Unique ID	Control ID	Domain	Level	Requirement Statement	Maps To HIPAA?	Cloudticity Inheritance	Cloudticity Service(s)	Palo	Cloudticity Description/Notes
0201.09j1Organizational.124	09.j Controls Against Malicious Code	02 Endpoint Protection	1	Anti-virus and anti-spyware are installed, operating and updated on all end-user devices to conduct periodic scans of the systems to identify and remove unauthorized software. Server environments for which the server software developer specifically recommends not installing host-based anti-virus and anti-spyware software are addressed via a network-based malware detection (NBMD) solution.	Yes	*Partial*	*TMDS, Oxygen Alerts*	*HIP Protection Rules*	*If using Cloudticity hosted TMDS, all instances have Trend Micro Deep Security installed with Anti-Malware, Web Reputation, Intrusion Prevention, Integrity Monitoring, and Log Inspection modules enabled.*
0202.09j1Organizational.3	09.j Controls Against Malicious Code	02 Endpoint Protection	1	Audit logs of the scans are maintained.	Yes	*Partial*	*TMDS*	*No*	*If using Cloudticity hosted TMDS, all instances have Trend Micro Deep Security installed with Anti-Malware, Web Reputation, Intrusion Prevention, Integrity Monitoring, and Log Inspection modules enabled.*
0204.09j2Organizational.1	09.j Controls Against Malicious Code	02 Endpoint Protection	2	Scans for malicious software are performed on boot and every twelve (12) hours.	Yes	*Partial*	*TMDS*	*No*	*If using Cloudticity hosted TMDS, all instances have Trend Micro Deep Security installed with Anti-Malware, Web Reputation, Intrusion Prevention, Integrity Monitoring, and Log Inspection modules enabled. Agent's are on each instance that scan in real-time. These agents perform boot-time scans as part of their real-time nature.*
0205.09j2Organizational.2	09.j Controls Against Malicious Code	02 Endpoint Protection	2	Malicious code that is identified is blocked, quarantined, and an alert is sent to the administrators.	Yes	*Partial*	*TMDS*	*No*	*If using Cloudticity hosted TMDS, all instances have Trend Micro Deep Security installed with Anti-Malware, Web Reputation, Intrusion Prevention, Integrity Monitoring, and Log Inspection modules enabled. Agent's are on each instance that scan in real-time. These agents quarantine and block malicious code using the intrusion prevention module.*
0206.09j2Organizational.34	09.j Controls Against Malicious Code	02 Endpoint Protection	2	Anti-malware is centrally managed and cannot be disabled by the users.	Yes	*Partial*	*TMDS*	*No*	*If using Cloudticity hosted TMDS, all instances have Trend Micro Deep Security installed with Anti-Malware, Web Reputation, Intrusion Prevention, Integrity Monitoring, and Log Inspection modules enabled. Agent's are on each instance that scan in real-time. These agents prevent bypass and changes to the client settings using the Integrity Monitoring module.*
0207.09j2Organizational.56	09.j Controls Against Malicious Code	02 Endpoint Protection	2	Centrally managed, up-to-date anti-spam and anti-malware protection is implemented at information system entry/exit points for the network and on all devices.	Yes	*Partial*	*TMDS*	*No*	*If using Cloudticity hosted TMDS, all instances have Trend Micro Deep Security installed with Anti-Malware, Web Reputation, Intrusion Prevention, Integrity Monitoring, and Log Inspection modules enabled.*
0214.09j1Organizational.6	09.j Controls Against Malicious Code	02 Endpoint Protection	1	Protection against malicious code is based on malicious code detection and repair software, security awareness, and appropriate system access and change management controls.	Yes	*Partial*	*TMDS, Oxygen Alerts*	*No*	*If using Cloudticity hosted TMDS, all instances have Trend Micro Deep Security installed with Anti-Malware, Web Reputation, Intrusion Prevention, Integrity Monitoring, and Log Inspection modules enabled. Agent's are on each instance that scan in real-time. These agents quarantine and block malicious code using the Intrusion Prevention and Anti-Malware modules*
0215.09j2Organizational.8	09.j Controls Against Malicious Code	02 Endpoint Protection	2	The organization addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.	Yes	*Partial*	*TMDS, Oxygen Alerts*	*No*	*If using Cloudticity hosted TMDS.*
0219.09j2Organizational.12	09.j Controls Against Malicious Code	02 Endpoint Protection	2	The information system implements safeguards to protect its memory from unauthorized code execution.	Yes	*Partial*	*TMDS*	*No*	*If using Cloudticity hosted TMDS.*
0226.09k1Organizational.2	09.k Controls Against Mobile Code	02 Endpoint Protection	1	The organization has implemented and regularly updates mobile code protection, including anti-virus and anti-spyware.	Yes	*Partial*	*TMDS*	*No*	*If using Cloudticity hosted TMDS, all instances have Trend Micro Deep Security installed with Anti-Malware, Web Reputation, Intrusion Prevention, Integrity Monitoring, and Log Inspection modules enabled. Agent's are on each instance that scan in real-time. These agents receive updated definition files automatically when they are available.*
0601.06g1Organizational.124	06.g Compliance with Security Policies and Standards	06 Configuration Management	1	Annual compliance reviews are conducted by security or audit individuals using manual or automated tools; if non-compliance is found, appropriate action is taken.	Yes	*Full*	*Quarterly Reviews*	*No*	*When Quarterly Reviews are utilized, security audits are performed on a quarterly basis for AWS infrastructure and Cloudticity access. Customer is responsible for all internal security policies and procedures.*
0602.06g1Organizational.3	06.g Compliance with Security Policies and Standards	06 Configuration Management	1	The results and recommendations of the reviews are documented and approved by management.	Yes	*Full*	*Quarterly Reviews*	*No*	*When Quarterly Reviews are utilized, security audits are performed on a quarterly basis for AWS infrastructure and Cloudticity access. Customer is responsible for all internal security policies and procedures.*
0603.06g2Organizational.1	06.g Compliance with Security Policies and Standards	06 Configuration Management	2	Automated compliance tools are used when possible.	Yes	*Full*	*Cloudticity Oxygen (HIPAA Technical Assessments, CIS Profile Checks, AWS Config Rules)*	*No*	*Cloudticity Oxygen provides a HIPAA technical assessment daily providing a compliance snapshot of the AWS account with regards to technical controls. If using Cloudticity provided CIS profile checks, instance are reviewed on a regular basis for abnormalities in configuration.*
0604.06g2Organizational.2	06.g Compliance with Security Policies and Standards	06 Configuration Management	2	The organization has developed a continuous monitoring strategy and implemented a continuous monitoring program.	Yes	*Full*	*Cloudticity Oxygen*	*No*	*Cloudticity Oxygen provides continuous monitoring with alerts for CPU, Memory, Disk I/O, Custom Metrics, Instance Status, SSM status, tagging/labelling, and Trend Micro.*
0613.06h1Organizational.12	06.h Technical Compliance Checking	06 Configuration Management	1	The organization performs annual checks on the technical security configuration of systems, either manually by an individual with experience with the systems and/or with the assistance of automated software tools, and takes appropriate action if non-compliance is found.	Yes	*Full*	*Quarterly Reviews, HIPAA Technical Assessments*	*No*	*If utilizing Cloudticity hosted TMDS, Cloudticity takes responsibility for vulnerability scanning on a regular interval. Customer is responsible for all application security implementation standards and penetration testing.*
0614.06h2Organizational.12	06.h Technical Compliance Checking	06 Configuration Management	2	Technical compliance checks are performed by an experienced specialist with the assistance of industry standard automated tools, which generate a technical report for subsequent interpretation. These checks are performed annually, but more frequently where needed, based on risk as part of an official risk assessment process.	Yes	*Full*	*Quarterly Reviews, HIPAA Technical Assessments*	*No*	*Cloudticity Oxygen provides a HIPAA technical assessment daily providing a compliance snapshot of the AWS account with regards to technical controls. If using Cloudticity provided CIS profile checks, instance are reviewed on a regular basis for abnormalities in configuration.*
0618.09b1System.1	09.b Change Management	06 Configuration Management	1	Changes to information assets, including systems, networks and network services, are controlled and archived.	No	*Full*	*Cloudticity Infrastructure Orchestration*	*No*	*Cloudticity provides change management through Teamwork tasks (For most changes) and Zendesk supports tickets (For requests less than 4 hours).*
0620.09b2System.3	09.b Change Management	06 Configuration Management	2	Fallback procedures are defined and implemented, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.	No	*Partial*	*Change Management*	*No*	*If using Cloudticity provided backups, a rollback strategy is part of the disaster recovery plan. This by default allows for rollback to the most recent AMI, which depending on the customer RTO/RPO is daily or hourly.*
0627.10h1System.45	10.h Control of Operational Software	06 Configuration Management	1	The organization maintains information systems according to a current baseline configuration and configures system security parameters to prevent misuse. Vendor supplied software used in operational systems is maintained at a level supported by the supplier, and uses the latest version of Web browsers on operational systems to take advantage of the latest security functions in the application.	No	*Partial*	*Cloudticity Hardened Images, Patching*	*No*	*If using Cloudticity provided hardened images, baseline configuration is based on CIS profiles. If using Cloudticity provided CIS profile check service, instances are monitored on a daily basis for configuration issues.*
0628.10h1System.6	10.h Control of Operational Software	06 Configuration Management	1	If systems or system components in production are no longer supported by the developer, vendor, or manufacturer, the organization must show evidence of a formal migration plan approved by management to replace the system or system components.	No	*Partial*	*Oxygen Alerts, AWS Technical Notifications w/ Teamwork Tasks*	*No*	*For all AWS or Cloudticity Oxygen services, Cloudticity is responsible for facilitating migration off soon-to-be deprecated services or features.*
0629.10h2System.45	10.h Control of Operational Software	06 Configuration Management	2	A rollback strategy is in place before changes are implemented, and an audit log is maintained of all updates to operational program libraries.	No	*Partial*	*Change Management*	*No*	*If using Cloudticity provided backups and patch management, a rollback strategy is part of the disaster recovery plan. This by default allows for rollback to the most recent AMI, which depending on the customer RTO/RPO is daily or hourly.*

0630.10h2System.6	10.h Control of Operational Software	06 Configuration Management	2	Physical or logical access is only given to suppliers for support purposes when necessary, with management approval, and such access is monitored.	No	*Full*	*Cloudticity Agreements*	*No*	*Cloudticity is a supplier of support. Cloudticity personnel are managed and authorized based on Cloudticity policies with implementation through Google Authentication. Access is given to the AWS services, but not necessarily the customer applications. On occassion, some customers provide access to their applications for professional services engagements. Professional services are reserved for highly certified and trained Cloudticity personnel.*
0638.10k2Organizational.34569	10.k Change Control Procedures	06 Configuration Management	2	Changes are formally controlled, documented and enforced in order to minimize the corruption of information systems.	Yes	*Partial*	*Change Management*	*No*	*Changes through Zendesk or Teamwork*
