Overview

Certifications & Attestations	Descriptions
ISO 27001	ISO 27001 is a security mangement standard that specifies best practices for security management and comprehensive security controls
SOC	Reports from AWS Systems & Organization Control (SOC are independent third-party examiniation reports that demonstrate how AWS achieves it's key compliance controls and objects. The AWS plaform is compatible with SOC 1, SOC 2, & SOC 3

Laws, Regulations, and Privacy Complia	Descriptions
HIPAA	U.S. Health Insurance Portability and Accountability Act (HIPAA) is a set of federal standards, which protect the security and privacy of PHI protected Health Information (PHI). AWS enables entities and their business associates covered by HIPAA to leverage the secure AWS environment for processing, maintaing and storing protected health information.
PCI DSS Level 1	The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard (means security for information that is protected by copyright or trademark) administered by the PCI Security Standards Council. All entitites that deal with online payments using cred cards and store, process or transmit cardholder data need to be PCI. DSS Level 1 compliant
GDPR	General Data Protection Regulation is the European Data Protection regulations appblicable as of May 25th, 2018 in all state member states to harmonize data privaacy laws across Europe. Focues on Data protection leveraging terms such as: • Data Owner • Data Steward • Data Custodian • Privacy Officer

Alignments & Frameworks	Descriptions
G-Cloud [UK]	The G-Cloud framework is an agreement between the UK government and cloud-based service providers. The framework enables public bodies to procure commodity-based, pay-as-you-go cloud services on government-approved short-term contracts. In order to host on AWS, public bodies need to beem the G-Cloud [UK] requirements.
NIST 800-146	Cloud computing Synopsis and Recommendation
NIST 800-145	The NIST Definition of Cloud Computing
NIST 800-210	General Access Control Guidenance for Cloud Systems https://doi.org/10.6028/NIST.SP.800-210
NIST 500-291	NIST Cloud Computing Stndards Roadmap https://www.nist.gov/system/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf
NIST 800-53	Cybersecurity standard and compliance framework developed by the National Institute of Standards in Technology. It's a continusly updated framework that tries tto flexibly define standards, controls, and assesments based on risk, cost-effectiveness, and capabilities.
ISO/IEC 19944-1:2020	Cloud computing and distributed platforms - Data flow, data categories and data use - part 1: fundimentals
SCAP	Security Content Automation Protocol is a standard system that helps you automate how you identify the vulnerabiilies in your system and comply with existing security requirements in your field. As an initiative of NIST SCAP offers you an opportunity to pinpint your scurity weaknesses and resolve them with a framework that has been proven and tested. Include: • XCCDF - Extensible Configuration Checklist Description Format • OVAL - Open Vulnerability and Assessment Language • CVE - Common Vulnerabilities and Exposures • CPE - Common Platform Emumeration

Control	NIST SP 800-53	NIST CSF	HITRUST	GDPR	CSA	ISO	PCI
•Business Associate Agreement (BAA) must exist with any third party or contractor handling data.	NIST SP 800-53 Rev. 5: SA-9	NIST CSF: PR.SC-3	HITRUST CSF13.j		CSA CCM 3.0.1: STA-05, STA-09, HRS-06, CCC-02	ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3	PCI DSS v3.2 12.2, 12.8
•Service Agreement must exist that defines the expectations and liability of both parties (e.g. Master Service Agreement)	NIST SP 800-53 Rev. 5: SA-9	NIST CSF: PR.SC-3	HITRUST CSF05.k, 09.e-g		CSA CCM 3.0.1: STA-05, STA-09, HRS-06, CCC-02	ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3	PCI DSS v3.2 12.2,12.8
•Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. •A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated automatically or regularly and assigned ownership by defined roles and responsibilities.	NIST SP 800-53 Rev. 5: CM-8 - MP-1 - PM-5 - SE-1	NIST CSF: ID.AM-1, ID.AM-2, ID.AM-5, PR.AC-4, PR.DS-3	HITRUST CSF 07.a-b	GDPR Article 32	CSA CCM 3.0.1: DCS-01	ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1	PCI DSS v3.2 2.4, 9.6.1,12.2
•All employees and contractors accessing platforms have current annual enterprise security awareness training.	NIST SP 800-53 Rev. 5: AR-5 - AT-1 - AT-2 - AT-3 - AT-4 - CP-3 - CP-4 - IR-2 - PL-4 - PM-14 - PM-6 - SA-16	NIST CSF: ID.AM-6, ID.GV-3, ID.GV-4, PR.AT-1, PR.AT-2, PR.AT-4, PR.AT-5, PR.IP-11, RS.,CO-1	HITRUST CSF02.e	GDPR Articles 32,28,39	CSA CCM 3.0.1: HRS-09	ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2, A.12.2.1	PCI DSS v3.2 12.4, 12.5, 12.8, 12.9
• Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: - Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure - Compliance with defined retention periods and end-of-life disposal requirements - Data classification and protection from unauthorized use, access, loss, destruction, and falsification	NIST SP 800-53 Rev. 5: CA-3 - RA-2 - RA-3 - SI-12	NIST CSF: ID.GV-4, ID.RA-1, ID.RA-3, ID.RA-4, ID.RA-5, ID.RM-1, RS.CO-5	HITRUST CSF 03.b	GDPR Articles 28,32	CSA CCM 3.0.1: GRM-02	ISO/IEC 27001:2013 Clause 6.1.2, 6.1.4	PCI DSS v3.2 6.1, 11.2, 11.3, 12.2

