systems. 2. Ensure that there is an intrusion detection system (IDS) or intrusion prevention system (IPS) deployed on all in-scope systems. 3. Ensure that IDS/IPS tool is configured in a manner that: • signature definitions are updated including the removal of false positive signatures • non-signature based attacks are defined • IDS/IPS are configured to capture malicious (both signature and non-signature based) traffic • alerts are reviewed and resolved by authorized personnel when malicious traffic is detected 4. Ensure that the ability to disable IDS/IPS tools are restricted to limited personnel, and can only be disabled with a proper justification and for a limited time.	1. Inspect the Organization has a policy or standard that details the use and management of intrusion detection system (IDS) or intrusion prevention system (IPS) tools on its in-scope systems. 2. Obtain a list of all in-scope systems, and for a given sample, confirm that IDS/IPS is running on those systems, and that they are up to date. 3. Inspect the IDS/IPS rulesets and ensure that they are configured with the items below: • signature definitions are updated including the removal of false positive signatures • non-signature based attacks are defined • IDS/IPS are configured to capture malicious (both signature and non-signature based) traffic • alerts are reviewed and resolved by authorized personnel when malicious traffic is detected 4. For a sample of alerts, confirm that they were reviewed and resolved by the authorized personnel. 5. Observe configuration showing that IDS/IPS tools cannot be disabled except by authorized personnel and can only be disabled with a proper justification and for a limited time.	E-SM-18 E-SM-19
SM-27	Systems Monitoring	System Monitoring Legal Opinion	Organization obtains legal opinion with regard to monitoring activities in accordance with applicable requirements and mandates.	Process	Preventive	Logging & Monitoring Standard	1. Design a legal process to ensure that only approved monitoring criteria is established as per applicable legal, contractual, and government requirements. 2. Ensure any change in monitoring criteria takes legal sign off into consideration.	1. Inspect organization's legal process to ensure approved monitoring criteria is established as per applicable legal, contractual, and government requirements. 2. Validate whether any change in monitoring criteria takes legal sign off into consideration.	E-SM-20
SM-28	Systems Monitoring	Privileged Session Monitoring	Organization monitors trusted data environments for unauthorized logical access connections.	Process	Detective	Logging & Monitoring Standard	1. Ensure that Organization's Security Monitoring standard includes the requirements for session monitoring. 2. Configure monitoring tool to ensure least privileged principle is followed. 3. Ensure that the organization monitors trusted data environments for unauthorized logical access connections.	1. Inspect Organization's Security Monitoring standard to determine whether the requirements for session monitoring are defined. 2. Inspect configurations of monitoring tool to ensure least privileged principle is followed. 3. Inspect evidence of the Organization monitoring trusted data environments for unauthorized logical access connections.	E-SM-10 E-SM-14 E-SM-21
SM-29	Systems Monitoring	Availability Monitoring Alert Criteria	Organization defines availability monitoring alert criteria, how alert criteria will be flagged, and identifies authorized personnel for flagged system alerts.	Process	Corrective	Logging & Monitoring Standard	1. Ensure that a documented Availability Monitoring Standard is present including requirements defined for responding to alerts and confirmed incidents. 2. Establish a process to ensure that the availability monitoring rules are defined and implemented to flag events, and notify authorized personnel. 3. Ensure that the system configurations of monitoring tools include Availability Monitoring Alert Criteria.	1. Inspect Organization's Availability Monitoring Standard to determine whether requirements for availability monitoring alert criteria are defined. 2. Inspect availability monitoring tool to determine whether availability monitoring rules are defined and implemented to flag events, and notify authorized personnel. 3. Inspect system configurations of monitoring tools for a sample of services to determine whether Availability Monitoring Alert Criteria are configured for monitoring and alerting purposes on in-scope systems.	E-SM-22 E-SM-23 E-SM-24

SM-30	Systems Monitoring	Availability Monitoring Alert Criteria Review	Organization reviews availability monitoring alert criteria on an annual basis.	Process	Corrective	Logging & Monitoring Standard	1. Ensure that a documented Security Monitoring Standard is present including process regarding availability monitoring alert criteria. 2.. Ensure that the availability monitoring alerts are reviewed on an annual basis.	1. Inspect Security Monitoring Standard to ensure process regarding availability monitoring alert criteria is defined. 2. Inspect evidence of availability monitoring alerts to ensure it is reviewed on an annual basis.	E-SM-10 E-SM-25
SM-31	Systems Monitoring	System Availability Monitoring	Critical systems are monitored in accordance with predefined availability criteria and alerts are sent to authorized personnel.	Process	Corrective	Information Systems Operations Policy	1. Ensure that a documented Availability Monitoring Standard is present including requirements defined for responding to alerts and confirmed incidents. 2. Ensure that a process has been established which generates alerts against the availability incidents identified. 3. Ensure that the alerts are resolved in a timely manner by authorized personnel.	1. Inspect Organization's Availability Monitoring Standard to determine whether requirements are defined for responding to alerts and confirmed incidents. 2. Inspect a sample of availability incident tickets from alerts generated to determine whether the alerts were resolved in a timely manner by authorized personnel.	E-SM-22 E-SM-26
SM-32	Systems Monitoring	Remote Access: Activity Log Audit	Logs from remote sessions are audited for prohibited activity on a weekly basis.	Process	Detective	Logging & Monitoring Standard	1. Establish a process that ensures the logs from remote sessions be reviewed for prohibited activity on a weekly basis.	1. Inspect evidence of logs of remote sessions to determine that the logs are reviewed for prohibited activity on a weekly basis.	E-SM-01 E-SM-27 E-SM-28
SO-01	Site Operations	Secured Facility	Physical access to restricted areas of the facility is protected by walls with non-partitioned ceilings, secured entry points, and/or manned reception desks.	Process	Preventive	Physical and Environmental Security Policy	1. Ensure that the Organization-owned data center facility is protected with: Non-partitioned ceilings Secured entry points; and/or Manned reception desks.	1. Observe the Organization-owned data center facility to determine whether the facility is protected with: Non-partitioned ceilings Secured entry points; and/or Manned reception desks.	E-SO-01
SO-02	Site Operations	Physical Protection and Positioning of Cabling	Organization power and telecommunication lines are protected from interference, interception, and damage.	Process	Preventive	Physical and Environmental Security Policy	1. Ensure that the Organization-owned data center facility has power and telecommunication lines tagged and labelled properly to protect from interference, interception, and damage.	1. Inspect Organization-owned data center facility to determine whether power and telecommunication lines are tagged and labelled properly to protect from interference, interception, and damage.	E-SO-02
SO-03	Site Operations	Global Coordination of Critical Functions: Information Security Safeguards	Organization consistently applies information security safeguards in datacenters and campuses.	Process	Corrective	Physical and Environmental Security Policy	1. Ensure that information security safeguards are in place in datacenters and campuses including but not limited to : Access Machines at entry/exit Fire extinguishers Fire Alarms etc.	1 Observe whether information security safeguards are in place in datacenters and campuses including but not limited to : Access Machines at entry/exit Fire extinguishers Fire Alarms etc.	E-SO-03
SO-04	Site Operations	Provisioning Physical Access	Physical access provisioning to an Organization datacenter requires management approval and documented specification of: • account type (e.g., standard, visitor, or vendor) • access privileges granted • intended business purpose • visitor identification method, if applicable • temporary badge issued, if applicable • access start date • access duration	Process	Preventive	Physical and Environmental Security Policy	1. Ensure all physical access to organization data centers have management approval and documentation. 2. Ensure physical access is granted after appropriate approvals.	1. Inspect the physical security system workflow to determine whether requests for physical access required management approval and required documented specification of: •Account type (e.g., visitor, vendor, or regular). •Access privileges granted. •Intended business purpose. •Visitor identification method, if applicable. •Temporary badge issued, if applicable. •Access start date. •Access duration. 2. Inspect physical access request documentation for a sample of new physical access requests to the Organization-owned data center and data rooms to determine whether access is approved.	E-SO-08 E-SO-09
SO-05	Site Operations	De-provisioning Physical Access	Physical access that is no longer required in the event of a termination or role change is revoked. If applicable, temporary badges are returned prior to exiting facility.	Process	Preventive	Physical and Environmental Security Policy	1. Design and document a process for temporary badges being returned prior to exiting the facility. 2. Ensure access is revoked in case of employee termination or role change.	1. Inspect Physical Access Policy to determine whether it contains the requirement for temporary badges to be returned prior to exiting the facility. 2. Obtain evidence to ensure no physical access is active for the terminated employees or unnecessary physical access for employees with a change in their roles and responsibilities.	E-SO-08 E-SO-10
SO-06	Site Operations	Periodic Review of Physical Access	Organization performs physical account and access reviews on a quarterly basis; corrective action is taken where applicable.	Process	Detective	Physical and Environmental Security Policy	1. Design and document a process for physical access review and frequency. 2. Ensure access review is performed as per defined frequency and necessary action is taken, if required..	1. Inspect Organization's Physical Access Policy to determine whether requirements for physical access review are defined. 2. Inspect quarterly physical access review documentation for a sample of quarters and a sample of Organization-owned data rooms to determine whether the access review is completed, and corrective actions is documented and resolved for any access that should be revoked.	E-SO-08 E-SO-11 E-SO-12