0639.10k2Organizational.78	10.k Change Control Procedures	06 Configuration Management	2	Installation checklists and vulnerability scans are used to validate the configuration of servers, workstations, devices and appliances and ensure the configuration meets minimum standards.	Yes	*Partial*	*Oxygen Alerts, HIPAA Technical Assessments, CIS Profile Checks*	*No*	*For instance configuration against best practices*
0640.10k2Organizational.1012	10.k Change Control Procedures	06 Configuration Management	2	Where development is outsourced, change control procedures to address security are included in the contract(s) and specifically require the developer to track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel or roles.	Yes	*Partial*	*Professional Services*	*No*	*For AWS changes and Cloudticity Oxygen new features*
0642.10k3Organizational.12	10.k Change Control Procedures	06 Configuration Management	3	The organization develops, documents, and maintains, under configuration control, a current baseline configuration of the information system, and reviews and updates the baseline as required.	Yes	*Full*	*Cloudticity Account Configuration, Cloudticity Hardened Images*	*No*	*If using Cloudticity provided hardened images*
0643.10k3Organizational.3	10.k Change Control Procedures	06 Configuration Management	3	The organization (i) establishes and documents mandatory configuration settings for information technology products employed within the information system using the latest security configuration baselines; (ii) identifies, documents, and approves exceptions from the mandatory established configuration settings for individual components based on explicit operational requirements; and (iii) monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	Yes	*Partial*	*Oxygen Alerts (Config Rules), CIS Profile Checks, Hardened Images, HIPAA Technical Assessment*	*No*	*If using Cloudticity provided hardened images, baseline configuration is based on CIS profiles. If using Cloudticity provided CIS profile check service, instances are monitored on a daily basis for configuration issues.*
0644.10k3Organizational.4	10.k Change Control Procedures	06 Configuration Management	3	The organization employs automated mechanisms to (i) centrally manage, apply, and verify configuration settings; (ii) respond to unauthorized changes to network and system security-related configuration settings; and (iii) enforce access restrictions and auditing of the enforcement actions.	Yes	*Partial*	*Oxygen Alerts (Config Rules), CIS Profile Checks, Hardened Images, HIPAA Technical Assessment*	*No*	*Cloudticity Oxygen provides automated alerts and dashboards for configuration settings in regards to AWS accounts, AWS services, Operating Systems (CIS profile checks). Cloudticity Oxygen services themselves, unmanaged SSM instances, and more.*
0663.10h1System.7	10.h Control of Operational Software	06 Configuration Management	1	The operating system has in place supporting technical controls such as antivirus, file integrity monitoring, host-based (personal) firewalls or port filtering tools, and logging as part of its baseline.	No	*Partial*	*TMDS*	*No*	*If using Cloudticity hosted TMDS, all instances have Trend Micro Deep Security installed with Anti-Malware, Web Reputation, Intrusion Prevention, Integrity Monitoring, and Log Inspection modules enabled. Agent's are on each instance that scan in real-time. These agents are configured as part of initial/baseline installation.*
0663.10h2Organizational.9	10.h Control of Operational Software	06 Configuration Management	2	The organization prevents program execution in accordance with the list of unauthorized (blacklisted) software programs and rules authorizing the terms and conditions of software program usage.	No	*Partial*	*TMDS*	*No*	*See Application Control Module in TMDS. If using Cloudticity hosted TMDS, all instances have Trend Micro Deep Security installed with Anti-Malware, Web Reputation, Intrusion Prevention, Integrity Monitoring, and Log Inspection modules enabled. Trend Micro utilizes blacklists that are updated on a regular basis across their entire network; referred to as Smart Protection Network. https://www.trendmicro.com/en_us/business/technologies/smart-protection-network.html*
0664.10h2Organizational.10	10.h Control of Operational Software	06 Configuration Management	2	The organization identifies unauthorized (blacklisted) software on the information system, including servers, workstations and laptops, employs an allow-all, deny-by-exception policy to prohibit the execution of known unauthorized (blacklisted) software on the information system, and reviews and updates the list of unauthorized (blacklisted) software periodically but no less than annually.	No	*Partial*	*TMDS*	*No*	*See Application Control Module in TMDS. If using Cloudticity hosted TMDS, all instances have Trend Micro Deep Security installed with Anti-Malware, Web Reputation, Intrusion Prevention, Integrity Monitoring, and Log Inspection modules enabled. Trend Micro utilizes blacklists that are updated on a regular basis across their entire network; referred to as Smart Protection Network. https://www.trendmicro.com/en_us/business/technologies/smart-protection-network.html*
0672.10k3System.5	10.k Change Control Procedures	06 Configuration Management	3	The integrity of all virtual machine images is ensured at all times by (i) logging and raising an alert for any changes made to virtual machine images, and (ii) making available to the business owner(s) and/or customer(s) through electronic methods (e.g., portals or alerts) the results of a change or move and the subsequent validation of the image's integrity.	Yes	*Partial*	*TMDS, Server Compliance (CIS Profile Checks)*	*No*	*If using Cloudticity hosted TMDS, all instances have Trend Micro Deep Security installed with Anti-Malware, Web Reputation, Intrusion Prevention, Integrity Monitoring, and Log Inspection modules enabled.*
068.06g2Organizational.34	06.g Compliance with Security Policies and Standards	06 Configuration Management	2	The organization employs assessors or assessment teams with a level of independence appropriate to its continuous monitoring strategy to monitor the security controls in the information system on an ongoing basis.	Yes	*Full*	*Quarterly Reviews*	*No*	*Cloudticity provides a team of assessor's including a Customer Success Manager (CSM) and Technical Account Manager (TAM) to assess the information system up to, but not including the application layer.*
069.06g2Organizational.56	06.g Compliance with Security Policies and Standards	06 Configuration Management	2	The internal security organization reviews and maintains records of compliance results (e.g., organization-defined metrics) in order to better track security trends within the organization, respond to the results of correlation and analysis, and to address longer term areas of concern as part of its formal risk assessment process.	Yes	*Partial*	*Quarterly Reviews*	*No*	*Cloudticity provides a HIPAA technical assessment dashboard, CIS profile checks, and quarterly reviews all geared toward compliance checks.*
0701.07a1Organizational.12	07.a Inventory of Assets	07 Vulnerability Management	1	An inventory of assets and services is maintained.	Yes	*Partial*	*CloudCheckr, Oxygen Monitoring (Config Rules), Oxygen Management (EC2 Inventory)*	*No*	*Cloudticity provides access to Cloudcheckr for inventory management of the entire AWS account. Cloudticity manages classification tags for o2:phi, o2:environment, o2:instance:backups: type, o2:platform, and others. Customer is reponsible for all assets outside of AWS services.*
0702.07a1Organizational.3	07.a Inventory of Assets	07 Vulnerability Management	1	The information lifecycle manages the secure use, transfer, exchange, and disposal of IT-related assets.	Yes	*Partial*	*Infrastructure Orchestration*	*No*	*AWS is responsible for the secure use, transfer, exchange, and disposal of AWS assets. See SOC2 audit for evidence. Customer is responsible for all assets outside of AWS services.*
0703.07a2Organizational.1	07.a Inventory of Assets	07 Vulnerability Management	2	The inventory of all authorized assets includes the owner of the information asset, custodianship, categorizes the information asset according to criticality and information classification, and identifies protection and sustainment requirements commensurate with the asset's categorization.	Yes	*Partial*	*CloudCheckr, Oxygen Monitoring (Config Rules), Oxygen Management (EC2 Inventory)*	*No*	*Cloudticity is responsible for managing classification tags on AWS resources for determining the environment (o2:environment) the resource belongs to and whether the resource processes or stores sensitive information (o2:phi). Customer is responsible for providing information when Cloudticity cannot determine the classification. Each customer has an explicitly identified technical contact that is responsible for owning/custodianship of AWS resources.*
0704.07a3Organizational.12	07.a Inventory of Assets	07 Vulnerability Management	3	Organizational inventories of IT assets are updated during installations, removals, and system changes, with full physical inventories performed for capital assets (at least annually) and for non-capital assets.	Yes	*Partial*	*CloudCheckr, Oxygen Monitoring (Config Rules), Oxygen Management (EC2 Inventory)*	*No*	*Cloudticity utilizes Cloudcheckr to provide inventory of AWS resources. Combined with resource tags, this can be used to reconcile capital/non-capital assets. Customer is responsible for all non-AWS asset inventory requirements.*
0705.07a3Organizational.3	07.a Inventory of Assets	07 Vulnerability Management	3	The IT Asset Lifecycle Program is regularly reviewed and updated.	Yes	*Partial*	*Cloudticity Infrastructure Orchestration*	*No*	*Cloudticity, in coordination with AWS, provides a full IT lifecycle program for AWS services, including all 6 stages of the lifecycle.*

0709.10m1Organizational.1	10.m Control of Technical Vulnerabilities	07 Vulnerability Management	1	Technical vulnerabilities are identified, evaluated for risk and corrected in a timely manner.	Yes	*Partial*	*Oxygen Alerts, HIPAA Technical Assessments, CIS Profile Checks, Quarterly Reviews*	*No*	*If utilizing Cloudticity hosted TMDS, Cloudticity takes responsibility for vulnerability scanning on a regular interval. If utilizing Cloudticity provided patching solution, Cloudticity is responsible for OS patching for vulnerability remediation. Customer is responsible for all application security implementation standards and penetration testing.*
0710.10m2Organizational.1	10.m Control of Technical Vulnerabilities	07 Vulnerability Management	2	A hardened configuration standard exists for all system and network components.	Yes	*Full*	*Cloudticity Hardened Images*	*No*	*If using Cloudticity provided hardened images*
0711.10m2Organizational.23	10.m Control of Technical Vulnerabilities	07 Vulnerability Management	2	A technical vulnerability management program is in place to monitor, assess, rank, and remediate vulnerabilities identified in systems.	Yes	*Partial*	*TMDS, Oxygen Patching, CIS Profile Checks, Oxygen Monitoring (Config Rules, GuardDuty)*	*No*	*For all Cloudticity Oxygen identified issues, including GuardDuty, configuration issues, and CIS profile check issues, an alert is generated that goes to a customer for inclusion into their change management process.*
0715.10m2Organizational.8	10.m Control of Technical Vulnerabilities	07 Vulnerability Management	2	Systems are appropriately hardened (e.g., configured with only necessary and secure services, ports and protocols enabled).	Yes	*Full*	*Cloudticity Hardened Images, Security Group Management*	*No*	*If using Cloudticity provided hardened images and CIS profile check service*