Network Security

Control	NIST SP 800-53	NIST CSF	HITRUST	GDPR	CSA	ISO	PCI
•Network shall be segmented based off levels of trust (eg. untrusted, trusted, DMZ). Further segmentation should occur to define functional zones (eg. database, storage, backup), and levels of risk. •Point-to-point connections shall only terminate to trusted endpoint. •Management/Control plane should be separate and not impacted by data plane •App-aware network filtering will be added to existing network level devices to offset the lack of visibility traditional network devices have into container network traffic due to the ephemeral nature of containerized apps' network topologies	NIST SP 800-53 Rev. 5: AC-4 - AC-10 - SC-7	NIST CSF: PR.AC-5	HITRUST CSF 01.m-o, w; 09.m; 09.w		CSA CCM 3.0.1: DSI-01, IVS-09	ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3	PCI DSS v3.2 1.1, 1.2, 2.2, 6.2, 10.8, 11.3
•Multiple layers of protection are deployed within the network path (e.g. Web Application Firewall, DDoS mitigation, Intrusion Detection/Prevention Systems), so as to prevent or detect network-based attacks, or attacks that are visible from the packet.	NIST SP 800-53 Rev. 5: AC-1 - SC-3 - SC-7	NIST CSF: PR.PT-3	HITRUST CSF 09.m, 11.c	GDPR Articles 25, 32	CSA CCM 3.0.1: IVS-13	ISO/IEC 27001:2013 A.9.1.2	PCI DSS v3.2 2.2, 7.1, 7.2, 9.3
•Ports and services should be restricted or disabled to only provide the least amount of functionality necessary to meet the requirements • Egress network traffic will be monitored to ensure traffic is not going across networks	NIST SP 800-53 Rev. 5: AC-3 - CM-7	NIST CSF: PR.PT-3	HITRUST CSF 01.s, 10.j	GDPR Articles 25,32	CSA CCM 3.0.1: IAM-13	ISO/IEC 27001:2013 A.9.1.2	PCI DSS v3.2 2.2, 7.1, 7.2, 9.3
•Network sessions will follow default timeouts and behaviors addressed in the respective protocol's RFC standards.	NIST SP 800-53 Rev. 5: SC-10 - AC-12	NIST CSF: PR.PT-4, PR.PT-5	HITRUST CSF 01.g,t		CSA CCM 3.0.1: AIS-01, IAM-12	ISO/IEC 27001:2013 A.13.1.1, A.13.2.1, A.14.1.3 A.17.1.2, A.17.2.1	PCI DSS v3.2 1 (all), 2 (all), 4.1
•Physical or logical high availability should exist. Critical or high risk paths/applications should have at least near real-time resolution in the event of an unforeseen break in connectivity.	NIST SP 800-53 Rev. 5: CP-7 - CP-8, - CP-11 - CP-13 - PL-8 - SA-14 - SC-6	NIST CSF: PR.PT-5	HITRUST CSF 01.m, 01.o, 09.s		CSA CCM 3.0.1: IVS-01	ISO/IEC 27001:2013 A.17.1.2, A.17.2.1	