SO-07	Site Operations	Physical Access Role Permission Authorization	Initial permission definitions, and changes to permissions, associated with physical access roles are approved by authorized personnel.	Process	Preventive	Physical and Environmental Security Policy	1. Ensure all physical access to organization data centers have management approval and documentation. 2. Ensure physical access is granted after appropriate approvals.	1 Inspect the physical security system workflow to determine whether requests for physical access require approval. 2 Inspect an approval of authorized personnel, for any initial permission or modifications of permissions, ensure they are associated to physical access roles.	E-SO-08 E-SO-09
SO-08	Site Operations	Monitoring Physical Access	Intrusion detection and video surveillance are installed at Organization datacenter locations; confirmed incidents are documented and tracked to resolution.	Process	Detective	Physical and Environmental Security Policy	1. Ensure that the Organization data center intrusion detection and video surveillance system are installed at Organization data center. 2. Ensure that event logs are used for resolution of incidents.	1. Observe the Organization data center intrusion detection and video surveillance system to determine whether intrusion detection and video surveillance systems are installed at Organization data center. 2. If applicable, for a sample of incident observe that event logs were used for the resolution of the incident.	E-SO-04 E-IR-07
SO-09	Site Operations	Surveillance Feed Retention	Surveillance feed data is retained for 90 days.	Technology	Corrective	Physical and Environmental Security Policy	1. Ensure that surveillance feed data is stored for 90 days.	1. Observe a sample of video footage showing the date and timestamp from the day of collection and one that is from 90 days before that. 2. Observe a configuration from the camera management system that shows that it is configured to retain surveillance video data for 90 days	E-SO-05
SO-10	Site Operations	Visitor Access	Physical access for visitors is managed through monitoring, maintaining records, escorting, and reviewing access monthly. Visitor access records to the facilities are kept for at least a year.	Process	Preventive	Physical and Environmental Security Policy	1. Design and document the requirement for visitor access, maintaining records, escorting, and reviewing access monthly. 2. Ensure visitor access is approved, with an escort. 3. Ensure monthly access reviews are performed. 4. Ensure retention of visitor access for at least a year.	1. Inspect Physical Access Policy to determine whether it contains the requirement for visitor access, maintaining records, escorting. and reviewing access monthly. 2. Obtain and validate evidence that visitor access is approved, with an escort. 3. Obtain and validate evidence of monthly access reviews. 4. Obtain and validate evidence of retention of visitor access for at least a year.	E-SO-08 E-SO-13 E-SO-14
SO-11	Site Operations	Physical Access Devices	Physical access devices (i.e., keys, combinations, access cards, etc.) are maintained through an inventory and restricted to authorized individuals. Appropriate devices are rotated when compromised or upon employee termination or transfer.	Process	Preventive	Physical and Environmental Security Policy	1. Ensure inventory of physical access devices is maintained. 2. Ensure access to inventory is limited to authorized personnel. 3. Ensure rotation of physical access devices when compromised, or employee termination or transfer.	1 Inspect the list of physical access devices. 2 Inspect the list of individuals who has an access to physical devices. 3 Inspect whether physical access devices were rotated when compromised or upon employee termination or transfer.	E-SO-15 E-SO-16 E-SO-17
SO-12	Site Operations	Temperature and Humidity Control	Temperature and humidity levels of datacenter environments are monitored and maintained at appropriate levels.	Technology	Detective	Physical and Environmental Security Policy	1. Ensure temperature and humidity monitoring system configurations at organization-owned data center are set to determine whether temperature and humidity levels are being monitored and configured to alert appropriate personnel when temperature or humidity levels exceed set limits. 2.Ensure that temperature and humidity alarms are generated over the threshold.	1. Inspect the temperature and humidity monitoring system and configurations at organization-owned data center to determine whether temperature and humidity levels are being monitored and configured to alert appropriate personnel when temperature or humidity levels exceed set limits. 2.Inspect the temperature and humidity alarms generated over the threshold to determine if any alarms were triggered.	E-SO-18 E-SO-19 E-SO-20
SO-13	Site Operations	Fire Suppression Systems	Emergency responders are automatically contacted when fire detection systems are activated; the design and function of fire detection and suppression systems are maintained at appropriate intervals.	Technology	Preventive	Physical and Environmental Security Policy	1. Ensure fire detection systems are in place and emergency responders are contacted, if required. 2. Ensure detection and suppression systems are tested at regular intervals.	1. Inspect Organization's Physical Security Policy, Alarm Management and System Maintenance Standard to determine whether requirements for fire detection/suppression systems are defined. 2. Observe the fire detection/suppression systems in use at the Organization-owned data center to determine whether they are in place. 3. Inspect the fire detection system monitoring contract in place to determine whether Organization has contracted with a third party to monitor fire detection systems for the Organization-owned data center. 4. Inspect fire suppression/detection certifications at the Organization owned data center to determine whether the design and function of these systems are tested at appropriate intervals.	E-SO-08 E-SO-06 E-SO-21

SO-14	Site Operations	Power Failure Protection	Organization employs uninterruptible power supplies (UPS) and generators to support critical systems in the event of a power disruption or failure. The design and function of relevant equipment is certified at appropriate intervals.	Process	Corrective	Physical and Environmental Security Policy	1. Ensure UPS and generators are employed to support critical systems in the event of a power disruption or failure. 2. Ensure that UPS and generator are certified at appropriate intervals.	1. Observe the UPS and generators at a sample of Organization-owned data center and data rooms to determine whether they are employed to support critical systems in the event of a power disruption or failure. 2. Inspect UPS and generator certifications for in-scope Organization owned-data center and data rooms to determine whether the equipment is certified at appropriate intervals.	E-SO-08 E-SO-07 E-SO-22
SO-15	Site Operations	Emergency Shutoff	Organization employs emergency power shut-off capabilities. Access to shut off power is restricted to authorized individuals.	Process	Preventive	Physical and Environmental Security Policy	1. Ensure process is documented for emergency power shut-off. 2. Ensure access to shut-off power is limited to authorized personnel.	1 Inspect documentation related to emergency power shut-off capabilities. 2 Obtain and validate a list of authorized personnel who have access to shut off power.	E-SO-08 E-SO-23
SO-16	Site Operations	Emergency Lighting	Organization employs emergency lighting in the event of a power disruption or failure. The design and function of relevant equipment is certified at appropriate intervals.	Process	Corrective	Physical and Environmental Security Policy	1. Ensure emergency lighting equipment's are tested at regular intervals.	1 Inspect certification of relevant equipment which may be used during emergency lighting in the event of a power disruption or failure.	E-SO-24
TA-01	Training and Awareness	General Security Awareness Training	Organization personnel complete security awareness training, which includes annual updates about relevant policies and how to report security events to the authorized response team. Records of training completion are documented and retained for tracking purposes.	People	Preventive	Training & Awareness Procedure	1. Ensure that the requirements for completion of security awareness training are defined in the Organization's Compliance Training Policy and Security Awareness Training Standard. 2. Ensure that the Organization's Security Awareness Training Material is well defined, documented, and up to date. 3. Ensure that there is a record of active employees and contractors maintained and updated by the organization. 4. Ensure that security awareness training is provided on a regular basis and the progress of all contractors and employees participating in the training tracked and documented..	1. Inspect Organization's Compliance Training Policy and Security Awareness Training Standard to determine whether requirements for completion of security awareness training are defined. 2. Inspect Organization's Security Awareness Training material to determine whether it details: Version history of the SAT to determine materials are updated during the audit period. How to report security events to the appropriate response team 3. Obtain the list of active employees and contractors. 4. For a sample of active employees and contractors, obtain and inspect the security awareness training completion records to determine whether training is completed annually and completion is tracked and documented.	E-TA-01 E-TA-02 E-TA-03
TA-02	Training and Awareness	Code of Conduct Training	Organization full-time and temporary employees and interns complete a code of business conduct training.	People	Preventive	Training & Awareness Procedure	1. Ensure that requirements for completion of business code of conduct training are defined with the organization's Compliance Training Policy. 2. Ensure that the training material for the Organization's Code of Business Conduct outlines the responsibilities of both full-time and temporary employees in adhering to the code. 3. Ensure employees have completed the Code of Business Conduct training as per the policy by examining training completion records for a group of new and existing employees.	1. Inspect Organization's Compliance Training Policy to determine whether requirements for completion of business code of conduct training are defined. 2. Inspect Organization's Code of Business Conduct training material to determine whether it includes Organization full-time and temporary Employees' responsibilities for adhering to the business code of conduct. 3. Inspect Code of Conduct training completion records for a selection of new and current employees to determine whether new hires and existing employees have completed Code of Business Conduct training in accordance with the policy.	E-TA-01 E-TA-02 E-TA-03