0716.10m3Organizational.1	10.m Control of Technical Vulnerabilities	07 Vulnerability Management	3	The organization conducts an enterprise security posture review as needed but no less than once within every three-hundred-sixty-five (365) days, in accordance with organizational IS procedures.	Yes	*Partial*	*Quarterly Reviews*	*No*	*Cloudticity facilitates network discovery, network port (Security Group) reviews, vulnerability scanning against CIS profiles, scanning for misconfiguration issues (lack of encryption, missing tags, etc), and vulnerability scanning alerts for GuardDuty events.*
0717.10m3Organizational.2	10.m Control of Technical Vulnerabilities	07 Vulnerability Management	3	Vulnerability scanning tools include the capability to readily update the information system vulnerabilities scanned.	Yes	*Partial*	*TMDS*	*No*	*If using Cloudticity TMDS*
0718.10m3Organizational.34	10.m Control of Technical Vulnerabilities	07 Vulnerability Management	3	The organization scans for vulnerabilities in the information system and hosted applications to determine the state of flaw remediation monthly (automatically) and again (manually or automatically) when new vulnerabilities potentially affecting the systems and networked environments are identified and reported.	Yes	*Partial*	*TMDS, Oxygen CIS Profile Checks, HIPAA Technical Assessment*	*No*	*Cloudticity Oxygen performs GuardDuty checks and misconfiguration checks at least daily. If using Cloudticity Oxygen's CIS Profile Check service, these scans are run at least daily. If using Cloudticity hosted TMDS, checks are complete in real-time by instance based agents.*
0719.10m3Organizational.5	10.m Control of Technical Vulnerabilities	07 Vulnerability Management	3	The organization updates the list of information system vulnerabilities scanned within every thirty (30) days or when new vulnerabilities are identified and reported.	Yes	*Partial*	*TMDS, CIS Profile Checks*	*Yes*	*Vulnerability checks are updated in multiple Cloudticity Oxygen services each month.*
0720.07a1Organizational.4	07.a Inventory of Assets	07 Vulnerability Management	1	The organization's asset inventory does not duplicate other inventories unnecessarily and ensures their respective content is aligned.	Yes	*Partial*	*Oxygen Monitoring (Config Rules), CloudCheckr*	*No*	*Cloudticity provides access to Cloudcheckr for inventory management of the entire AWS account. Customer is reponsible for all assets outside of AWS services.*
0725.07a3Organizational.5	07.a Inventory of Assets	07 Vulnerability Management	3	The organization provides a updated inventory identifying assets with sensitive information (e.g., ePHI, PII) to the CIO or information security official, and the senior privacy official on an organization-defined basis, but no less than annually.	Yes	*Partial*	*Oxygen Tagging, CloudCheckr*	*No*	*Cloudcheckr can be used to provide an inventory based on the o2:phi tag*
0786.10m2Organizational.13	10.m Control of Technical Vulnerabilities	07 Vulnerability Management	2	A prioritization process is implemented to determine which patches are applied across the organizations systems.	Yes	*Partial*	*Patching*	*No*	*If using Cloudticity provided patching*
0787.10m2Organizational.14	10.m Control of Technical Vulnerabilities	07 Vulnerability Management	2	Patches installed in the production environment are also installed in the organizations disaster recovery environment in a timely manner.	Yes	*Not Applicable - Cloudticity Architecture Principles do not require a separate DR environment. AWS services are architected in a highly available manner using multiple Availability Zones (AZs).*	*N/A*	*No*	*All customers are moved to highly available architectures through their lifecycle*
0805.01m1Organizational.12	01.m Segregation in Networks	08 Network Protection	1	The organization's security gateways (e.g. firewalls) enforce security policies and are configured to filter traffic between domains, block unauthorized access, and are used to maintain segregation between internal wired, internal wireless, and external network segments (e.g., the Internet) including DMZs and enforce access control policies for each of the domains.	Yes	*Partial*	*Infrastructure Orchestration, Security Group Management*	*Yes*	*VPC, Security Groups, and Network Diagram*
0806.01m2Organizational.12356	01.m Segregation in Networks	08 Network Protection	2	The organizations network is logically and physically segmented with a defined security perimeter and a graduated set of controls, including subnetworks for publicly accessible system components that are logically separated from the internal network, based on organizational requirements; and traffic is controlled based on functionality required and classification of the data/systems based on a risk assessment and their respective security requirements.	Yes	*Partial*	*Infrastructure Orchestration, Security Group Management*	*Yes*	*VPC, Security Groups, and Network Diagram*
0808.10b2System.3	10.b Input Data Validation	08 Network Protection	2	For any public-facing Web applications, application-level firewalls have been implemented to control traffic. For any public-facing applications that are not Web-based, the organization has implemented a network-based firewall specific to the application type. If the traffic to the public-facing application is encrypted, ensuring that the device either sits behind the encryption or is capable of decrypting the traffic prior to analysis.	No	*Partial*	*Infrastructure Orchestration, Security Group Management, Quarterly Reviews*	*No*	*Cloudticity hosted TMDS, WAF's, Security groups, AWS Shield*
0809.01n2Organizational.1234	01.n Network Connection Control	08 Network Protection	2	Network traffic is controlled in accordance with the organizations access control policy through firewall and other network-related restrictions for each network access point or external telecommunication service's managed interface.	Yes	*Partial*	*Infrastructure Orchestration, Security Group Management, Quarterly Reviews*	*Yes*	
0810.01n2Organizational.5	01.n Network Connection Control	08 Network Protection	2	Transmitted information is secured and, at a minimum, encrypted over open, public networks.	Yes	*Partial*	*TMDS, Infrastructure Orchestration (WAF, ALB), Security Group Management, Quarterly Reviews*	*No*	
08101.09m2Organizational.14	09.m Network Controls	08 Network Protection	2	The organizations uses secured and encrypted communication channels when migrating physical servers, applications or data to virtualized servers.	Yes	*Partial*	*Infrastructure Orchestration*	*No*	*If using Cloudticity for migration professional services*
0811.01n2Organizational.6	01.n Network Connection Control	08 Network Protection	2	Exceptions to the traffic flow policy are documented with a supporting mission/business need, duration of the exception, and reviewed at least annually; traffic flow policy exceptions are removed when no longer supported by an explicit mission/business need.	Yes	*Partial*	*CloudCheckr using ignored best practice checks*	*No*	
0814.01n1Organizational.12	01.n Network Connection Control	08 Network Protection	1	The abilty of users to connect to the internal network is restricted using a deny-by-default and allow-by-exception policy at managed interfaces according to the access control policy and the requirements of clinical and business applications.	Yes	*Partial*	*Security Group Management*	*Yes*	*Security Groups configuration and management*
0816.01w1System.1	01.w Sensitive System Isolation	08 Network Protection	1	The sensitivity of applications/systems is explicitly identified and documented by the application/system owner.	No	*Partial*	*Oxygen Tagging, CloudCheckr*	*No*	*Cloudticity manages classification tags on AWS resources in coordination with customers, including o2:phi, o2:environment, o2:instance: backups:type, o2:platform, and others. Customer is responsible for non-AWS assets.*
0817.01w2System.123	01.w Sensitive System Isolation	08 Network Protection	2	Unless the risk is identified and accepted by the data owner, sensitive systems are isolated (physically or logically) from non-sensitive applications/systems.	No	*Partial*	*Oxygen Tagging, Infrastructure Orchestration*	*No*	*Cloudticity manages classification tags on AWS resources in coordination with customers, including o2:phi, o2:environment, o2:instance: backups:type, o2:platform, and others. Customer is responsible for non-AWS assets.*
0819.09m1Organizational.23	09.m Network Controls	08 Network Protection	1	A current network diagram (including wireless networks) exists and is updated whenever there are network changes and no less than every six months.	Yes	*Partial*	*Quarterly Reviews*	*No*	*There were network diagrams in place. Why are these no longer updated? I believe Matt kept them up-to-date. Cloudticity provides a network diagram for AWS resources upon request.*
0820.09m2Organizational.1	09.m Network Controls	08 Network Protection	2	The organization uniquely identifies and authenticates network devices that require authentication mechanisms before establishing a connection, that at a minimum, use shared information (i.e., MAC or IP address) and access control lists to control remote network access.	Yes	*Partial*	*N/A*	*Yes*	*N/A*
0821.09m2Organizational.2	09.m Network Controls	08 Network Protection	2	The organization tests and approves all network connections and firewall, router, and switch configuration changes prior to implementation. Any deviations from the standard configuration or updates to the standard configuration are documented and approved in a change control system. All new configuration rules beyond a baseline-hardened configuration that allow traffic to flow through network security devices, such as firewalls and network-based IPS, are also documented and recorded, with a specific business reason for each change, a specific individuals name responsible for that business need, and an expected duration of the need.	Yes	*Partial*	*Security Group Management, Quarterly Reviews*	*Yes*	*If using Cloudticity managed Palo Alto or Cloudticity managed security groups (Zendesk/Teamwork are Change Control Mechanisms)*

0822.09m2Organizational.4	09.m Network Controls	08 Network Protection	2	Firewalls restrict inbound and outbound traffic to the minimum necessary.	Yes	*Full*	*Cloudticity Oxygen, Security Group Management*	*No*	*For AWS Security Groups, Cloudticity checks for potentially hazardous open ports on a recurring basis through customer scheduled quarterly reviews and daily HIPAA technical assessments through the Oxygen Dashboards*
0825.09m3Organizational.23	09.m Network Controls	08 Network Protection	3	Technical tools such as an IDS/IPS are implemented and operating on the network perimeter and other key points to identify vulnerabilities, monitor traffic, and detect attack attempts and successful compromises, and mitigate threats; and these tools are updated on a regular basis.	Yes	*Full*	*Cloudticity Hosted TMDS*	*No*	*If using Cloudticity hosted TMDS*
0826.09m3Organizational.45	09.m Network Controls	08 Network Protection	3	Firewall and router configuration standards are defined and implemented and are reviewed every six months.	Yes	*Partial*	*Security Group Management, Quarterly Reviews*	*No*	*For AWS Security Groups, Cloudticity checks for potentially hazardous open ports on a recurring basis through customer scheduled quarterly reviews and daily HIPAA technical assessments through the Oxygen portal*
0828.09m3Organizational.8	09.m Network Controls	08 Network Protection	3	Quarterly network scans are performed to identify unauthorized components/devices.	Yes	*Partial*	*CloudCheckr, Oxygen Tagging*	*No*	*Cloudticity Oxygen provides alerts whenever an unauthorized access attempt is made to the AWS API (which covers all AWS services)*
0829.09m3Organizational.911	09.m Network Controls	08 Network Protection	3	The organization utilizes firewalls from at least two different vendors that employ stateful packet inspection (also known as dynamic packet filtering).	Yes	*Partial*	*Infrastructure Orchestration (WAF, Security Groups)*	*Yes*	*Customers may use both AWS Security Group and Palo Alto firewalls, both of which provide stateful packet inspection.*