Access Management

Control	NIST SP 800-53	NIST CSF	HITRUST	GDPR	CSA	ISO	PCI
•Account privileges (both human and non-human) will be granted based off functional role and least amount of privilege necessary to perform their function. Roles/groups will have a manager assigned for attestation and approvals.	NIST SP 800-53 Rev. 5: AC-1 - AC-2 - AC-3 - AC-5 - AC-6 - AC-14 - AC-16 - AC-24	NIST CSF: PR.AC-4	HITRUST CSF 01.a-c, v; 09.c	GDPR Articles 25,32	CSA CCM 3.0.1: IAM-05	ISO/IEC 27001:2013 A.9.2.1,A.9.2.2,A.9.2.3,A.9.2.4,A.9.2.6,A.9.3.1, A.9.4.2,A.9.4.3 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8	PCI DSS v3.2 6.4.2, 7.1, 7.2
•Production use of shared, non-unique, or default accounts will not be permitted.	NIST SP 800-53 Rev. 5: IA-2 - IA-4	NIST CSF: PR.AC-1,6,7	HITRUST CSF 01.b-c,i,v;10.j	GDPR Articles 25,32	CSA CCM 3.0.1: IAM-09, IAM-12	ISO/IEC 27001:2013 A.7.1.1, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3	PCI DSS v3.2 8.1, 8.2, 12.3, 7.1,7.2, 8.1, 8.2.2
•Identity trusts should be centrally administered, and remote sites securely federated. Single-Sign-On is utilized where technically feasible.	NIST SP 800-53 Rev. 5: IA-2 - IA-5 - IA-8	NIST CSF: PR.AC-1,6,7	HITRUST CSF01.d	GDPR Articles 25,32	CSA CCM 3.0.1: IAM-12	ISO/IEC 27001:2013 A.7.1.1, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3	PCI DSS v3.2 8.1, 8.2, 12.3, 7.1,7.2, 8.1, 8.2.2
•Where password are used, they shall adhere to industry recognized standards of length, complexity, and duration. Additional complexity is required for privileged and process/service/non-human accounts.	NIST SP 800-53 Rev. 5: IA-5 - IA-6	NIST CSF: PR.AC-1	HITRUST CSF 01.b,d,f,q,r	GDPR Articles 25,32	CSA CCM 3.0.1: IAM-12	ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3	PCI DSS v3.2 8.1, 8.2, 12.3, 7.1,7.2, 8.1, 8.2.2
•Human accounts accessing sensitive and/or confidential data or accessing management platforms that contain sensitive and/or confidential data will require multi-factor authentication.	NIST SP 800-53 Rev. 5: IA-2 - IA-5	NIST CSF: PR.AC-4	HITRUST CSF01.q	GDPR Articles 25,32	CSA CCM 3.0.1: IAM-12	ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5	PCI DSS v3.2 6.4.2, 7.1, 7.2
•Administrative session timeouts can occur after a configurable period of inactivity, and lockouts can occur after a configurable number of invalid attempts.	NIST SP 800-53 Rev. 5: AC-7 - AC-11 - AC-12 - IA-5 - IA-6	NIST CSF: PR.AC-7	HITRUST CSF01.d,g,p	GDPR Articles 25,32	CSA CCM 3.0.1: IAM-12	ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4	
•Monitoring shall occur of account provisioning, removal, and modifications. Monitoring and analytics shall occur of account usage.	NIST SP 800-53 Rev. 5: AC-1 - AC-2 - AU-2	NIST CSF: DE.CM-3, PR.AC-1	HITRUST CSF01.a-c	GDPR Articles 25,32	CSA CCM 3.0.1: IAM-11,12	ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3	PCI DSS v3.2 8.1, 8.2, 12.3, 7.1,7.2, 8.1, 8.2.2
•All credentials (human, non-human, privileged, non-privileged, administrative, service call/API) and credential integrity are maintained through the use of secure secret storage and transmission. Cleartext, weak and/or deprecated cryptographic mechanisms, will not be permitted for any account.	NIST SP 800-53 Rev. 5: IA-5 - SC-13 - SC-28	NIST CSF: PR.AC-1, PR.AC-6	HITRUST CSF 01.p	GDPR Article 32	CSA CCM 3.0.1: IAM-12	ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3, A.7.1.1, A.9.2.1	PCI DSS v3.2 8.1, 8.2, 12.3, 7.1,7.2, 8.1, 8.2.2
•Timely or automatic removal, modification of privileges and access, shall occur upon employment termination or contract expiration, application decommission (in the case of non-human accounts), change in job function, transfer, or inactivity.	NIST SP 800-53 Rev. 5: AC-2 - PS-4 - PS-5	NIST CSF: PR.AC-1, PR.AC-4, PR.IP-11	HITRUST CSF02.g,i	GDPR Article 32	CSA CCM 3.0.1: IAM-11	ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 ISO/IEC 27001:2013 A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4	PCI DSS v3.2 8.1, 8.2, 12.3, 7.1,7.2, 8.1, 8.2.2
•Account access shall be authorized and re-validated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function.	NIST SP 800-53 Rev. 5: AC-11 - AC-12	NIST CSF: PR_AC-7	HITRUST CSF 01.e		CSA CCM 3.0.1: IAM-10	ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4	