TA-03	Training and Awareness	Accessibility Training	Organization personnel complete accessibility awareness training, which includes annual updates about relevant policies and how to report accessibility events internally. Records of training completion are documented and retained for tracking purposes.	People	Preventive	Training & Awareness Procedure	1. Ensure that the training material includes information about annual updates to relevant policies and instructions on how to report accessibility events internally. 2. Ensure that well defined and documented records of training completion are maintained by the organization.	1 Inspect training material to determine whether it detailed annual updates about relevant policies and how to report accessibility events internally. 2 Inspect training completion records for a sample of employees.	E-TA-02 E-TA-03
TA-04	Training and Awareness	Phishing Awareness	Organization performs periodic phishing campaigns.	People	Preventive	Training & Awareness Procedure	1. Ensure that the organization conducts regular phishing campaigns to help employees get better at spotting and handling real phishing threats	1. Verify that the organization performs periodic phishing campaigns to evaluate and improve their employees' ability to recognize and respond to real phishing threats.	E-TA-04
TA-05	Training and Awareness	Developer Security Training	Organization's software engineers are required to complete training based on secure coding techniques on an annual basis.	People	Preventive	Training & Awareness Procedure	1. Ensure that review of the security training material includes guidance on yearly Secure Coding Training for PCI developers and software engineers. 2. Ensure that the secure coding training was provided and completed by the employees within the last 365 days. 3. Make sure that engineers are registered for the Security Engineering Training program as required.	1. Inspect the Security Training Material to validate that the standard provides guidance on annual Secure Coding Training for PCI developers and software engineers. 2. For a sample of employees obtain evidences showing secure coding training completion. Validate that the date of completion is in the last 365 days. 3. Ensure that all engineers are enrolled in the Security Engineering Training program as needed.	E-TA-02 E-TA-03
TA-06	Training and Awareness	Payment Card Processing Security Awareness Training	Organization personnel that interact with cardholder data systems receive awareness training to be aware of attempted tampering or replacement of devices. Training should include the following: • verify the identity of third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • do not install, replace, or return devices without verification • be aware of suspicious behavior around devices (e.g., attempts by unknown persons to unplug or open devices) • report suspicious behavior and indications of device tampering or substitution to authorized personnel (e.g., to a manager or security officer)	People	Preventive	Training & Awareness Procedure	1. Ensure that the training materials to check if they cover the following topics: • Confirming the identity of third-party repair or maintenance personnel before giving them access to devices. • Not making changes or returning devices without proper verification. • Being alert to unusual behavior around devices, like unauthorized attempts to tamper with them. • Reporting any suspicious behavior or signs of device tampering to authorized personnel, such as a manager or security officer.	1 Inspect training material to determine whether it detailed: • verify the identity of third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • do not install, replace, or return devices without verification • be aware of suspicious behavior around devices (e.g., attempts by unknown persons to unplug or open devices) • report suspicious behavior and indications of device tampering or substitution to authorized personnel (e.g., to a manager or security officer) 2 Inspect training completion records for a selection of employees.	E-TA-02 E-TA-03

TA-07	Training and Awareness	Role-based Security Training: HIPAA	Organization personnel with access to personal health information (PHI) are required to attend and complete HIPAA privacy training.	People	Preventive	Training & Awareness Procedure	1. Ensure access to sensitive information including (PHI) is given to limited employees (based on roles and responsibilities) and records for the same shall be maintained. 2. Ensure all employee that accesses PHI shall complete mandatory training of HIPAA security and privacy. 3. Training records for the same needs to be maintained for tracking purpose.	1. Inspect the population of Organization personnel who have access to PHI. 2. Inspect completion records for a sample of employees with access to PHI, for evidence that the employees had completed HIPAA security and privacy training.	E-TA-05 E-TA-03
TA-08	Training and Awareness	Role-based Security Training	Organization personnel with key security responsibilities complete relevant role-based training on an annual basis: • personnel must complete training prior to obtaining access to privileged security systems • personnel with contingency responsibilities must complete role-based training within 10 days of assuming the role • records of training completion are documented and retained for tracking purposes	People	Preventive	Training & Awareness Procedure	1. Ensure role-based training material contains details around key security responsibilities. 2. Training records for each employee shall be maintained for future tracking.	1 Inspect training material to determine whether it detailed key security responsibilities relevant to role-based trainings. 2 Inspect training completion records for a sample of employees.	E-TA-02 E-TA-03
TA-09	Training and Awareness	Security Champion Training	Service teams select a "Security Champion" to ensure security engagement responsibilities are assigned and tracked to completion; Security Champions receive training on how to execute responsibilities.	People	Preventive	Training & Awareness Procedure	1. Ensure there is a process by which the service teams select a "Security Champion" and they complete their security champions training. 2. Maintain training records for the Security Champions.	1. Inspect documentation related to Security Champions and verify that they are defined for selected service teams. 2. Inspect training completion records for a sample of Security Champions.	E-TA-02 E-TA-03
TPM-01	Third-Party Management	Third-Party Assurance Review	On a periodic basis, management reviews controls within third-party assurance reports to ensure that they meet organizational requirements; if control gaps are identified in the assurance reports, management takes action to address impact the disclosed gaps have on the organization.	Process	Detective	Vendor Information Security Policy	1. Ensure there is a documented procurement policy and information security standard which consists information that includes but not limited to third-party assurance reviews. 2. Ensure a formal questionnaire is prepared, which will be used for assessing third-party risks during the onboarding process. 3. Ensure there is an action plan for control gaps identified at the time of vendor security review for their third-party controls.	1. Inspect Organization Procurement Policy and Vendor Information Security Standard to determine whether requirements for third-party assurance reviews are defined. 2. Observe Organization Risk Assessment system to determine whether a questionnaire for systematically assessing third-party risks is defined. 3. For a sample of vendors, inspect whether the corresponding Vendor Security Review (VSR) is completed to determine whether management has assessed the third party's controls to determine Organization requirements are met and management took action on control gaps as applicable.	E-TPM-01 E-TPM-07 E-TPM-02 E-TPM-03
TPM-02	Third-Party Management	Vendor Risk Management	Organization performs a risk assessment to determine the data types that can be shared with a managed service provider.	Process	Preventive	Vendor Information Security Policy	1. Ensure there is process to conduct vendor security review and all vendors must go through the review; records for documentation and risk rating needs to be maintained.	1. Validate for a sample for service providers that an assessment was conducted and a risk rating is assigned to them as part of the VSR process. 2. Validate that the vendors are listed in the vendor management tool	E-TPM-04
TPM-03	Third-Party Management	Forensic Investigations	Organization enables procedures to conduct a forensic investigation in the event that a hosted merchant or service provider is compromised.	Process	Preventive	Vendor Information Security Policy	1. Ensure there is documented process for conducting a forensic investigation in the event when a hosted merchant or service provider is compromised. 2. Ensure documentation for the same needs to be maintained for tracking purposes and corrective actions.	1. Inspect documentation to determine whether procedures to conduct a forensic investigation in the event when a hosted merchant or service provider is compromised, are defined. 2. For sample investigations validate whether appropriate documentation is retained.	E-TPM-05 E-TPM-06
TPM-04	Third-Party Management	Privacy Risk Assessment	Organization reviews the privacy practices of service providers who access, collect, process, transfer, or store personal information on Organization's behalf upon initial procurement and renewal; non-compliance is tracked through remediation.	Process	Corrective	Vendor Information Security Policy	1. Ensure that a process is defined and documented to review the privacy practices of service providers who access, collect, process, transfer, or store personal information on Organization's behalf. 2. Ensure that the reviews are conducted at the time of initial procurement and at renewal. 3. Ensure that any non-compliances are tracked to remediation.	1. Inspect and validate that a process is defined and documented to review the privacy practices of service providers who access, collect, process, transfer, or store personal information on Organization's behalf. 2. Validate for a sample vendor that the reviews are conducted at the time of initial procurement and at renewal. 3. Validate for a sample non-compliance event that it was tracked to remediation.	E-TPM-07 E-TPM-08 E-TPM-09