0830.09m3Organizational.1012	09.m Network Controls	08 Network Protection	3	A DMZ is established with all database(s), servers and other system components storing or processing covered information placed behind it to limit external network traffic to the internal network.	Yes	*Partial*	*Infrastructure Orchestration (VPC, Public/Private Subnets, WAF, Security Groups)*	*No*	*This is the purpose of the VPC. All resources reside in the VPC. Who answered this, it's completely off-the-mark?*
0832.09m3Organizational.14	09.m Network Controls	08 Network Protection	3	The organization uses at least two DNS servers located on different subnets, which are geographically separated and perform different roles (internal and external) to eliminate single points of failure and enhance redundancy.	Yes	*Partial*	*Infrastructure Orchestration (Route 53)*	*No*	*Route 53 configuration and management*
0835.09n1Organizational.1	09.n Security of Network Services	08 Network Protection	1	Agreed services provided by a network service provider/manager are formally managed and monitored to ensure they are provided securely.	Yes	*Provided by AWS*	*N/A*	*No*	*Cloudticity is responsible for monitoring and managing AWS provided network services on behalf of customers.*
0837.09.n2Organizational.2	09.n Security of Network Services	08 Network Protection	2	Formal agreements with external information system providers include specific obligations for security and privacy.	Yes	*Partial*	*Cloudticity Agreements*	*No*	*Cloudticity is an external service provider with policy requirements that handle security and privacy through HITRUST CSF controls*
0850.01o1Organizational.12	01.o Network Routing Control	08 Network Protection	1	Routing controls are implemented through security gateways (e.g., firewalls) used between internal and external networks (e.g., the Internet and 3rd party networks).	Yes	*Partial*	*Infrastructure Orchestration (Security Groups)*	*No*	*Cloudticity is responsible for configuring, monitoring, and managing proper use of VPC's, routing tables, public/private subnets, and security groups.*
0859.09m1Organizational.78	09.m Network Controls	08 Network Protection	1	The organization ensures the security of information in networks, availability of network services and information services using the network, and the protection of connected services from unauthorized access.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
0860.09m1Organizational.9	09.m Network Controls	08 Network Protection	1	The organization formally manages equipment on the network, including equipment in user areas.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
0863.09m2Organizational.910	09.m Network Controls	08 Network Protection	2	The organization builds a firewall configuration that restricts connections between un-trusted networks and any system components in the covered information environment; and any changes to the firewall configuration are updated in the network diagram.	Yes	*Partial*	*Infrastructure Orchestration (Security Groups)*	*Yes*	*Cloudticity provides, as part of base AWS configuration, public and private subnets. Trusted networks reside in private subnets and require VPN access. The Palo does this also.*
0865.09m2Organizational.13	09.m Network Controls	08 Network Protection	2	The organization (i) authorizes connections from the information system to other information systems outside of the organization through the use of interconnection security agreements or other formal agreement; (ii) documents each connection, the interface characteristics, security requirements, and the nature of the information communicated; (iii) employs a deny all, permit by exception policy for allowing connections from the information system to other information systems outside of the organization; and (iv) applies a default-deny rule that drops all traffic via host-based firewalls or port filtering tools on its endpoints (workstations, servers, etc.), except those services and ports that are explicitly allowed.	Yes	*Partial*	*Security Group Management*	*No*	*Cloudticity uses Security Groups to...*
0866.09m3Organizational.1516	09.m Network Controls	08 Network Protection	3	The organization describes the groups, roles, and responsibilities for the logical management of network components and ensures coordination of and consistency in the elements of the network infrastructure.	Yes	*Full*	*Security Group Management, Quarterly Reviews, Cloudticity Account Configuration*	*No*	
0868.09m3Organizational.18	09.m Network Controls	08 Network Protection	3	The organization builds a firewall configuration to restrict inbound and outbound traffic to that which is necessary for the covered data environment.	Yes	*Full*	*Security Group Management, WAF Configuration*	*No*	*Cloudticity provides, as part of base configuration, a VPC with public and private subnets. All instances reside in the private subnets with load balancers in the public subnets. Traffic from public to private subnets uses SSL. Private subnets use NAT gateways for outbound communication.*
0870.09m3Organizational.20	09.m Network Controls	08 Network Protection	3	Access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.	Yes	*Full*	*Security Group Management*	*Yes*	
0871.09m3Organizational.22	09.m Network Controls	08 Network Protection	3	Authoritative DNS servers are segregated into internal and external roles.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
0887.09n2Organizational.5	09.n Security of Network Services	08 Network Protection	2	The organization requires external/outsourced service providers to identify the specific functions, ports, and protocols used in the provision of the external/outsourced services.	Yes	*Partial*	*TMDS, Security Group Management*	*Yes*	*Palo does this also.*
0888.09n2Organizational.6	09.n Security of Network Services	08 Network Protection	2	The contract with the external/outsourced service provider includes the specification that the service provider is responsible for the protection of covered information shared.	Yes	*Partial*	*Cloudticity Agreements*	*No*	
0894.01m2Organizational.7	01.m Segregation in Networks	08 Network Protection	2	Networks are segregated from production-level networks when migrating physical servers, applications or data to virtualized servers.	Yes	*Partial*	*Infrastructure Orchestration*	*No*	*Cloudticity facilitates migration from physical resources to AWS resources using segregated networks.*
0912.09s1Organizational.4	09.s Information Exchange Policies and Procedures	09 Transmission Protection	1	Cryptography is used to protect the confidentiality and integrity of remote access sessions to the internal network and to external systems.	Yes	*Full*	*Cloudticity Managed VPN*	*Yes*	*By default, all storage mediums on AWS are encrypted at rest by Cloudticity (Exception: root volumes). All transmissions from/to the AWS environment must be encrypted in transit using SSL. This is enforced on load balancers and through security groups, but is ultimately a customer's responsibility to make sure all applications are setup correctly for encryption in transit. Customers can access the private subnets (internal network) using a VPN solution such as OpenVPN, Palo Alto, or equivalent.*
0913.09s1Organizational.5	09.s Information Exchange Policies and Procedures	09 Transmission Protection	1	Strong cryptography protocols are used to safeguard covered information during transmission over less trusted / open public networks.	Yes	*Partial*	*Infrastructure Orchestration (ALB/ELB Configuration)*	*No*	*By default, all storage mediums on AWS are encrypted at rest by Cloudticity (Exception: root volumes). All transmissions from/to the AWS environment must be encrypted in transit using SSL. This is enforced on load balancers and through security groups, but is ultimately a customer's responsibility to make sure all applications are setup correctly for encryption in transit. Customers can access the private subnets (internal network) using a VPN solution such as OpenVPN, Palo Alto, or equivalent.*
0928.09v1Organizational.45	09.v Electronic Messaging	09 Transmission Protection	1	Stronger controls are implemented to protect certain electronic messages, and electronic messages are protected throughout the duration of its end-to-end transport path using cryptographic mechanisms unless protected by alternative measures.	Yes	*Partial*	*Infrastructure Orchestration (ALB/ELB Configuration)*	*No*	*N/A*
0939.09x2Organizational.12	09.x Electronic Commerce Services	09 Transmission Protection	2	The organization enters into and maintains a documented agreement for electronic commerce arrangements between trading partners on the agreed terms of trading, including details of authorization, as well as other agreements with information service and value-added network providers as needed.	Yes	*Partial*	*Cloudticity Agreements*	*No*	
0942.09x2Organizational.5	09.x Electronic Commerce Services	09 Transmission Protection	2	Cryptographic controls are used to enhance security, taking into account compliance with legal requirements.	Yes	*Partial*	*Infrastructure Orchestration (ALB/ELB Configuration)*	*No*	*If using Cloudticity provided hardened images with encryption-at-rest enabled on all storage resources*
0944.09y1Organizational.2	09.y On-line Transactions	09 Transmission Protection	1	Security is maintained through all aspects of the transaction.	No	*Partial*	*Infrastructure Orchestration (ALB/ELB Configuration)*	*No*	*If using Cloudticity provided hardened images with encryption-at-rest enabled on all storage resources*

0945.09y1Organizational.3	09.y On-line Transactions	09 Transmission Protection	1	Protocols used to communicate between all involved parties are secured using cryptographic techniques (e.g., SSL).	No	*Partial*	*Infrastructure Orchestration (ALB/ELB Configuration)*	*No*	*Cloudticity provides guidance around use of encryption-in-transit between all applications. Cloudticity enforces, through best practice guidance and Oxygen alerts, use of SSL on all public facing endpoints. Cloudticity also provide alerts for security groups open ports that may pose a security risk.*
0946.09y2Organizational.14	09.y On-line Transactions	09 Transmission Protection	2	The organization requires the use of encryption between, and the use of electronic signatures by, each of the parties involved in the transaction.	No	*Partial*	*Infrastructure Orchestration (ALB/ELB Configuration)*	*No*	*Cloudticity provides guidance around use of encryption-in-transit between all applications. Cloudticity enforces, through best practice guidance and Oxygen alerts, use of SSL on all public facing endpoints. Cloudticity Oxygen also provide alerts for security groups open ports that may pose a security risk.*
0947.09y2Organizational.2	09.y On-line Transactions	09 Transmission Protection	2	The organization ensures the storage of the transaction details are located outside of any publicly accessible environments (e.g., on a storage platform existing on the organization's intranet) and not retained and exposed on a storage medium directly accessible from the Internet.	No	*Partial*	*Infrastructure Orchestration, Quarterly Reviews*	*No*	
0948.09y2Organizational.3	09.y On-line Transactions	09 Transmission Protection	2	Where a trusted authority is used (e.g., for the purposes of issuing and maintaining digital signatures and/or digital certificates), security is integrated and embedded throughout the entire end-to-end certificate/signature management process.	No	*Partial*	*Infrastructure Orchestration (ACM)*	*No*	
0949.09y2Organizational.5	09.y On-line Transactions	09 Transmission Protection	2	The protocols used for communications are enhanced to address any new vulnerability, and the updated versions of the protocols are adopted as soon as possible.	No	*Partial*	*Infrastructure Orchestration (ALB/ELB Configuration)*	*No*	*For all non-application protocols (ALB for example)*