Application Security

Control	NIST SP 800-53	NIST CSF	HITRUST	GDPR	CSA	ISO	PCI
•Enterprise developed application interfaces (socket, graphical user interface, application and programming interface) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g. SEI CERT, OWASP).	NIST SP 800-53 Rev. 5: SA-15 - SI family	NIST CSF: PR.AC-5	HITRUST CSF 10.b, 10.c, 10.e	GDPR Articles 25,28,32	CSA CCM 3.0.1: AIS-01	ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3	PCI DSS v3.2 1.1, 1.2, 2.2, 6.2, 10.8, 11.3
•Enterprise developed application source code is scanned for vulnerabilities within the development pipeline. Vulnerabilities found are treated like bugs and weighted/assessed in order of criticality or impact. Critical and high results must be remediated prior to production promotion	NIST SP 800-53 Rev. 5: SA-11 - SI family	NIST CSF: PR.IP-2, ID.RA-1	HITRUST CSF 10.a, 10.k, 10.l	GDPR Articles 25,28,32	CSA CCM 3.0.1: CCC-03	ISO/IEC 27001:2013 A.12.6.1, A.18.2.3	PCI DSS v3.2 6.1, 11.2, 11.3, 12.2
•In instances of remotely hosted software/infrastructure, penetration tests are performed against applications to identify software flaws, and improper configurations and measure the vulnerability impact. New applications must have a penetration test performed, and any critical findings remediated, before production promotion. •Existing applications that contain or have access to PII, PHI, or PCI data will have annual penetration tests, with any critical findings remediated within 30 days.	NIST SP 800-53 Rev. 5: RA-5 - CA-8	NIST CSF: ID.RA-1	HITRUST CSF 10.m	GDPR Articles 25,32	CSA CCM 3.0.1: TVM-02	ISO/IEC 27001:2013 A.12.6.1, A.18.2.3	PCI DSS v3.2 6.1, 11.2, 11.3, 12.2
•In instances of remotely hosted physical, virtual infrastructure/operating systems and container runtimes, vulnerability scans must be performed. There should be authenticated scans to provide complete and accurate asset vulnerability, and unauthenticated external scans to provide exploitability. Scans will be performed quarterly, at a minimum. Results should be weighted/assessed by risk level to determine remediation timeframe.	NIST SP 800-53 Rev. 5: RA-5 - CA-7	NIST CSF: PR.AC-5	HITRUST CSF 06.h, 10.m	GDPR Articles 32,25	CSA CCM 3.0.1: IVS-05, TVM-02	ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3	PCI DSS v3.2 1.1, 1.2, 2.2, 6.2, 10.8, 11.3
•Instances of remotely hosted physical or virtual infrastructure/operating systems, will have demonstratable endpoint protection and detection from known and unknown threats and vulnerabilities. Processes that that unauthorized or no approved for use, should not be permitted to run.	NIST SP 800-53 Rev. 5: RA-5 - CA-7	NIST CSF: PR.AC-5	HITRUST CSF 06.h, 10.m	GDPR Articles 25,32	CSA CCM 3.0.1: IVS-05, TVM-02	ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3	PCI DSS v3.2 1.1, 1.2, 2.2, 6.2, 10.8, 11.3