TPM-05	Third-Party Management	Network Access Agreement: Vendors	Third-party entities which gain access to the Organization network sign a network access agreement.	Process	Preventive	Vendor Information Security Policy	1. Ensure that all third-party vendors sign the network access agreement before accessing the organization's network.	1. For a sample of vendors validate whether a signed Network Security Agreement Exists prior to onboarding.	E-TPM-10
TPM-06	Third-Party Management	Vendor Non-disclosure Agreements	Agency temporary workers, independent contractors, and third-party entities consent to a non-disclosure clause.	Process	Preventive	Vendor Information Security Policy	1. Ensure that a process is defined and documented for all agency temporary workers and independent contractors to sign a non-disclosure clauses before accessing the organization's network.	1. Obtain listings of agency temporary workers and independent contractors from the Contingent Workforce team 2. For a sample of agency temporary workers, independent contractors, inspect Agreement to determine that non-disclosure clause is acknowledged.	E-TPM-11
TPM-07	Third-Party Management	Cardholder Data Security Agreement	Organization managed service providers that manage, store, or transmit cardholder data on behalf of the customer must provide written acknowledgement to customers of their responsibility to protect cardholder data and the cardholder data environment.	Process	Preventive	Vendor Information Security Policy	1. Ensure that a process is defined and documented for all the managed service providers that manage, store, or transmit cardholder data on behalf of the customer to provide a written acknowledgement to customers of their responsibility to protect cardholder data and the cardholder data environment.	1. Validate for a sample Managed Service Provider that they have provided acknowledgement to customers of their responsibility to protect cardholder data and the cardholder data environment.	E-TPM-12
TPM-08	Third-Party Management	HIPAA Business Associate Agreement	Organization Business Associate Agreements must contain provisions for the following: • permitted uses and disclosures of Protected Health Information (PHI) • PHI safeguards to prevent unauthorized use or disclosure • communications regarding the unauthorized use or disclosure of PHI • PHI availability • contract termination and disposition of PHI	Process	Preventive	Vendor Information Security Policy	1. Ensure there is a documented business associate agreement which includes clauses but not limited to : • permitted uses and disclosures of Protected Health Information (PHI) • PHI safeguards to prevent unauthorized use or disclosure • communications regarding the unauthorized use or disclosure of PHI • PHI availability • contract termination and disposition of PHI 2. Ensure that a process is defined for all business associates to sign and acknowledge to this agreement	1. Inspect Organization's Business Associate Agreements and validate that it includes the following: • permitted uses and disclosures of Protected Health Information (PHI) • PHI safeguards to prevent unauthorized use or disclosure • communications regarding the unauthorized use or disclosure of PHI • PHI availability • contract termination and disposition of PHI 2. For a sample business associate validate that they have signed the said agreement.	E-TPM-13
TPM-09	Third-Party Management	HIPAA Business Associate Subcontractor Agreement	Organization requires a Business Associate Subcontractor Agreement with Business Associates from which it receives or transmits protected health information (PHI); Business Associates under contract are required to provide assurance that they adhere to Organization's security standards, which includes the security of PHI and reporting security events that potentially expose PHI.	Process	Preventive	Vendor Information Security Policy	1. Ensure there is a documented business associate subcontractor agreement which includes, but not limited to: security of PHI and reporting of security events that potentially exposes PHI. 2. Ensure that all business associates are under this agreement and provide assurance that they adhere to Organization's security standards.	1. Inspect Organization's Business Associate Subcontractor Agreement document. 2. Inspect an executed agreement for Organization's Business Associate, for evidence that Business Associates provide Assurance that they comply with Organization's security standards, which includes the security of PHI and reporting security events that potentially expose PHI.	E-TPM-14
TPM-10	Third-Party Management	Network Service Level Agreements (SLA)	Vendors providing networking services to Organization are contractually bound to provide secure and available services as documented in SLAs.	Process	Preventive	Vendor Information Security Policy	1. Ensure that a process is defined and documented for ensuring SLA in case of network services. 2. Ensure appropriate contracts are created with network service providers to ensure availability of network services. 3. Ensure appropriate monitoring is enabled to identify any network downtime and SLA breaches.	1. Inspect and a validate that a process is defined and documented for ensuring SLA in case of network services. 2. Validate for a sample vendor that contracts are created to ensure availability of network services. 3.Validate monitoring configuration to confirm that it is enabled to identify any network downtime and SLA breaches.	E-TPM-15 E-TPM-16
TPM-11	Third-Party Management	Personal Information Processing and Transfer Agreement	Appropriate data processing and transfer agreements are established for the collection, processing, transfer, or storage of personal information by, or on behalf of, Organization.	Process	Preventive	Vendor Information Security Policy	1. Ensure that a process is defined and documented for establishing data processing and transfer agreements for the collection, processing, transfer, or storage of personal information by, or on behalf of, the Organization. 2. Ensure these agreements are signed and retained appropriately as per organization's policy.	1. Inspect and validate that a process is defined and documented for establishing data processing and transfer agreements for the collection, processing, transfer, or storage of personal information by, or on behalf of, the Organization. 2. Validate for a sample agreement that it is signed and retained appropriately as per organization's policy.	E-TPM-17
TPM-12	Third-Party Management	Approved Service Provider Listing	Organization maintains a list of approved managed service providers and the services they provide to Organization.	Process	Preventive	Vendor Information Security Policy	1. Ensure there is a documented process for vendor onboarding and termination. 2. Ensure that activities for vendor onboarding and offboarding are logged and maintained appropriately. 3. Ensure that the list of active vendors is reviewed and updated periodically.	1. Inspect and validate that there is a documented process for vendor onboarding and termination. 2. Validate that activities for vendor onboarding and offboarding are logged and maintained appropriately. 3. Validate the list of active vendors and verify that it is reviewed and updated periodically.	E-TPM-18

TPM-13	Third-Party Management	Vendor Information Security Standard	Organization has documented a Vendor Information Security Standard that defines the responsibilities and governance requirements regarding vendor information security engagements. Contractual agreements are entered into with vendors who process or store Organization data that define information Security terms and service level agreements.	Process	Preventive	Vendor Information Security Policy	1. Ensure there is documented vendor information security standard which is available on intranet for employees. 2. Ensure vendor information security standard defines the responsibilities and governance requirements regarding vendor information security engagements. 3. Ensure appropriate agreements are established with vendors who process or store Organization data.	1. Inspect and validate that there is a documented vendor information security standard which is available on intranet for employees. 2. Validate vendor information security standard defines the responsibilities and governance requirements regarding vendor information security engagements. 3. For a sample vendor validate that agreements are established.	E-TPM-07 E-TPM-19
VM-01	Vulnerability Management	Vulnerability Scans	Organization conducts vulnerability scans against the production environment; scan tools are updated prior to running scans.	Process	Detective	Vulnerability Management Policy	1. Ensure that the requirements for periodic vulnerability scans are defined and documented. 2. Ensure a process is established for updating the scanning tool version prior to running the scan.	1. Review Vulnerability Management policy and/or standard to validate that they define requirements for periodic vulnerability scans. 2. Inspect scanning tool version information to ensure they are up to date. 3. Validate evidence for a sample of service production hosts/accounts to ensure that vulnerability scans are conducted and tickets are created as appropriate.	E-VM-01 E-VM-02 E-VM-03
VM-02	Vulnerability Management	Vulnerability Scans: Cardholder Data Environment	Vulnerability scans are conducted against cardholder environments at least quarterly or after significant change; critical vulnerability resolution is confirmed via a rescan.	Process	Detective	Vulnerability Management Policy	1. Ensure that the requirements for quarterly vulnerability scans against cardholder data environement are defined and documented. 2. Ensure a process is established to initiate a scan after every significant change. 3. Ensure all critical vulnerabilities are tracked to resolution and confirmed via a rescan	1. Inspect and validate whether the requirements for quarterly vulnerability scans against cardholder data environement are defined and documented. 2. Validate that a process is established to initiate a scan after every significant change. 3. Validate for a sample critical vulnerability whether it was tracked to resolution and confirmed via a rescan	E-VM-01 E-VM-04
VM-03	Vulnerability Management	Vulnerability Scans: Audit Log Review	When vulnerabilities are identified, Organization analyzes audit logs to see if it has been previously exploited. Identified exploitations are resolved through incident management.	Process	Detective	Vulnerability Management Policy	1. Ensure that a process is defined and documented to verify the exploitability of a vulnerability via audit logs. 2. Ensure all identified exploitations are resolved through the incident management process.	1. Inspect and validate that a process is defined and documented to verify the exploitability of a vulnerability via audit logs. 2. Validate for a sample exploitation that it was resolved through the incident management process.	E-VM-01 E-VM-05
VM-04	Vulnerability Management	Vulnerability Scans: Trend Analysis	Organization reviews vulnerability trends over time to include in risk assessments; high and moderate risk vulnerabilities are remediated in 30 and 90 days, respectively.	Process	Corrective	Vulnerability Management Policy	1. Ensure that a process has been defined and documented for reviewing vulnerability trends. 2. Ensure that appropriate SLAs are defined to remediate high and moderate vulnerabilities in 30 and 90 days. 3. Ensure the results of these reviews are included in risk assessments.	1. Inspect and validate that a process has been defined and documented for reviewing vulnerability trends. 2. Validate that appropriate SLAs are defined to remediate high and moderate risk vulnerabilities in 30 and 90 days. 3. For a sample of vulnerabilities, validate whether medium and high risk vulnerabilities were remediated within the SLA.	E-VM-01 E-VM-06
VM-05	Vulnerability Management	Approved Scanning Vendor	At least quarterly, Organization engages an Approved Scanning Vendor (ASV) to conduct external vulnerability scans.	Process	Detective	Vulnerability Management Policy	1. Ensure a process has been defined and documented to conduct ASV scans for PCI envrionments every 90 days. 2. Ensure all findings are remediated and re-scanning is done to maintain compliance.	1. Inspect and validate whether a process has been defined and documented to conduct ASV scans for PCI envrionments every 90 days. 2. Validate for a sample quarter that, if applicable, all findings were remediated and re-scan was done to maintain compliance.	E-VM-01 E-VM-07
VM-06	Vulnerability Management	Application Penetration Testing	Organization conducts penetration tests periodically.	Process	Detective	Vulnerability Management Policy	1. Ensure that a process has been defined and documented for conducting penetration tests. 2. Ensure the results of the penetration tests are appropriately documented and tracked till remediation.	1. Inspect and validate whether a process has been defined and documented for conducting penetration tests. 2. Validate the results of last penetration test and verify whether the findings were tracked till remediation.	E-VM-01 E-VM-08