099.09m2Organizational.11	09.m Network Controls	09 Transmission Protection	2	The organization uses FIPS-validated cryptographic mechanisms during transmission to prevent unauthorized disclosure of information and detect changes to information unless otherwise protected by organization-defined alternative physical measures.	Yes	*Partial*	*KMS, CloudHSM*	*No*	
1002.01d1System.1	01.d User Password Management	10 Password Management	1	Passwords are not displayed when entered.	Yes	*Partial*	*AWS Console Access, Cloudticity Oxygen Access, Cloudticity hosted TMDS Access*	*No*	*N/A*
1003.01d1System.3	01.d User Password Management	10 Password Management	1	User identities are verified prior to performing password resets.	Yes	*Partial*	*AWS Console Access, Cloudticity Oxygen Access, Cloudticity hosted TMDS Access*	*No*	*N/A*
1004.01d1System.8913	01.d User Password Management	10 Password Management	1	The organization maintains a list of commonly-used, expected or compromised passwords, and updates the list at least every 180 days and when organizational passwords are suspected to have been compromised, either directly or indirectly; verifies, when users create or update passwords, that the passwords are not found on the organization-defined list of commonly-used, expected or compromised passwords; allows users to select long passwords and passphrases, including spaces and all printable characters; and employs automated tools to assist the user in selecting strong passwords and authenticators.	Yes	*Partial*	*AWS Console Access*	*No*	*N/A*
1009.01d2System.4	01.d User Password Management	10 Password Management	2	Temporary passwords are unique and not guessable.	Yes	*Partial*	*AWS Console Access*	*No*	*N/A*
1027.01d2System.6	01.d User Password Management	10 Password Management	2	Electronic signatures that are not based upon biometrics employ at least two distinct identification components that are administered and executed.	Yes	*Partial*	*AWS Console Access*	*No*	*N/A*
1031.01d1System.34510	01.d User Password Management	10 Password Management	1	The organization changes passwords for default system accounts, whenever there is any indication of password compromise, at first logon following the issuance of a temporary password, and requires immediate selection of a new password upon account recovery.	Yes	*Partial*	*AWS Console Access (including Root Account Ownership)*	*No*	*Cloudticity Oxygen monitors IAM user accounts to alert on password and access key rotation needs. Cloudticity facilitates user management and password configuration for AWS accounts.*
1106.01b1System.1	01.b User Registration	11 Access Control	1	User identities are verified prior to establishing accounts.	Yes	*Partial*	*Cloudticity Support*	*No*	*Yes, for application user registration and deregistration for granting and revoking access. This also includes AWS user management if utilizing a third party directory service for SSO to AWS, like Active Directory.*
1107.01b1System.2	01.b User Registration	11 Access Control	1	Default and unnecessary system accounts are removed, disabled, or otherwise secured (e.g., the passwords are changed and privileges are reduced to the lowest levels of access.)	Yes	*Partial*	*AWS Console Access (including Root Account Ownership), Quarterly Reviews*	*No*	*Yes, for application user registration and deregistration for granting and revoking access. This also includes AWS user management if utilizing a third party directory service for SSO to AWS, like Active Directory.*
1108.01b1System.3	01.b User Registration	11 Access Control	1	Account managers are notified when users' access rights change (e.g., termination, change in position) and modify the user's account accordingly.	Yes	*Partial*	*Cloudticity Support, Quarterly Reviews*	*No*	*Yes, for application user registration and deregistration for granting and revoking access. This also includes AWS user management if utilizing a third party directory service for SSO to AWS, like Active Directory.*
1109.01b1System.479	01.b User Registration	11 Access Control	1	User registration and de-registration, at a minimum, communicate relevant policies to users and require acknowledgement (e.g. signed or captured electronically), check authorization and minimum level of access necessary prior to granting access, ensure access is appropriate to the business and/or clinical needs (consistent with sensitivity/risk and does not violate segregation of duties requirements), address termination and transfer, ensure default accounts are removed and/or renamed, remove or block critical access rights of users who have changed roles or jobs, and automatically remove or disable inactive accounts.	Yes	*Partial*	*Cloudticity Support, Quarterly Reviews*	*No*	*Yes, for application user registration and deregistration for granting and revoking access. This also includes AWS user management if utilizing a third party directory service for SSO to AWS, like Active Directory.*
11109.01q1Organizational.57	01.q User Identification and Authentication	11 Access Control	1	The organization ensures that redundant user IDs are not issued to other users and that all users are uniquely identified and authenticated for both local and remote access to information systems.	Yes	*Partial*	*Cloudticity Support, Quarterly Reviews*	*No*	*Yes, for application user registration and deregistration for granting and revoking access. This also includes AWS user management if utilizing a third party directory service for SSO to AWS, like Active Directory.*
1111.01b2System.1	01.b User Registration	11 Access Control	2	Group, shared or generic accounts and passwords (e.g., for first-time log-on) are not used.	Yes	*Partial*	*Cloudticity Support, Quarterly Reviews*	*No*	*Cloudticity does not allow shared, group, or generic accounts. Unique individual accounts are issued per employee*
11112.01q2Organizational.67	01.q User Identification and Authentication	11 Access Control	2	The information system employs replay-resistant authentication mechanisms such as nonce, one-time passwords, or time stamps to secure network access for privileged accounts; and, for hardware token-based authentication, employs mechanisms that satisfy minimum token requirements discussed in NIST SP 800-63-2, Electronic Authentication Guideline.	Yes	*Partial*	*Baseline AWS Configuration with password controls and forced MFA*	*No*	*Yes, for application user registration and deregistration for granting and revoking access. This also includes AWS user management if utilizing a third party directory service for SSO to AWS, like Active Directory.*
11113.01q3Organizational.1	01.q User Identification and Authentication	11 Access Control	3	The organization employs multifactor authentication for network access to privileged and non-privileged accounts, such that one of the factors is provided by a device separate from the system gaining access, and for local access to privileged accounts (including those used for non-local maintenance and diagnostic sessions).	Yes	*Partial*	*Baseline AWS Configuration with password controls and forced MFA*	*No*	
11154.02i1Organizational.5	1	11 Access Control	1	Access rights to information assets and facilities is reduced or removed before the employment or other workforce arrangement terminates or changes, depending on the evaluation of risk factors.	No	*Partial*	*Cloudticity Support, Quarterly Reviews*	*No*	*Cloudticity facilitates AWS user management using Zendesk support tickets for change management.*
1118.01j2Organizational.124	01.j User Authentication for External Connections	11 Access Control	2	The organization has implemented encryption (e.g. VPN solutions or private lines) and logs remote access to the organization's network by employees, contractors or third party.	Yes	*Full*	*Palo (Global Protect)*	*Yes*	
11180.01c3System.6	01.c Privilege Management	11 Access Control	3	Access to management functions or administrative consoles for systems hosting virtualized systems are restricted to personnel based upon the principle of least privilege and supported through technical controls.	Yes	*Partial*	*AWS Console Access*	*No*	*Why TMDS?*
1120.09ab3System.9	09.ab Monitoring System Use	11 Access Control	3	Unauthorized remote connections to the information systems are monitored and reviewed at least quarterly, and appropriate action is taken if an unauthorized connection is discovered.	Yes	*Partial*	*Oxygen Monitoring (GuardDuty)*	*No*	*Alerts for Unauthorized Access Attempts*
11219.01b1Organizational.10	01.b User Registration	11 Access Control	1	The organization maintains a current listing of all workforce members (individuals, contractors and Business Associates) with access to PHI.	Yes	*Partial*	*IAM User Management*	*No*	*Cloudticity maintains a current listing of all workforce members with access to customer data. This is controlled through Google Authentication controls.*
1122.01q1System.1	01.q User Identification and Authentication	11 Access Control	1	Unique IDs that can be used to trace activities to the responsible individual are required for all types of organizational and non-organizational users.	Yes	*Partial*	*IAM User Management, CloudTrail, S3 Access Logs, Quarterly Reviews*	*Yes*	*Cloudticity configures unique IAM users, groups, and roles for accessing information systems. Customer is responsible for all application users and unique ID's.*
11220.01b1System.10	01.b User Registration	11 Access Control	1	User registration and de-registration formally address establishing, activating, modifying, reviewing, disabling and removing accounts.	Yes	*Partial*	*IAM User Management, CloudTrail, S3 Access Logs, Quarterly Reviews*	*No*	*Cloudticity is responible for user management within the AWS console. Customer is advised to submit a Zendesk support ticket for changes, additions, and removals.*

1125.01q2System.1	01.q User Identification and Authentication	11 Access Control	2	Multi-factor authentication methods are used in accordance with organizational policy, (e.g., for remote network access).	Yes	*Partial*	*Cloudticity AWS User Management requires MFA, AWS console sign in is required for Session Management through the console.*	*No*	*Yes, for application user registration and deregistration for granting and revoking access. This also includes AWS user management if utilizing a third party directory service for SSO to AWS, like Active Directory.*
1128.01q2System.5	01.q User Identification and Authentication	11 Access Control	2	Help desk support requires user identification for any transaction that has information security implications.	Yes	*Partial*	*AWS User Management through Cloudticity support requires approval of additions and terminations*	*No*	*Yes, for application user registration and deregistration for granting and revoking access. This also includes AWS user management if utilizing a third party directory service for SSO to AWS, like Active Directory.*
1132.01v2System.3	01.v Information Access Restriction	11 Access Control	2	Covered information is encrypted when stored in non-secure areas and, if not encrypted at rest, the organization must document its rationale.	Yes	*Partial*	*Infrastructure Orchestration (Encrypted secondary volumes)*	*No*	*By default, all storage mediums on AWS are encrypted at rest by Cloudticity (Exception: root volumes). All transmissions from/to the AWS environment must be encrypted in transit using SSL. This is enforced on load balancers and through security groups, but is ultimately a customer's responsibility to make sure all applications are setup correctly for encryption in transit. Customers can access the private subnets (internal network) using a VPN solution such as OpenVPN, Palo Alto, or equivalent.*