Data Security

Control	NIST SP 800-53	NIST CSF	HITRUST	GDPR	CSA	ISO	PCI
•For the purposes of a proof-of-concept/evaluation, de-identified data will be used. Production data can be used once the POC is complete and all additional controls and service agreements are met.	NIST SP 800-53 Rev. 5: DM-1 (App J) - DM-3 (App J)	NIST CSF: PR.DS-7	HITRUST CSF 13.l		CSA CCM 3.0.1: DSI-05	ISO/IEC 27001:2013 A.12.1.4	PCI DSS v3.2 6.4.1, 6.4.2
•Data in transit is cryptographically protected. This includes inter and intra data transmission. •Container communication across multiple hosts will be done over a virtual and encrypted network	NIST SP 800-53 Rev. 5: SC-8 - SC-11 - SC-12	NIST CSF: PR.DS-2	HITRUST CSF09.vxy, 10.df	GDPR Article 32	CSA CCM 3.0.1: EKM-03, IPY-04, IVS-10, MOS-11	ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	PCI DSS v3.2 4.1, 4.2, 4.3
•Data at rest is cryptographically protected.	NIST SP 800-53 Rev. 5: MP-8 - SC-12 - SC-28	NIST CSF: PR.DS-1	HITRUST CSF09.vxy, 10.f		CSA CCM 3.0.1: EKM-03, IPY-04, IVS-10, MOS-11	ISO/IEC 27001:2013 A.8.2.3	PCI DSS v3.2 3.1, 3.3, 3.4, 3.5, 3.6, 3.7
•Data labeled to define ownership, data type, sensitivity, regulatory requirements, and business criticality. Labeling can be inherited in instances of data aggregation.	NIST SP 800-53 Rev. 5: AC-4 - AC-5 - AC-6 - CP-2 - PE-19 - PS-3 - PS-6 - SA-14 - SC-6 - SC-7 - SC-8 - SC-13 - SC-31 - SI-4	NIST CSF: ID.AM-5, PR.DS-5	HITRUST CSF 07.d-e	GDPR Articles 6 GDPR Articles 25,32	CSA CCM 3.0.1: DSI-01, DSI-04	ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4,A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3	PCI DSS v3.2 9.6.1, 12.2
•Access or transmission of data can be tracked based off labeling, sensitivity, or keyword. Highest priority given to confidential and secret information.	NIST SP 800-53 Rev. 5: AU-6 - CA-7 - IR-4 - IR-5 - IR-8 - SI-4	NIST CSF: DE.AE-2-5; DE.CM1-3,6-7	HITRUST CSF 06.c, 09.ab	GDPR Articles 32,33,34	CSA CCM 3.0.1: IVS-01	ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4	PCI DSS v3.210.6.1, 11.4, 12.5.2, 10.1
•Cryptographic keys used in the transmission, storage, or processing of McKesson created data/content are directly managed by the organization. •Data keys are securely protected and encrypted, in a separate environment than the encrypted data. •Strong, centralized key management is used for file, volume and application encryption (for data at rest, in use and in motion). The scope of key management is limited to specific functional units or roles.	NIST SP 800-53 Rev. 5: SC-12 - SC-13 - SC-17	NIST CSF: PR.DS-1, PR.DS-2	HITRUST CSF 06.d, 10.g		CSA CCM 3.0.1: EKM-01, EKM-02, EKM-03	ISO/IEC 27001:2013 A.8.2.3 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	PCI DSS v3.2 3.1, 3.3, 3.4, 3.5, 3.6, 3.7
•Data can be removed or destroyed by the data owner or entity such that it cannot be retrievable by any third party.	NIST SP 800-53 Rev. 5: MP-6	NIST CSF: PR.IP-6	HITRUST CSF 08.l, 09.p	GDPR Article 32	CSA CCM 3.0.1: DSI-07	ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7	PCI DSS v3.2 3.1, 9.8
•Development/Testing environments and data are kept separate from production.	NIST SP 800-53 Rev. 5: CM-2	NIST CSF: PR.DS-7	HITRUST CSF09.d, 10.h	GDPR Article 25	CSA CCM 3.0.1: IVS-08	ISO/IEC 27001:2013 A.12.1.4	PCI DSS v3.2 6.4.1, 6.4.2