VM-07	Vulnerability Management	Application Penetration Testing: Cardholder Data Environment	Organization conducts penetration tests against cardholder data environments (CDE) and includes the following requirements: • testing covers the entire CDE perimeter and critical data systems • testing verifies that CDE perimeter segmentation is operational • testing is performed from both inside and outside the CDE network • testing validates segmentation and scope-reduction controls (e.g., tokenization processes) • network layer penetration tests include components that support network functions as well as operating systems • at the application level, testing provides coverage, at a minimum, against the security testing requirements defined in VM-05-01 (01) • testing is performed with consideration of threats verified in the last 12 months from external alerts, directives, and advisories defined in VM-06-02 • testing is performed with consideration of vulnerabilities reported through Organization's PSIRT process within the last 12 months • risk ratings are assigned to discovered	Process	Detective	Vulnerability Management Policy	1. Ensure that a process has been defined and documented for conducting penetration tests for the Card Holder Data Environments. 2. Ensure that the testing covers the following requirements: • testing covers the entire CDE perimeter and critical data systems • testing verifies that CDE perimeter segmentation is operational • testing is performed from both inside and outside the CDE network • testing validates segmentation and scope-reduction controls (e.g., tokenization processes) • network layer penetration tests include components that support network functions as well as operating systems • at the application level, testing provides coverage, at a minimum, against the security testing requirements defined in VM-05-01 (01) • testing is performed with consideration of threats verified in the last 12 months from external alerts, directives, and advisories defined in VM-06-02 • testing is performed with consideration of vulnerabilities reported through Organization's PSIRT process within the last 12 months • risk ratings are assigned to discovered vulnerabilities, which are tracked through remediation	1. For PCI in-scope services, obtain and inspect evidence to show that external pen test, internal pen test, and segmentation tests were performed appropriately. 2. Validate the pen test reports documented the below mentioned requirements: • testing covers the entire CDE perimeter and critical data systems • testing verifies that CDE perimeter segmentation is operational • testing is performed from both inside and outside the CDE network • testing validates segmentation and scope-reduction controls (e.g., tokenization processes) • network layer penetration tests include components that support network functions as well as operating systems • at the application level, testing provides coverage, at a minimum, against the security testing requirements defined in VM-05-01 (01) • testing is performed with consideration of threats verified in the last 12 months from external alerts, directives, and advisories defined in VM-06-02 • testing is performed with consideration of vulnerabilities reported through Organization's PSIRT process within the last 12 months • risk ratings are assigned to discovered vulnerabilities, which are tracked through remediation	E-VM-01 E-VM-08
VM-08	Vulnerability Management	Infrastructure Patch Management	Organization installs security-relevant patches, including software or firmware updates; identified end-of-life software must have a documented decommission plan in place.	Process	Preventive	Infrastructure Management Policy	1. Ensure that a process for patch management and end-of-life requirements is defined and documented. 2. Ensure that patch updates are implemented for all compute resources. 3. Ensure all end-of-life software are decommissioned with a documented plan.	1. Inspect and validate that a process for patch management and end-of-life requirements is defined and documented. 2. For a sample of servers/virtual machine validate that patch updates are implemented. 3. For a sample of end-of-life software validate that it was decommissioned with a documented plan.	E-VM-09 E-VM-10 E-VM-11
VM-09	Vulnerability Management	Enterprise Antivirus	Organization has managed enterprise antivirus deployments to detect and respond to malicious activities.	Technology	Corrective	Vulnerability Management Policy	1. Ensure a process has been defined and documented for deploying antivirus to detect and respond to malicious activities. 2. Ensure that antivirus is deployed on all applicable systems.	1. Inspect and validate whether a process has been defined and documented for deploying antivirus to detect and respond to malicious activities. 2. For a sample system validate that antivirus is deployed.	E-VM-01 E-VM-12
VM-10	Vulnerability Management	Enterprise Antivirus Tampering	Antivirus mechanisms cannot be disabled or altered by users unless specifically authorized by management.	Process	Corrective	Vulnerability Management Policy	1. Ensure that appropriate policies are configured to prevent users from disabling or altering antivirus mechanisms.	1. Validate whether appropriate policies are configured to prevent users from disabling or altering antivirus mechanisms.	E-VM-13
VM-11	Vulnerability Management	Enterprise Antivirus Scope	Vulnerability scans are periodically performed on systems that do not require anti-virus; management determines if anti-virus should be required on the system based on scan results and associated risk.	Process	Corrective	Vulnerability Management Policy	1. Ensure a process is defined and documented to perform vulnerability scans on all systems. 2. Ensure the process identifies systems on which antivirus should be deployed.	1. Inspect and validate a process is defined and documented to perform vulnerability scans on all systems. 2. Validate whether the scan identifies systems on which antivirus should be deployed.	E-VM-01 E-RM-02
VM-12	Vulnerability Management	Maintenance Tools: Inspect Media	Organization checks media containing diagnostic and test programs for malicious code before the media are used in production systems.	Process	Detective	Vulnerability Management Policy	1. Ensure a process has been defined and documented to check media with diagnostic and test programs before using in production. 2. Ensure that only media without any malicious code are used in production.	1. Inspect and validate that a process has been defined and documented to check media with diagnostic and test programs before using in production. 2. Validate using logs and scan results that only media without any malicious code were used in production.	E-VM-01 E-VM-14
VM-13	Vulnerability Management	Code Security Check	Organization conducts periodic source code checks for vulnerabilities.	Process	Detective	Secure Development Lifecycle Policy	1. Ensure a process has been defined and documented for performing source code check for vulnerabilities. 2. Ensure all vulnerabilities are tracked and resolved as per organization's SLA.	1. Inspect and validate whether a process has been defined and documented for performing source code check for vulnerabilities. 2. For a sample source code vulnerability validate that it was tracked and resolved per SLA.	E-VM-15 E-RM-02

VM-14	Vulnerability Management	Code Security Check: Cardholder Data Environment	Where applicable, security testing performed prior to releasing code into production includes the following: • code injection • buffer overflows • insecure cryptographic storage • insecure communications • improper error handling • high-risk vulnerabilities • cross-site scripting • improper access control • cross-site request forgery • broken authentication session management	Process	Detective	Secure Development Lifecycle Policy	1. Ensure a process has been defined and documented for performing source code check for vulnerabilities. 2. Ensure the following aspects are covered as part of the testing: • code injection • buffer overflows • insecure cryptographic storage • insecure communications • improper error handling • high-risk vulnerabilities • cross-site scripting • improper access control • cross-site request forgery • broken authentication session management 3. Ensure all vulnerabilities are tracked and resolved as per organization's SLA.	1. Inspect and validate whether a process has been defined and documented for performing source code check for vulnerabilities. 2. Validate for a sample scan whether the following aspects were covered as part of the testing: • code injection • buffer overflows • insecure cryptographic storage • insecure communications • improper error handling • high-risk vulnerabilities • cross-site scripting • improper access control • cross-site request forgery • broken authentication session management 3. For a sample source code vulnerability validate that it was tracked and resolved per SLA.	E-VM-15 E-RM-02
VM-15	Vulnerability Management	Third-Party Library Check	Organization scans third-party libraries for vulnerabilities according to the service risk rating assignment.	Technology	Detective	Secure Development Lifecycle Policy	1. Ensure a process has been defined and documented for performing source code check for vulnerabilities. 2. Ensure that third-party libraries are scanned for vulnerabilities as per service risk rating assignment. 3. Ensure all vulnerabilities are tracked and resolved as per organization's SLA.	1. Inspect and validate whether a process has been defined and documented for performing source code check for vulnerabilities. 2. Validate for a sample scan whether third-party libraries are scanned for vulnerabilities as per service risk rating assignment. 3. For a sample source code vulnerability validate that it was tracked and resolved per SLA.	E-VM-15 E-RM-02
VM-16	Vulnerability Management	Non-disclosure of Error Detail	Information systems are designed to ensure error messages generated provide adequate information for taking corrective action without revealing sensitive information.	Technology	Preventive	Secure Development Lifecycle Policy	1. Ensure that a process is defined to design Information systems in such a way that error messages generated provide adequate information for taking corrective action without revealing sensitive information.	1. Inspect the type of error messages configured in a sample of applications. 2. Ensure no sensitive data or user information is provided via error messages. Additionally, ensure appropriate corrective actions are highlighted in the error message.	E-VM-15 E-VM-16
VM-17	Vulnerability Management	Embedded Authenticators	Quality Engineering checks to ensure that static passwords are not embedded within application source code or access scripts, prior to deployment on the Organization network.	Process	Detective	Secure Development Lifecycle Policy	1. Ensure a process has been defined and documented for performing source code check for vulnerabilities. 2. Ensure that static passwords are not embedded within application source code or access scripts, prior to deployment on the Organization network. 3. Ensure all vulnerabilities are tracked and resolved as per organization's SLA.	1. Inspect and validate whether a process has been defined and documented for performing source code check for vulnerabilities. 2. Validate for a sample scan whether a check was done so that static passwords are not embedded within application source code or access scripts, prior to deployment on the Organization network. 3. For a sample source code vulnerability validate that it was tracked and resolved per SLA.	E-VM-15 E-RM-02
VM-18	Vulnerability Management	External Information Security Inquiries	Organization reviews information-security-related inquiries, complaints, and disputes.	Process	Preventive	Incident Management Policy	1. Ensure a process has been defined and documented to receive information related inquiries, complaints, and disputes. 2. Ensure all of the received inquiries, disputes, and compliants are reviewed and resolved as applicable.	1. Inspect and validate that a process has been defined and documented to receive information related inquiries, complaints, and disputes. 2. Validate for a sample query that it was reviewed and resolved as applicable.	E-IR-02 E-VM-17
VM-19	Vulnerability Management	External Alerts and Advisories	Organization reviews alerts and advisories from management approved security forums and communicates verified threats to authorized personnel.	Process	Preventive	Incident Management Policy	1. Ensure that a process has been defined and documented to review alerts and advisories from approved security forums. 2. Ensure that management reviews the list of approved security forums and updates accordingly. 3. Ensure all verified threats are communicated to authorized personnel and tracked to resolution	1. Inspect and validate that a process has been defined and documented to review alerts and advisories from approved security forums. 2. Validate whether the management reviews the list of approved security forums and updates accordingly using last update evidence. 3. Validate communication and resolution evidence for a sample of verified threats.	E-IR-02 E-VM-18 E-VM-19