1135.02i1Organizational.1234	02.i Removal of Access Rights	11 Access Control	1	Upon termination or changes in employment for employees, contractors, third-party users or other workforce arrangement, physical and logical access rights and associated materials (e.g., passwords, keycards, keys, documentation that identify them as current members of the organization) are removed or modified to restrict access within 24 hours and old accounts are closed after 90 days of opening new accounts.	Yes	*Partial*	*AWS User Management through Cloudticity support requires approval of additions and terminations, Quarterly Reviews*	*No*	*Yes, for application user registration and deregistration for granting and revoking access. This also includes AWS user management if utilizing a third party directory service for SSO to AWS, like Active Directory.*
1138.06e2Organizational.12	06.e Prevention of Misuse of Information Assets	11 Access Control	2	Computer login banners are displayed outlining the terms and conditions of access and must be accepted before access is granted.	Yes	*Partial*	*Hardened Images*	*No*	*Need to confirm that hardened images contain banner warning.*
1139.01b1System.68	01.b User Registration	11 Access Control	1	Account types are identified (individual, shared/group, system, application, guest/anonymous, emergency and temporary), conditions for group and role membership are established, and, if used, shared/group account credentials are modified when users are removed from the group.	Yes	*Partial*	*Cloudticity Support, IAM User Management*	*No*	*Yes, for application user registration and deregistration for granting and revoking access. This also includes AWS user management if utilizing a third party directory service for SSO to AWS, like Active Directory.*
1143.01c1System.123	01.c Privilege Management	11 Access Control	1	Privileges are formally authorized and controlled, allocated to users on a need-to-use and event-by-event basis for their functional rol (e.g., user or administrator), and documented for each system product/element.	Yes	*Partial*	*Cloudticity Support, IAM User Management*	*No*	*Yes, for application privileges including audit logs/behavior, boundary protection system rules, access authorizations, authentication parameters, and system configurations/parameters. This also includes AWS user privileges if utilizing a third party directory service for SSO to AWS, like Active Directory.*
1144.01c1System.4	01.c Privilege Management	11 Access Control	1	The organization explicitly authorizes access to specific security relevant functions (deployed in hardware, software, and firmware) and security-relevant information.	Yes	*Partial*	*Cloudticity Support, IAM User Management*	*No*	*Yes, for application privileges including audit logs/behavior, boundary protection system rules, access authorizations, authentication parameters, and system configurations/parameters. This also includes AWS user privileges if utilizing a third party directory service for SSO to AWS, like Active Directory.*
1145.01c2System.1	01.c Privilege Management	11 Access Control	2	Role-based access control is implemented and capable of mapping each user to one or more roles, and each role to one or more system functions.	Yes	*Partial*	*Cloudticity Support, IAM User Management*	*No*	*Yes, for application privileges including audit logs/behavior, boundary protection system rules, access authorizations, authentication parameters, and system configurations/parameters. This also includes AWS user privileges if utilizing a third party directory service for SSO to AWS, like Active Directory.*
1150.01c2System.10	01.c Privilege Management	11 Access Control	2	The access control system for the system components storing, processing or transmitting covered information is set with a default "deny-all" setting.	Yes	*Partial*	*Infrastructure Orchestration (Security Groups, Bucket Policies)*	*No*	*Yes, for application privileges including audit logs/behavior, boundary protection system rules, access authorizations, authentication parameters, and system configurations/parameters. This also includes AWS user privileges if utilizing a third party directory service for SSO to AWS, like Active Directory.*
1151.01c3System.1	01.c Privilege Management	11 Access Control	3	The organization limits authorization to privileged accounts on information systems to a pre-defined subset of users.	Yes	*Partial*	*Cloudticity Support (IAM User Management), Quarterly Reviews*	*No*	
1152.01c3System.2	01.c Privilege Management	11 Access Control	3	The organization audits the execution of privileged functions on information systems and ensures information systems prevent non-privileged users from executing privileged functions.	Yes	*Partial*	*Cloudticity Support (IAM User Management), Quarterly Reviews*	*No*	
1166.01e1System.12	01.e Review of User Access Rights	11 Access Control	1	User access rights are reviewed after any changes and reallocated as necessary.	Yes	*Partial*	*Cloudticity Support (IAM User Management)*	*No*	*Cloudticity provides regular reviews of user access rights for applications. This also includes AWS user access rights if utilizing a third party directory service for SSO to AWS, like Active Directory.*
1168.01e2System.2	01.e Review of User Access Rights	11 Access Control	2	The organization reviews critical system accounts and privileged access rights every 60 days; all other accounts, including user access and changes to access authorizations, are reviewed every 90 days.	Yes	*Partial*	*Quarterly Reviews*	*No*	
1175.01j1Organizational.8	01.j User Authentication for External Connections	11 Access Control	1	Remote access to business information across public networks only takes place after successful identification and authentication.	Yes	*Partial*	*Cloudticity Managed VPN*	*Yes*	*N/A*
1177.01j2Organizational.6	01.j User Authentication for External Connections	11 Access Control	2	User IDs assigned to vendors are reviewed in accordance with the organization's access review policy, at a minimum annually.	Yes	*Partial*	*Quarterly Reviews*	*No*	
1192.01l1Organizational.1	01.l Remote Diagnostic and Configuration Port Protection	11 Access Control	1	Access to network equipment is physically protected.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1193.01l2Organizational.13	01.l Remote Diagnostic and Configuration Port Protection	11 Access Control	2	Controls for the access to diagnostic and configuration ports include the use of a key lock and the implementation of supporting procedures to control physical access to the port.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1194.01l2Organizational.2	01.l Remote Diagnostic and Configuration Port Protection	11 Access Control	2	Ports, services, and similar applications installed on a computer or network systems, which are not specifically required for business functionality, are disabled or removed.	Yes	*Partial*	*CIS Profile Checks, Quarterly Reviews, Security Groups*	*No*	
1195.01l3Organizational.1	01.l Remote Diagnostic and Configuration Port Protection	11 Access Control	3	The organization reviews the information system within every three hundred and sixty- five (365) days to identify and disables unnecessary and non-secure functions, ports, protocols, and/or services.	Yes	*Partial*	*CIS Profile Checks, Quarterly Reviews*	*No*	
1196.01l3Organizational.24	01.l Remote Diagnostic and Configuration Port Protection	11 Access Control	3	The organization identifies unauthorized (blacklisted) software on the information system, prevents program execution in accordance with a list of unauthorized (blacklisted) software programs, employs an allow-all, deny-by exception policy to prohibit execution of known unauthorized (blacklisted) software, and reviews and updates the list of unauthorized (blacklisted) software programs annually.	Yes	*Partial*	*TMDS*	*Yes*	*The Palo uses application controls (Example: Restrict media streaming)* *TMDS uses Application Control module to blacklist/whitelist*
1202.09aa1System.1	09.aa Audit Logging	12 Audit Logging & Monitoring	1	A secure audit record is created for all activities on the system (create, read, update, delete) involving covered information.	Yes	*Partial*	*Unified Logging, S3 Object Access Logging*	*No*	*Yes, for all customer applications.*
1203.09aa1System.2	09.aa Audit Logging	12 Audit Logging & Monitoring	1	Audit records include the unique user ID, unique data subject ID, function performed, and date/time the event was performed.	Yes	*Partial*	*Unified Logging*	*No*	*N/A*
1204.09aa1System.3	09.aa Audit Logging	12 Audit Logging & Monitoring	1	The activities of privileged users (administrators, operators, etc.) include the success/failure of the event, time the event occurred, the account involved, the processes involved, and additional information about the event.	Yes	*Partial*	*Unified Logging*	*No*	*N/A*
1206.09aa2System.23	09.aa Audit Logging	12 Audit Logging & Monitoring	2	Auditing is always available while the system is active and tracks key events, success/failed data access, system security configuration changes, privileged or utility use, any alarms raised, activation and de-activation of protection systems (e. g., A/V and IDS), activation and deactivation of identification and authentication mechanisms, and creation and deletion of system-level objects.	Yes	*Partial*	*TMDS, Infrastructure Orchestration (CloudTrail, S3 Object Level Access)*	*No*	
1207.09aa2System.4	09.aa Audit Logging	12 Audit Logging & Monitoring	2	Audit records are retained for 90 days and older audit records are archived for one year.	Yes	*Full*	*S3 Lifecycle Policies & Unified Logging & VPC Flow Logs, Cloudtrail*	*No*	
1208.09aa3System.1	09.aa Audit Logging	12 Audit Logging & Monitoring	3	Audit logs are maintained for management activities, system and application startup/shutdown/errors, file changes, and security policy changes.	Yes	*Partial*	*TMDS, Infrastructure Orchestration (CloudTrail, S3 Object Level Access)*	*No*	*AWS requires Cloudtrail and Config to be enabled*

1209.09aa3System.2	09.aa Audit Logging	12 Audit Logging & Monitoring	3	The information system generates audit records containing the following detailed information: (i) filename accessed; (ii) program or command used to initiate the event; and (iii) source and destination addresses.	Yes	*Partial*	*TMDS, Infrastructure Orchestration (CloudTrail, S3 Object Level Access)*	*No*	
12100.09ab2System.15	09.ab Monitoring System Use	12 Audit Logging & Monitoring	2	The organization monitors the information system to identify irregularities or anomalies that are indicators of a system malfunction or compromise and help confirm the system is functioning in an optimal, resilient and secure state.	Yes	*Partial*	*Unified Logging, Oxygen Monitoring (GuardDuty, Config Rules, CloudWatch Events)*	*No*	
12102.09ab1Organizational.4	09.ab Monitoring System Use	12 Audit Logging & Monitoring	1	The organization periodically tests its monitoring and detection processes, remediates deficiencies, and improves its processes.	Yes	*Partial*	*Cloudticity SDLC*	*No*	*Yes, for all customer applications.*
12103.09ab1Organizational.5	09.ab Monitoring System Use	12 Audit Logging & Monitoring	1	Information collected from multiple sources is aggregated for review.	Yes	*Partial*	*Unified Logging*	*No*	*N/A*
1212.09ab1System.1	09.ab Monitoring System Use	12 Audit Logging & Monitoring	1	All applicable legal requirements related to monitoring authorized access and unauthorized access attempts are met.	Yes	*Partial*	*Unified Logging*	*No*	*N/A*
1213.09ab2System.128	09.ab Monitoring System Use	12 Audit Logging & Monitoring	2	Automated systems deployed throughout the organization's environment are used to monitor key events and anomalous activity, and analyze system logs, the results of which are reviewed regularly.	Yes	*Partial*	*Unified Logging, Oxygen Monitoring (GuardDuty, Config Rules, CloudWatch Events, Cloudtrail)*	*No*	
1214.09ab2System.3456	09.ab Monitoring System Use	12 Audit Logging & Monitoring	2	Monitoring includes privileged operations, authorized access or unauthorized access attempts, including attempts to access deactivated accounts, and system alerts or failures.	Yes	*Partial*	*Oxygen Monitoring (GuardDuty, Config Rules), CloudCheckr*	*No*	