Operational Security

Control	NIST SP 800-53	NIST CSF	HITRUST	GDPR	CSA	ISO	PCI
•All administrative activity can be logged, with clearly defined information as to who, what, when, how. •90 days of administrative/audit logs should be available for immediate retrieval. •Retention beyond 90 days can be cold storage; spanning 1 year for access to PCI data and 6 years for access to PHI data.	NIST SP 800-53 Rev. 5:AU family	NIST CSF: PR.DS-2	HITRUST CSF01.s, 06.i, 09.aa-ae	GDPR Articles 25,32,28,33,26	CSA CCM 3.0.1: IVS-01	ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	PCI DSS v3.2 4.1, 4.2, 4.3
•Administrative and operational logs, and usage data, can aggregated to centralized locations and correlated. •Baselines are established for expected operation and administration.	NIST SP 800-53 Rev. 5: AU-6 - CA-7 - IR-4 - IR-5 - IR-8 - SI-4	NIST CSF: DE.AE-2-5; DE.CM1-3,6-7	HITRUST CSF 01.j, 01.s, 09.ab	GDPR Articles 32,33,34	CSA CCM 3.0.1: IVS-01	ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4 A.12.4.1, A.16.1.7	PCI DSS v3.2 10.6.1, 11.4, 12.5.2, 10.1, 12.10.5
•Logs can be ingested and analyzed by a security information and event management system. System will able to detect and alert to cybersecurity events.	NIST SP 800-53 Rev. 5: AU-6 - CA-7 - IR-4 - IR-5 - IR-8 - SI-4	NIST CSF: DE.AE-2-5; DE.CM1-3,6-7	HITRUST CSF01.j, 01.s, 09.ab	GDPR Articles 32,33,34	CSA CCM 3.0.1: IVS-01	ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4 A.12.4.1, A.16.1.7	PCI DSS v3.2 10.6.1, 11.4, 12.5.2, 10.1, 12.10.5
•Policies and procedures are established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management. •Points of contact (service owners/managers, and operations) are identified and informed of their roles and responsibilities during and following an incident.	NIST SP 800-53 Rev. 5: IR Family	NIST CSF: ID.GV-3,	HITRUST CSF11.a,c	GDPR Articles 32,33,34,31	CSA CCM 3.0.1: IVS-01	ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5	PCI DSS v3.2 3.1, 9.8, 12.10
•Connectivity flows are documented (either automatically or manually) and placed in a centralized location.	NIST SP 800-53 Rev. 5: SA-5 - SA-10	PR.IP-1	HITRUST CSF 09.a, 09.i, 09.r		BCR-04, CCC-03	27002:2013 14.2.2	PCI DSS v3.2 2.5
•External/Crowd Sourced threat feeds can be consumed and correlated to monitored activity. •Conversely de-identified data received from internal monitoring and incidents can be shared with external, trusted entities to assist the larger cyber security landscape.	NIST SP 800-53 Rev. 5: SI-5 - PM-15	NIST CSF: RS.CO-5	HITRUST CSF 05.g, 11.b	GDPR Articles 31; 36; 40 GDPR Articles 45;	CSA CCM 3.0.1: TVM-02	ISO/IEC 27001:2013 A.6.1.4	
•Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards that focus on system availability, confidentiality, and integrity of systems and services.	NIST SP 800-53 Rev. 5: SI-5 - PM-15	NIST CSF: RS.CO-5	HITRUST CSF 09.i	GDPR Articles 31; 36; 40 GDPR Articles 45; 48; 49	CSA CCM 3.0.1: CCC-03	ISO/IEC 27001:2013 A.6.1.4	

Business Continuity and Disaster Recovery (BCDR)

Control	NIST SP 800-53	NIST CSF	HITRUST	GDPR	CSA	ISO	PCI
• Impact of any disruption to the organization is defined and documented, and incorporates the following: - Identify critical products and services - Identify all dependencies, including processes, applications, business partners, and third-party service providers - Understand threats to critical products and services - Determine impacts resulting from planned or unplanned disruptions and how these vary over time - Establish the maximum tolerable period for disruption - Establish priorities for recovery - Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption - Estimate the resources required for resumption	NIST SP 800-53 Rev. 5: CP-1 - CP-2	NIST CSF: ID.AM-5, ID.AM-5, ID.AM-5, PR.AC-4, PR.DS-3	HITRUST CSF 03.a-d,12.a-c	GDPR: Article 28, 32, 33	CSA CCM 3.0.1: DCS-01	ISO/IEC 27001:2013 A.8.2.1 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5	PCI DSS v3.2 9.6.1, 12.2
•Subject to the technical ability or necessity, configuration/system state should have daily differential backups, and weekly full backup. •Backups will be stored in a location logically and physically separate from the system. •Data will only be accessible by system owners	NIST SP 800-53 Rev. 5: AU-6 - CA-7 - IR-4 - IR-5 - IR-8, - SI-4	NIST CSF: DE.AE-2-5; DE.CM1-3,6-7	HITRUST CSF 01.j, 01.s, 09.ab	GDPR: Article 32, 33, 34		ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4	PCI DSS v3.2 10.6.1, 11.4, 12.5.2, 10.1, 12.10.5
•Application and user data must have both high availability and backup solutions appropriate to their levels of data classification and regulatory requirements. •High availabilty should have exact data replication between physically diverse environments. •Backups that would allow for full system restoration will be stored in a location logically and physically separate from the system(s)							