VM-20	Vulnerability Management	Third-Party Security Assessment	Organization engages qualified managed service providers to perform independent information security assessments.	Process	Detective	Information Security Management Standard	1. Ensure a process has been defined and documented to engage qualified managed service providers for performing independent information security assessments. 2. Ensure these assessments are performed in accordance with organization requirements.	1. Inspect and valudate whether a process has been defined and documented to engage qualified managed service providers for performing independent information security assessments. 2. Validate whether these assessments were performed in accordance with organization requirements.	E-SG-01 E-VM-20
VM-21	Vulnerability Management	Security Testing Window	Security administrators notify relevant parties prior to executing technical security assessments; assessment details and results are documented in a ticket.	Process	Preventive	Vulnerability Management Policy	1. Ensure a process has been defined and documented to notify relevant parties before executing technical security assessments. 2. Ensure all assessment details and results are appropriately documented.	1. Inspect and validate whether a process has been defined and documented to notify relevant parties before executing technical security assessments. 2. Validate for a sample assessment whether details and results were appropriately documented. 3. Also validate whether appropriate notification was sent to all relevant parties prior to executing the assessment.	E-VM-01 E-VM-21
VM-22	Vulnerability Management	Vulnerability Remediation	Organization assigns a risk rating to identified vulnerabilities and prioritizes remediation of legitimate vulnerabilities according to the assigned risk.	Process	Corrective	Vulnerability Management Policy	1. Ensure a process has been defined and documented for assigning risk rating to all identified vulnerabilities. 2. Ensure vulnerabilities are remediated and prioritized as per the risk rating.	1. Inspect and validate whether a process has been defined and documented for assigning risk rating to all identified vulnerabilities. 2. Validate for a sample of vulnerabilities whether they were remediated as per their risk rating.	E-VM-01 E-VM-20
VM-23	Vulnerability Management	Backlog Prioritization	Organization documents identified bugs, prioritize bug fixes according to risk, and tracks resolution as part of the product release cycle.	Process	Corrective	Vulnerability Management Policy	1. Ensure a process has been defined and documented for creating documentation for identified bugs. 2. Ensure all identified bugs are fixed according to risk and are tracked till resolution	1. Inspect and validate that a process has been defined and documented for creating documentation for identified bugs. 2. Validate for a sample of all identified bugs whether they were fixed according to risk and were tracked till resolution	E-VM-01 E-VM-22

Reference #	Evidence Domain	Evidence Title
E-AM-01	Asset Management	Asset Management Policy
E-AM-02	Asset Management	Asset Inventory
E-AM-03	Asset Management	Asset Reconciliation Records
E-AM-04	Asset Management	Network Discovery Scan Records
E-AM-05	Asset Management	Evidence of Media Snapshots
E-AM-06	Asset Management	Asset Movement Records
E-AM-07	Asset Management	Portable Media Configuration Evidence
E-AM-08	Asset Management	Asset Maintenance Records
E-AM-09	Asset Management	Payment Card Device Verification Records
E-AM-10	Asset Management	Hardware Installation Records
E-AM-11	Asset Management	Software Bill of Materials
E-BC-01	Business Continuity	Business Continuity Policy
E-BC-02	Business Continuity	Business Continuity Plan
E-BC-03	Business Continuity	Business Continuity/Disaster Recovery Test Results
E-BC-04	Business Continuity	Business Impact Analysis Documentation
E-BC-05	Business Continuity	Capacity Planning Meeting Minutes
E-BM-01	Backup Management	Backup Management Policy
E-BM-02	Backup Management	Backup Restoration Test Results
E-BM-03	Backup Management	Evidence of Failed Backup Review
E-BM-04	Backup Management	Backup Configuration Evidence
E-BM-05	Backup Management	Alternate Telecommunications Agreement
E-BM-06	Backup Management	Sample Alerts for Backup Failure
E-BM-07	Backup Management	Backup Configuration Evidence
E-CFM-01	Configuration Management	Firewall standard
E-CFM-02	Configuration Management	Configuration Management Standard
E-CFM-03	Configuration Management	Periodic Rule review documentation
E-CFM-04	Configuration Management	System generated Latest patch versioning documentation
E-CFM-05	Configuration Management	Configuration deviation samples
E-CFM-06	Configuration Management	Security hardening standard
E-CFM-07	Configuration Management	Authorized application/software listing
E-CFM-08	Configuration Management	List of denied activities on information systems
E-CFM-09	Configuration Management	Review history documentation
E-CFM-10	Configuration Management	Information systems activity logs

E-CFM-11	Configuration Management	Security hardening and configuration baselines checks review documentation
E-CFM-12	Configuration Management	Sample of device log reconciliation with Asset register
E-CFM-13	Configuration Management	NTP Server configuration
E-CFM-14	Configuration Management	Sample server configuration
E-CFM-15	Configuration Management	NTP server logs
E-CFM-16	Configuration Management	Logical Access Management Standard
E-CFM-17	Configuration Management	Access Review Records
E-CFM-18	Configuration Management	Sample of server logs
E-CFM-19	Configuration Management	Sample of collaborative computing device logs
E-CFM-20	Configuration Management	Authorized approval matrix
E-CFM-21	Configuration Management	Change Management Standard
E-CFM-22	Configuration Management	Sample of change requests
E-CFM-23	Configuration Management	Sample of documented approval on production job changes
E-CFM-24	Configuration Management	Sample of documented change monitoring details
E-CHM-01	Change Management	Change Management Policy
E-CHM-02	Change Management	Change Management Tool Configuration
E-CHM-03	Change Management	Change Records
E-CHM-04	Change Management	Company Website Link
E-CMS-01	Customer Managed Security	Customer capabilities in access management console
E-CMS-02	Customer Managed Security	Customer Authentication Standard
E-CMS-03	Customer Managed Security	Customer Admin Console
E-CMS-04	Customer Managed Security	Customer contracts and agreements
E-CMS-05	Customer Managed Security	Privileged User Roles capabilities
E-CRY-01	Cryptography	List of approved key storage solutions
E-CRY-02	Cryptography	Periodic Access Review documentation
E-CRY-03	Cryptography	Sample of Key rotation evidence
E-CRY-04	Cryptography	Key Management Standard
E-CRY-05	Cryptography	Sample key custodian acknowledgement form
E-CRY-06	Cryptography	Data Classification and Handling Standard
E-CRY-07	Cryptography	Data Encryption Standard
E-CRY-08	Cryptography	Latest TLS Version evidence
E-CRY-09	Cryptography	Digital Certificates Validity
E-CRY-10	Cryptography	Qualys SSL Labs Scan Results
E-CRY-11	Cryptography	Load Balancer Configuration

E-CRY-12	Cryptography	Security Group Configuration
E-CRY-13	Cryptography	Remediation & Tracking of expired SSL
E-CRY-14	Cryptography	Sample confirmation on databases/storage location list
E-CRY-15	Cryptography	Evidence of encryption enabled
E-CRY-16	Cryptography	List of cloud storage resources
E-CRY-17	Cryptography	Access List of Key Repository
E-CRY-18	Cryptography	Review history of authorized key stores list
E-CRY-19	Cryptography	Process documentation for Decryption key storage
E-CRY-20	Cryptography	Sample of signed Key Custodian Acknowledgements
E-CRY-21	Cryptography	Sample of SSL Test results
E-CRY-22	Cryptography	SSL Configuration Files
E-CRY-23	Cryptography	Software Development Lifecycle Policy
E-CRY-24	Cryptography	Configuration evidence for accessing software signing keys
E-DM-01	Data Management	Data Management Policy
E-DM-02	Data Management	Periodic Review Records
E-DM-03	Data Management	Data Categorization Evidence
E-DM-04	Data Management	Terms of Service
E-DM-05	Data Management	Consent Records
E-DM-06	Data Management	Terms of Service Update Process
E-DM-07	Data Management	Data Access Request Records
E-DM-08	Data Management	Data Deletion Request Records
E-DM-09	Data Management	Privacy inquiry Records
E-DM-10	Data Management	Sample Test Data
E-DM-11	Data Management	Access or update process document
E-DM-12	Data Management	Personal information access/update request records
E-DM-13	Data Management	Database Screenshots
E-DM-14	Data Management	PAN authorization records
E-DM-15	Data Management	Personal Information Media Inventory
E-DM-16	Data Management	Integrity Checks
E-DM-17	Data Management	Media Erasure records
E-DM-18	Data Management	Sanitization Procedures Testing Records
E-DM-19	Data Management	Personal Information Deletion Records

E-DM-20	Data Management	Temporary Files deletion configuration
E-DM-21	Data Management	Sample Alerts showcasing restricted data via public websites is prohibited
E-DM-22	Data Management	DLP Configuration
E-DM-23	Data Management	Configuration for posting on Public Websites
E-EM-01	Entity Management	Board of directors charter
E-EM-02	Entity Management	Board of directors meetings minutes
E-EM-03	Entity Management	List of members on the audit committee
E-EM-04	Entity Management	Audit committee charter
E-EM-05	Entity Management	Audit Committee meeting minutes
E-EM-06	Entity Management	Evidence of follow up items or action plans
E-EM-07	Entity Management	Documented corporate strategy in the Information Security policy
E-EM-08	Entity Management	Operating plan procedure/process
E-EM-09	Entity Management	Evidence showcasing the plans are communicated to the stakeholders (MOM)
E-EM-10	Entity Management	Latest Cyber Security Insurance
E-EM-11	Entity Management	Latest MOM of audit committee
E-EM-12	Entity Management	Internal audit plan
E-EM-13	Entity Management	Internal audit report
E-EM-14	Entity Management	Minutes of meeting showcasing the Internal financial control assessment results
E-EM-15	Entity Management	Minutes of meeting showcasing the security compliance status and issues identified
E-EM-16	Entity Management	Minutes of meeting showcasing the security compliance results
E-EM-17	Entity Management	Organization's control set
E-EM-18	Entity Management	Customer service agreement
E-IAM-01	Identity and Access Management	Logical Access Policy
E-IAM-02	Identity and Access Management	Access Management Portal Workflow
E-IAM-03	Identity and Access Management	Access Provisioning Logs
E-IAM-04	Identity and Access Management	Access Modification Logs
E-IAM-05	Identity and Access Management	Sample alert for Access Modification
E-IAM-06	Identity and Access Management	Access Termination Logs
E-IAM-07	Identity and Access Management	Access De-Provisioning Logs
E-IAM-08	Identity and Access Management	Access Review Reconciliation
E-IAM-09	Identity and Access Management	Corrective Action in Access Management Portal
E-IAM-10	Identity and Access Management	Shared secret rotation evidence
E-IAM-11	Identity and Access Management	Password Change evidence
E-IAM-12	Identity and Access Management	List of User IDs