1216.09ab3System.12	09.ab Monitoring System Use	12 Audit Logging & Monitoring	3	Automated systems are used to review monitoring activities of security systems (e. g., IPS/IDS) and system records on a daily basis, and identify and document anomalies.	Yes	*Partial*	*Unified Logging, TMDS, Oxygen Monitoring (GuardDuty, Config Rules), CloudCheckr*	*No*	
1217.09ab3System.3	09.ab Monitoring System Use	12 Audit Logging & Monitoring	3	Alerts are generated for technical personnel to analyze and investigate suspicious activity or suspected violations.	Yes	*Partial*	*Unified Logging, TMDS, Oxygen Monitoring (GuardDuty, Config Rules)*	*No*	
1218.09ab3System.47	09.ab Monitoring System Use	12 Audit Logging & Monitoring	3	Automated systems support near real-time analysis and alerting of events (e.g., malicious code, potential intrusions) and integrate intrusion detection into access and flow control mechanisms.	Yes	*Partial*	*Unified Logging, TMDS, Oxygen Monitoring (GuardDuty, Config Rules)*	*No*	
1219.09ab3System.10	09.ab Monitoring System Use	12 Audit Logging & Monitoring	3	The information system is able to automatically process audit records for events of interest based on selectable criteria.	Yes	*Partial*	*Unified Logging*	*No*	
1220.09ab3System.56	09.ab Monitoring System Use	12 Audit Logging & Monitoring	3	Monitoring includes inbound and outbound communications and file integrity monitoring.	Yes	*Partial*	*TMDS*	*No*	
1222.09ab3System.8	09.ab Monitoring System Use	12 Audit Logging & Monitoring	3	The organization analyzes and correlates audit records across different repositories using a security information and event management (SIEM) tool or log analytics tools for log aggregation and consolidation from multiple systems/machines/devices, and correlates this information with input from non-technical sources to gain and enhance organization-wide situational awareness. Using the SIEM tool, the organization devise profiles of common events from given systems/machines/devices so that it can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.	Yes	*Partial*	*Unified Logging*	*No*	
1229.09c1Organizational.1	09.c Segregation of Duties	12 Audit Logging & Monitoring	1	Separation of duties is used to limit the risk of unauthorized or unintentional modification of information and systems.	Yes	*Full*	*IAM Users, Groups, and Roles Management*	*No*	
1230.09c2Organizational.1	09.c Segregation of Duties	12 Audit Logging & Monitoring	2	No single person is able to access, modify, or use information systems without authorization or detection.	Yes	*Partial*	*Cloudticity Workflow for AWS IAM User Management requires approval by primary technical contact, Quarterly Reviews*	*No*	
1270.09ad1System.12	09.ad Administrator and Operator Logs	12 Audit Logging & Monitoring	1	The organization ensures proper logging is enabled in order to audit administrator activities; and reviews system administrator and operator logs on a regular basis.	Yes	*Partial*	*Unified Logging, Infrastructure Orchestration (CloudTrail)*	*No*	
1271.09ad1System.1	09.ad Administrator and Operator Logs	12 Audit Logging & Monitoring	1	An intrusion detection system managed outside of the control of system and network administrators is used to monitor system and network administration activities for compliance.	Yes	*Partial*	*TMDS, Oxygen Monitoring (GuardDuty)*	*No*	*Yes, for all customer application administrators and customer system operators.*
1277.09c2Organizational.4	09.c Segregation of Duties	12 Audit Logging & Monitoring	2	The initiation of an event is separated from its authorization to reduce the possibility of collusion.	Yes	*Partial*	*Cloudticity Workflow for AWS IAM User Management requires approval by primary technical contact*	*No*	
1278.09c2Organizational.56	09.c Segregation of Duties	12 Audit Logging & Monitoring	2	The organization identifies duties that require separation and defines information system access authorizations to support separation of duties; and incompatible duties are segregated across multiple users to minimize the opportunity for misuse or fraud.	Yes	*Partial*	*Cloudticity Workflow for AWS IAM User Management requires approval by primary technical contact*	*No*	
1308.09j1Organizational.5	09.j Controls Against Malicious Code	13 Education, Training and Awareness	1	The organization prohibits users from installing unauthorized software, including data and software from external networks, and ensures users are made aware and trained on these requirements.	Yes	*Partial*	*TMDS (Application Control)*	*No*	*N/A*
1401.05i1Organizational.1239	05.i Identification of Risks Related to External Parties	14 Third Party Assurance	1	Access to the organizations information and systems by external parties is not permitted until due diligence has been conducted, the appropriate controls have been implemented, and a contract/agreement reflecting the security requirements is signed acknowledging they understand and accept their obligations.	Yes	*Partial*	*Cloudticity Agreements*	*No*	*N/A*
1403.05i1Organizational.67	05.i Identification of Risks Related to External Parties	14 Third Party Assurance	1	Access granted to external parties is limited to the minimum necessary and granted only for the duration required.	Yes	*Partial*	*Cloudticity Personnel*	*No*	*IAM User Management*
1404.05i2Organizational.1	05.i Identification of Risks Related to External Parties	14 Third Party Assurance	2	Due diligence of the external party includes interviews, document review, checklists, certification reviews (e.g. HITRUST) or other remote means.	Yes	*Full*	*Cloudticity HITRUST Audit Documentation*	*No*	
1406.05k1Organizational.110	05.k Addressing Security in Third Party Agreements	14 Third Party Assurance	1	A standard agreement with third parties is defined and includes the required security controls in accordance with the organization's security policies.	Yes	*Partial*	*Cloudticity Agreements*	*No*	*Cloudticity is a third party that notifies customers of transfers and terminations.* *Customer is responsible for all other third parties.*
1407.05k2Organizational.1	05.k Addressing Security in Third Party Agreements	14 Third Party Assurance	2	The specific limitations of access, arrangements for compliance auditing, penalties, and the requirement for notification of third party personnel transfers and terminations are identified in the agreement with the third party.	Yes	*Partial*	*Cloudticity Agreements*	*No*	
1408.09e1System.1	09.e Service Delivery	14 Third Party Assurance	1	Service Level Agreements (SLAs) or contracts with an agreed service arrangement address liability, service definitions, security controls, and other aspects of services management.	Yes	*Full*	*Cloudticity Agreements*	*No*	
1410.09e2System.23	09.e Service Delivery	14 Third Party Assurance	2	The organization addresses information security and other business considerations when acquiring systems or services; including maintaining security during transitions and continuity following a failure or disaster.	Yes	*Partial*	*Cloudticity Agreements*	*No*	
1411.09f1System.1	09.f Monitoring and Review of Third Party Services	14 Third Party Assurance	1	The results of monitoring activities of third-party services are compared against the Service Level Agreements or contracts at least annually.	Yes	*Partial*	*Cloudticity Agreements & SLA's*	*No*	
1412.09f2System.12	09.f Monitoring and Review of Third Party Services	14 Third Party Assurance	2	Regular progress meetings are conducted as required by the SLA to review reports, audit trails, security events, operational issues, failures and disruptions, and identified problems/issues are investigated and resolved accordingly.	Yes	*Partial*	*Cloudticity Agreements & SLA's*	*No*	
1413.09f2System.3	09.f Monitoring and Review of Third Party Services	14 Third Party Assurance	2	Network services are periodically audited to ensure that providers have implemented the required security features and meet the requirements agreed with management, including new and existing regulations.	Yes	*Provided by AWS*	*N/A*	*No*	*Yes, for all customer supplied third parties.*
1416.10l1Organizational.1	10.l Outsourced Software Development	14 Third Party Assurance	1	Where software development is outsourced, formal contracts are in place to address the ownership and security of the code and application.	Yes	*Partial*	*Cloudticity Agreements*	*No*	*N/A*
1422.05j2Organizational.3	05.j Addressing Security When Dealing with Customers	14 Third Party Assurance	2	All security requirements resulting from work with external parties or internal controls are reflected by the agreement with the external party.	Yes	*Partial*	*Cloudticity Agreements*	*No*	
1428.05k1Organizational.2	05.k Addressing Security in Third Party Agreements	14 Third Party Assurance	1	The organization identifies and mandates information security controls to specifically address supplier access to the organization's information and information assets.	Yes	*Partial*	*Cloudticity Agreements*	*No*	*Cloudticity is a third party with policies that address supplier access to information and assets.* *Customer is responsible for all other third parties.*
1429.05k1Organizational.34	05.k Addressing Security in Third Party Agreements	14 Third Party Assurance	1	The organization maintains written agreements (contracts) that include: (i) an acknowledgement that the third party (e.g., a service provider) is responsible for the security of the data and requirements to address the associated information security risks and (ii) requirements to address the information security risks associated with information and communications technology services (e.g., cloud computing services) and product supply chain.	Yes	*Partial*	*Cloudticity Agreements*	*No*	*Cloudticity is a third party with a signed BAA with each customer that addresses the security requirements.* *Customer is responsible for all other third parties.*
1430.05k1Organizational.56	05.k Addressing Security in Third Party Agreements	14 Third Party Assurance	1	The agreement ensures that there is no misunderstanding between the organization and the third party and satisfies the organization as to the indemnity of the third party.	Yes	*Partial*	*Cloudticity Agreements*	*No*	
1431.05k1Organizational.7	05.k Addressing Security in Third Party Agreements	14 Third Party Assurance	1	The organization establishes personnel security requirements, including security roles and responsibilities, for third-party providers that are coordinated and aligned with internal security roles and responsibilities.	Yes	*Partial*	*Cloudticity Agreements*	*No*	

1432.05k1Organizational.89	05.k Addressing Security in Third Party Agreements	14 Third Party Assurance	1	The organization ensures a screening process is carried out for contractors and third party users; and, where contractors are provided through an organization, (i) the contract with the organization clearly specifies the organization's responsibilities for screening and the notification procedures they need to follow if screening has not been completed or if the results give cause for doubt or concern and, in the same way, (ii) the agreement with the third party clearly specifies all responsibilities and notification procedures for screening.	Yes	*Partial*	*Cloudticity Agreements*	*No*	
1438.09e2System.4	09.e Service Delivery	14 Third Party Assurance	2	The service provider protects the company's data with reasonable controls (e.g., policies and procedures) designed to detect, prevent, and mitigate risk.	Yes	*Partial*	*Cloudticity Agreements*	*No*	*Yes, for all customer supplied third parties.*
1442.09f2System.456	09.f Monitoring and Review of Third Party Services	14 Third Party Assurance	2	The organization employs a service management relationship and process between itself and a third party to monitor (i) security control compliance by external service providers on an ongoing basis and (ii) network service features and service levels to detect abnormalities and violations.	Yes	*Partial*	*Cloudticity Agreements*	*No*	*Yes, for all customer supplied third parties.*