E-IAM-13	Identity and Access Management	Access to IAM groups
E-IAM-14	Identity and Access Management	Configuration showing 90 days termination
E-IAM-15	Identity and Access Management	Configuration showing trigger is configured
E-IAM-16	Identity and Access Management	Password Policy
E-IAM-17	Identity and Access Management	Existing User listing
E-IAM-18	Identity and Access Management	Password policy from console
E-IAM-19	Identity and Access Management	Remote Access Standard
E-IAM-20	Identity and Access Management	VPN Connection walkthrough
E-IAM-21	Identity and Access Management	System config for Multi Factor Authentication
E-IAM-22	Identity and Access Management	Access Reset process
E-IAM-23	Identity and Access Management	Session timeout config for server
E-IAM-24	Identity and Access Management	Access Management Policy
E-IAM-25	Identity and Access Management	Active Directory Screenshot
E-IAM-26	Identity and Access Management	Account lockout parameters
E-IAM-27	Identity and Access Management	Sample configuration screenshot from Federal Systems
E-IAM-28	Identity and Access Management	Sample error information
E-IAM-29	Identity and Access Management	Authorized session manager evidence
E-IAM-30	Identity and Access Management	List of privileged users
E-IAM-31	Identity and Access Management	Access approval evidence
E-IAM-32	Identity and Access Management	Tunneling restriction config evidence
E-IAM-33	Identity and Access Management	Zero Trust Implementation Configuration
E-IAM-34	Identity and Access Management	Access grant evidences
E-IAM-35	Identity and Access Management	Production access authentication
E-IAM-36	Identity and Access Management	Source Code access restrictions
E-IAM-37	Identity and Access Management	Changes made to source code and logs
E-IAM-38	Identity and Access Management	Service accounts listing
E-IAM-39	Identity and Access Management	Shared credential management tool screenshots
E-IAM-40	Identity and Access Management	Network Diagram
E-IAM-41	Identity and Access Management	Access approvals
E-IAM-42	Identity and Access Management	Sample Access Configuration
E-IAM-43	Identity and Access Management	VPN Configuration and process
E-IAM-44	Identity and Access Management	Server configuration for idle session timeout
E-IAM-45	Identity and Access Management	Credential expiry configuration
E-IAM-46	Identity and Access Management	Session expiration enabled configuration

E-IAM-47	Identity and Access Management	Remote access configuration
E-IAM-48	Identity and Access Management	Remote Access credentials listing
E-IAM-49	Identity and Access Management	Remote Vendor access listing and permissions granted
E-IAM-50	Identity and Access Management	Credential Listing
E-IAM-51	Identity and Access Management	Identifiers listing
E-IAM-52	Identity and Access Management	password setting mechanism
E-IAM-53	Identity and Access Management	password encryption evidence
E-IAM-54	Identity and Access Management	Hardware Token Based Authentication Process document
E-IAM-55	Identity and Access Management	Hardware token granting evidence
E-IR-01	Incident Response	Incident Response Plan
E-IR-02	Incident Response	Incident Management Policy
E-IR-03	Incident Response	Review history
E-IR-04	Incident Response	Incident Training Records
E-IR-05	Incident Response	Incident Training Material
E-IR-06	Incident Response	Sample of incidents
E-IR-07	Incident Response	Logs of Incident maintained
E-IR-08	Incident Response	Link to public website
E-IR-09	Incident Response	Incident Legal Communications Requirements Standard
E-IR-10	Incident Response	Business Associates Agreement
E-IR-11	Incident Response	Sample external communication of the incident
E-IR-12	Incident Response	Sample of customer support inquiry
E-MDM-01	Mobile Device Management	Mobile device management policy
E-MDM-02	Mobile Device Management	List of all mobile devices registered with MDM tool
E-MDM-03	Mobile Device Management	Sample mobile device configuration screenshots from the MDM tool
E-MDM-04	Mobile Device Management	Sample mobile device screenshots showcasing the devices are encrypted in the MDM tool
E-MDM-05	Mobile Device Management	Sample mobile device configuration screenshots showcasing the security features are enabled
E-MDM-06	Mobile Device Management	List of high risk travel locations
E-NO-01	Network Operations	Network Security Standard
E-NO-02	Network Operations	Firewall Configuration
E-NO-03	Network Operations	DMZ Configuration
E-NO-04	Network Operations	Network security rules inventory
E-NO-05	Network Operations	Security Rules Configuration
E-NO-06	Network Operations	Dynamic packet filtering configuration
E-NO-07	Network Operations	NAT Configuration

E-NO-08	Network Operations	Network Infrastructure Rules Review Records
E-NO-09	Network Operations	Sample of network configuration settings for applicable systems
E-NO-10	Network Operations	Sample of network architecture for applicable systems
E-NO-11	Network Operations	Configuration of DNS Servers
E-NO-12	Network Operations	Email Configuration
E-NO-13	Network Operations	Vendor Agreement
E-NO-14	Network Operations	Network Architecture Diagram
E-NO-15	Network Operations	Network Segmentation Testing Records
E-NO-16	Network Operations	Configuration of Logical Segregation
E-NO-17	Network Operations	Data Flow Diagrams
E-NO-18	Network Operations	Approved Traffic Flow and configuration
E-NO-19	Network Operations	Network Monitoring Software Configuration
E-NO-20	Network Operations	Sample alerts sent showcasing unauthorized wireless access points
E-NO-21	Network Operations	Wireless Access Point Configuration
E-NO-22	Network Operations	Wireless Connections Configuration
E-NO-23	Network Operations	Denial of Service Protection Plan Configuration on network devices
E-PR-01	People Resources	Human Resource Policy
E-PR-02	People Resources	Background Check Evidence for sample new hire employees
E-PR-03	People Resources	Sample Quarterly Check In Reminders
E-PR-04	People Resources	Career Portal Snapshot
E-PR-05	People Resources	Hiring Process for a sample employee
E-PR-06	People Resources	Termination Process Evidence for sample employees
E-PR-07	People Resources	For sample employees, evidence of an exit interview
E-PR-08	People Resources	Evidence of action taken for employees violating policies, if any
E-PR-09	People Resources	Code of Ethics
E-PR-10	People Resources	Evidence of annual certification
E-PR-11	People Resources	Hotline Case Tracking Evidence
E-PR-12	People Resources	Audit Committee Communication Evidence
E-PR-13	People Resources	List of roles that requires national security clearances
E-PR-14	People Resources	List of personnel with national security clearances
E-PR-15	People Resources	Screening and Rescreening Evidences
E-PR-16	People Resources	Reinvestigation Evidences
E-PR-17	People Resources	Code of Business Conduct
E-PR-18	People Resources	Business Partner Code of Conduct

E-PRIV-01	Privacy	Privacy Policy
E-PRIV-02	Privacy	Privacy Review Evidence
E-PRIV-03	Privacy	Privacy Readiness Review Evidence
E-PRIV-04	Privacy	Consent Notice Snapshot
E-PRIV-05	Privacy	Legal Disclosure Process
E-PRIV-06	Privacy	PII Processing Agreements
E-PRIV-07	Privacy	Customer Sample PII Agreement
E-PRIV-08	Privacy	PII Processing Records
E-PRIV-09	Privacy	Personal Health Information Documentation Records
E-PRIV-10	Privacy	Law enforcement Process
E-PRIV-11	Privacy	Sample investigation requests
E-PRIV-12	Privacy	Evidence Sharing method screenshot
E-PS-01	Proactive Security	Network Security Standard
E-PS-02	Proactive Security	EDR Configuration Documentation
E-PS-03	Proactive Security	Threat Hunting program documentation
E-PS-04	Proactive Security	Threat indicator documentation
E-PS-05	Proactive Security	Periodic Threat Modeling documentation
E-PS-06	Proactive Security	Documentation on gathering intelligence on adversary personas
E-RM-01	Risk Management	Vulnerability management standard
E-RM-02	Risk Management	Latest vulnerability assessment report
E-RM-03	Risk Management	Risk Management Standard
E-RM-04	Risk Management	Risk assessment report
E-RM-05	Risk Management	Sample evidences for the risks treatment plan for the identified risks
E-RM-06	Risk Management	Risk Assessment HIPAA Report
E-RM-07	Risk Management	Compliance Review report
E-RM-08	Risk Management	Sample evidences of corrective actions taken in case of any deficiencies identified
E-RM-09	Risk Management	Quarterly Review Evidence
E-RM-10	Risk Management	Common Controls Framework
E-RM-11	Risk Management	Audit Reports and associated documentation
E-RM-12	Risk Management	Audit Plan
E-RM-13	Risk Management	Audit Checklist
E-RM-14	Risk Management	Remediation Plan
E-RM-15	Risk Management	Finding documentation
E-RM-16	Risk Management	Documented Corrective Action Plan

E-RM-17	Risk Management	Statement of Applicability (SOA)
E-SDD-01	System Design Documentation	Evidence of system diagrams
E-SDD-02	System Design Documentation	Evidence of whitepapers
E-SG-01	Security Governance	Information Security Management Standard
E-SG-02	Security Governance	Evidence of periodic review of organization's policies and standards (with version history)
E-SG-03	Security Governance	Sample of communication mail sent to employees
E-SG-04	Security Governance	Sample Policy Exceptions
E-SG-05	Security Governance	Document Management Criteria
E-SG-06	Security Governance	Document Retention Evidence
E-SG-07	Security Governance	Documented proprietary rights agreement and organization's network access agreement
E-SG-08	Security Governance	Information Security management Standard is uploaded on intranet
E-SG-09	Security Governance	MOM of ISMS steering committee
E-SG-10	Security Governance	ISMS Scope document
E-SG-11	Security Governance	Risk Management Policy
E-SG-12	Security Governance	Risk Matrix
E-SG-13	Security Governance	PCI charter
E-SG-14	Security Governance	Approved budget allocation documentation
E-SG-15	Security Governance	MOM of management meetings
E-SG-16	Security Governance	Enterprise Data Catalogue
E-SG-17	Security Governance	Software License Agreement/Policy
E-SG-18	Security Governance	Software monitoring compliance report to ensure the compliance posture
E-SLC-01	Service Lifecycle	Organization product lifecycle standard
E-SLC-02	Service Lifecycle	Secure product lifecycle
E-SLC-03	Service Lifecycle	Source code standard
E-SLC-04	Service Lifecycle	Source code repository
E-SLC-05	Service Lifecycle	Central Source Code Repository
E-SLC-06	Service Lifecycle	Shared Secret Rotation Logs
E-SLC-07	Service Lifecycle	Minutes of project scope and budget plan meeting
E-SLC-08	Service Lifecycle	Formal sign-off on the project plan
E-SLC-09	Service Lifecycle	Service Lifecycle Program
E-SLC-10	Service Lifecycle	Information system Operation
E-SLC-11	Service Lifecycle	Formal Approval/documents from the authorized personnel
E-SM-01	Systems Monitoring	Logging Standard
E-SM-02	Systems Monitoring	Logging configuration

E-SM-03	Systems Monitoring	Sample of production server logs
E-SM-04	Systems Monitoring	Access review documentation
E-SM-05	Systems Monitoring	NTP logs and configuration
E-SM-06	Systems Monitoring	Quarterly Log reconciliation report
E-SM-07	Systems Monitoring	Sample of remediation documentation
E-SM-08	Systems Monitoring	Enterprise Antivirus Solution configuration
E-SM-09	Systems Monitoring	Sample of antivirus logs
E-SM-10	Systems Monitoring	Security Monitoring Standard
E-SM-11	Systems Monitoring	List of monitoring rules
E-SM-12	Systems Monitoring	Sample of alert rules
E-SM-13	Systems Monitoring	Log integrity checks
E-SM-14	Systems Monitoring	Monitoring tool configuration
E-SM-15	Systems Monitoring	Log evidence from remote sessions
E-SM-16	Systems Monitoring	Evidence of monitoring tool installation
E-SM-17	Systems Monitoring	Alerting criteria
E-SM-18	Systems Monitoring	Sample of security monitoring rules configuration
E-SM-19	Systems Monitoring	Sample of alerts generated
E-SM-20	Systems Monitoring	Sample of legal sign off on monitoring criteria
E-SM-21	Systems Monitoring	Alerting criteria for unauthorized logical access connections
E-SM-22	Systems Monitoring	Availability Monitoring Standard
E-SM-23	Systems Monitoring	Availability Monitoring Rules
E-SM-24	Systems Monitoring	Availability Monitoring Tool Configuration
E-SM-25	Systems Monitoring	Sample of Availability Monitoring Alerts
E-SM-26	Systems Monitoring	Sample of Availability Incident Tickets
E-SM-27	Systems Monitoring	Remote Session logs
E-SM-28	Systems Monitoring	Periodic log review documentation
E-SO-01	Site Operations	Images/Physical inspection confirming Non-partitioned ceilings Secured entry points; and/or Manned reception desks
E-SO-02	Site Operations	Images/Physical inspection confirming data center facility has power and telecommunication lines tagged and labelled
E-SO-03	Site Operations	Images/Physical inspection confirming information security safeguards in place at Access Machines at entry/exit, Fire extinguishers, Fire Alarms etc.
E-SO-04	Site Operations	Sample CCTV video of data center from intrusion detection and video surveillance system

E-SO-05	Site Operations	Configuration from the camera management system that shows that it is configured to retain surveillance video data for 90 days
E-SO-06	Site Operations	Images/Physical inspection confirming the fire detection/suppression systems in use at the Organization-owned data center
E-SO-07	Site Operations	Images/Physical inspection confirming UPS and generators at a selection of Organization-owned data center
E-SO-08	Site Operations	Physical Access Policy
E-SO-09	Site Operations	Approval evidences for physical access
E-SO-10	Site Operations	De-provisioning evidences
E-SO-11	Site Operations	Physical Access Review evidence
E-SO-12	Site Operations	termination Process Evidence for sample employees
E-SO-13	Site Operations	Visitor Approval records
E-SO-14	Site Operations	Visitor access monthly reviews
E-SO-15	Site Operations	List of physical devices
E-SO-16	Site Operations	Access list to inventory
E-SO-17	Site Operations	Evidence of Key Rotation when compromised/ employee termination or transfer
E-SO-18	Site Operations	Temperature and Humidity configuration
E-SO-19	Site Operations	Temperature and Humidity Threshold defined in system
E-SO-20	Site Operations	Temperature and Humidity Alarms triggered and remediation
E-SO-21	Site Operations	fire suppression/detection certifications
E-SO-22	Site Operations	UPS and generator maintenance certificates
E-SO-23	Site Operations	List of authorized personnel with access to shut-off power
E-SO-24	Site Operations	Emergency lighting equipment certificates
E-TA-01	Training and Awareness	Compliance Training Policy
E-TA-02	Training and Awareness	Training Material
E-TA-03	Training and Awareness	Training Records
E-TA-04	Training and Awareness	Evidence of phishing campaigns set up by the organization (Eg - mails sent etc)
E-TA-05	Training and Awareness	Access records who have access to PHI
E-TPM-01	Third Party Management	Procurement Policy
E-TPM-02	Third Party Management	Questionnaire for assessing third party risks
E-TPM-03	Third Party Management	Action Plan for vendor security review
E-TPM-04	Third Party Management	Vendor Security Reviews Evidence
E-TPM-05	Third Party Management	Forensic investigation process document
E-TPM-06	Third Party Management	Sample Forensic Investigations
E-TPM-07	Third Party Management	Vendor information security standard

E-TPM-08	Third Party Management	Privacy Review Evidence
E-TPM-09	Third Party Management	Remediation Evidence of non-compliances identified during Vendor Security Reviews
E-TPM-10	Third Party Management	Network access Agreement
E-TPM-11	Third Party Management	Sample Agreements for temporary workers
E-TPM-12	Third Party Management	Evidence to Acknowledgement to Customers for Card Holder Data responsibilities
E-TPM-13	Third Party Management	Business Associate Agreement
E-TPM-14	Third Party Management	Business Associate Subcontractor Agreement document
E-TPM-15	Third Party Management	Vendor SLA document
E-TPM-16	Third Party Management	Results of Network Configuration Monitoring
E-TPM-17	Third Party Management	Data Processing and Transfer Agreement
E-TPM-18	Third Party Management	Vendor onboarding/ termination document
E-TPM-19	Third Party Management	Sample Vendor Agreement
E-VM-01	Vulnerability Management	Vulnerability Management Policy
E-VM-02	Vulnerability Management	Scan Tool version evidence
E-VM-03	Vulnerability Management	Scanning evidence for a sample hosts/accounts
E-VM-04	Vulnerability Management	Resolution and rescan evidence for a sample vulnerability
E-VM-05	Vulnerability Management	Sample exploited vulnerability resolution evidence
E-VM-06	Vulnerability Management	Sample vulnerability remediation evidence
E-VM-07	Vulnerability Management	Approved Scanning Vendor (ASV) Scan evidence
E-VM-08	Vulnerability Management	Penetration Test Results
E-VM-09	Vulnerability Management	Infrastructure Management Policy
E-VM-10	Vulnerability Management	Patch Implementation Evidence
E-VM-11	Vulnerability Management	End of Life software decomission plan
E-VM-12	Vulnerability Management	Antivirus Deployment Evidence
E-VM-13	Vulnerability Management	Antivirus Configuration Policies
E-VM-14	Vulnerability Management	Media usage logs
E-VM-15	Vulnerability Management	Secure Development Lifecycle Policy
E-VM-16	Vulnerability Management	Sample Error Messages
E-VM-17	Vulnerability Management	Sample Disputes, inquiries and complaints
E-VM-18	Vulnerability Management	Management Review Evidence
E-VM-19	Vulnerability Management	Verified Threats resolution evidence
E-VM-20	Vulnerability Management	Sample Independent Information Security Assessment Results
E-VM-21	Vulnerability Management	Sample Assessment Ticket and notification
E-VM-22	Vulnerability Management	Sample Identified Bugs