1450.05i2Organizational.2	05.i Identification of Risks Related to External Parties	14 Third Party Assurance	2	The organization obtains satisfactory assurances that reasonable information security exists across its information supply chain by performing an annual review, which includes all partners/third party providers upon which their information supply chain depends.	Yes	*Partial*	*Cloudticity Agreements*	*No*	
1464.09e2Organizational.5	09.e Service Delivery	14 Third Party Assurance	2	The organization restricts the location of facilities that process, transmit or store covered information (e.g., to those located in the United States), as needed, based on its legal, regulatory, contractual and other security and privacy-related obligations.	Yes	*Partial*	*Infrastructure Orchestration (Regions)*	*No*	*Yes, for all customer supplied third parties.*
1504.06e1Organizational.34	06.e Prevention of Misuse of Information Assets	15 Incident Management	1	Management approves the use of information assets and takes appropriate action when unauthorized activity occurs.	Yes	*Partial*	*Unified Logging, Oxygen Monitoring (Config Rules), Cloudticity Workflow for AWS IAM User Management requires approval by primary technical contact*	*No*	*IAM User Management with approval/change control through Cloudticity support*
1506.11a1Organizational.2	11.a Reporting Information Security Events	15 Incident Management	1	There is a point of contact for reporting information security events who is made known throughout the organization, always available, and able to provide adequate and timely response. The organization maintains a list of third-party contact information, which can be used to report a security incident.	Yes	*Partial*	*Oxygen Monitoring (Alerts are sent to the technical contact or distribution list containing the point-of-contact)*	*No*	*Yes, for all customer applications or customer identified events.*
1512.11a2Organizational.8	11.a Reporting Information Security Events	15 Incident Management	2	Intrusion detection/information protection system (IDS/IPS) alerts are utilized for reporting information security events.	Yes	*Partial*	*TMDS, Oxygen Monitoring (GuardDuty)*	*No*	
1517.11c1Organizational.3	11.c Responsibilities and Procedures	15 Incident Management	1	There is a point of contact who is responsible for coordinating incident responses and has the authority to direct actions required in all phases of the incident response process.	Yes	*Partial*	*Oxygen Monitoring (Alerts are sent to the technical contact or distribution list containing the point-of-contact)*	*No*	*Yes, for all customer applications or customer identified events.*
1561.11d2Organizational.14	11.d Learning from Information Security Incidents	15 Incident Management	2	The organization has implemented an incident handling capability for security incidents that addresses (i) policy (setting corporate direction) and procedures defining roles and responsibilities; (ii) incident handling procedures (business and technical); (iii) communication; (iv) reporting and retention; and (v) references to a vulnerability management program.	Yes	*Partial*	*Oxygen Monitoring (Alerts are sent to the technical contact or distribution list containing the point-of-contact)*	*No*	
1562.11d2Organizational.2	11.d Learning from Information Security Incidents	15 Incident Management	2	The organization coordinates incident handling activities with contingency planning activities.	Yes	*Partial*	*Cloudticity Workflow and Incident Management of incidents found by Cloudticity Oxygen. Cloudticity DR*	*No*	
1589.11c1Organizational.5	11.c Responsibilities and Procedures	15 Incident Management	1	The organization tests and/or exercises its incident response capability regularly.	Yes	*Partial*	*Cloudticity DR, Failover*	*Yes*	*Yes, for all customer applications or customer identified events.*
1601.12c1Organizational.1238	12.c Developing and Implementing Continuity Plans Including Information Security	16 Business Continuity & Disaster Recovery	1	The organization can recover and restore business operations and establish an availability of information in the time frame required by the business objectives and without a deterioration of the security measures.	Yes	*Partial*	*Cloudticity DR*	*No*	*If utilizing Cloudticity provided DR for all AWS services.*
1602.12c1Organizational.4567	12.c Developing and Implementing Continuity Plans Including Information Security	16 Business Continuity & Disaster Recovery	1	The contingency program addresses required capacity, identifies critical missions and business functions, defines recovery objectives and priorities, and identifies roles and responsibilities.	Yes	*Partial*	*Cloudticity DR*	*No*	*If utilizing Cloudticity provided DR for all AWS services.*
1604.12c2Organizational.16789	12.c Developing and Implementing Continuity Plans Including Information Security	16 Business Continuity & Disaster Recovery	2	Alternative storage and processing sites are identified (permanent and/or temporary) at a sufficient distance from the primary facility and configured with security measures equivalent to the primary site, and the necessary third party service agreements have been established to allow for the resumption of information systems operations of critical business functions within the time-period defined (e.g. priority of service provisions) based on a risk assessment, including Recovery Time Objectives (RTO), in accordance with the organizations availability requirements.	Yes	*Partial*	*Cloudticity DR, Infrastructure Orchestration (High Availability)*	*No*	*Multi-AZ*
1605.12c2Organizational.2	12.c Developing and Implementing Continuity Plans Including Information Security	16 Business Continuity & Disaster Recovery	2	Emergency power and backup telecommunications are available at the main site.	Yes	*Provided by AWS*	*N/A*	*No*	*N/A*
1607.12c2Organizational.4	12.c Developing and Implementing Continuity Plans Including Information Security	16 Business Continuity & Disaster Recovery	2	Business continuity planning includes identification and agreement on all responsibilities, business continuity processes, and the acceptable loss of information and services.	Yes	*Partial*	*Cloudticity DR*	*No*	*If using Cloudticity DR*
1616.09l1Organizational.16	09.l Back-up	16 Business Continuity & Disaster Recovery	1	Backup copies of information and software are made and tests of the media and restoration procedures are regularly performed at appropriate intervals.	Yes	*Partial*	*Oxygen EC2 Backups*	*No*	
1617.09l1Organizational.23	09.l Back-up	16 Business Continuity & Disaster Recovery	1	A formal definition of the level of backup required for each system is defined and documented including how each system will be restored, the scope of data to be imaged, frequency of imaging, and duration of retention based on relevant contractual, legal, regulatory and business requirements.	Yes	*Partial*	*Cloudticity DR, Oxygen EC2 Backups*	*No*	*If using Cloudticity Oxygen backups with Cloudticity provided DR*
1618.09l1Organizational.45	09.l Back-up	16 Business Continuity & Disaster Recovery	1	The backups are stored in a physically secure remote location, at a sufficient distance to make them reasonably immune from damage to data at the primary site, and reasonable physical and environmental controls are in place to ensure their protection at the remote location.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1619.09l1Organizational.7	09.l Back-up	16 Business Continuity & Disaster Recovery	1	Inventory records for the backup copies, including content and current location, are maintained.	Yes	*Partial*	*AWS Console > EC2 > AMIs page*	*No*	
1621.09l2Organizational.1	09.l Back-up	16 Business Continuity & Disaster Recovery	2	Automated tools are used to track all backups.	Yes	*Partial*	*Oxygen EC2 Backups*	*No*	*Automated alerts exist for failed backup creation*
1622.09l2Organizational.23	09.l Back-up	16 Business Continuity & Disaster Recovery	2	The integrity and security of the backup copies are maintained to ensure future availability, and any potential accessibility problems with the backup copies are identified and mitigated in the event of an area-wide disaster.	Yes	*Partial*	*Oxygen EC2 Backups*	*No*	
1623.09l2Organizational.4	09.l Back-up	16 Business Continuity & Disaster Recovery	2	Covered information is backed-up in an encrypted format to ensure confidentiality.	Yes	*Partial*	*Oxygen EC2 Backups*	*No*	
1634.12b1Organizational.1	12.b Business Continuity and Risk Assessment	16 Business Continuity & Disaster Recovery	1	The organization identifies the critical business processes requiring business continuity.	Yes	*Partial*	*Cloudticity DR*	*No*	*If utilizing Cloudticity provided DR for all AWS services.*
1670.12d2Organizational.1	12.d Business Continuity Planning Framework	16 Business Continuity & Disaster Recovery	2	Each business unit creates at a minimum one business continuity plan.	Yes	*Partial*	*Cloudticity DR*	*No*	*If using Cloudticity DR*
1671.12d2Organizational.2	12.d Business Continuity Planning Framework	16 Business Continuity & Disaster Recovery	2	The organization ensures business continuity matters are always timely addressed in its management of system changes.	Yes	*Partial*	*Cloudticity DR*	*No*	*If using Cloudticity DR*
1672.12d2Organizational.3	12.d Business Continuity Planning Framework	16 Business Continuity & Disaster Recovery	2	The business continuity planning framework addresses the specific, minimal set of information security requirements as well as (i) temporary operational procedures to follow pending completion of recovery and restoration, and (ii) the responsibilities of the individuals, describing who is responsible for executing which component of the plan (alternatives should be nominated as required).	Yes	*Partial*	*Cloudticity DR*	*No*	*If using Cloudticity DR*
1735.03d2Organizational.23	03.d Risk Evaluation	17 Risk Management	2	Risk assessments are conducted whenever there is a significant change in the environment, or a change that could have a significant impact, and the results of the assessments are included in the change management process, so they may guide the decisions within the change management process (e.g., approvals for changes).	Yes	*Partial*	*Change Requests*	*No*	*Change Management Process*
1788.10a2Organizational.2	10.a Security Requirements Analysis and Specification	17 Risk Management	2	The organization has established and appropriately protected secure development environments for system development and integration efforts that cover the entire system development life cycle.	Yes	*Partial*	*Cloudticity Oxygen, Infrastructure Orchestration*	*No*	
1789.10a2Organizational.3	10.a Security Requirements Analysis and Specification	17 Risk Management	2	The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of security requirements and controls in developed and acquired information systems.	Yes	*Partial*	*Infrastructure Orchestration*	*No*	
1790.10a2Organizational.45	10.a Security Requirements Analysis and Specification	17 Risk Management	2	The organization includes business requirements for the availability of information systems when specifying the security requirements; and, where availability cannot be guaranteed using existing architectures, redundant components or architectures are considered along with the risks associated with implementing such redundancies.	Yes	*Partial*	*Quarterly Reviews*	*No*	

1791.10a2Organizational.6	10.a Security Requirements Analysis and Specification	17 Risk Management	2	Specifications for the security control requirements state automated controls will be incorporated in the information system, supplemented by manual controls as needed, as evidenced throughout the SDLC.	Yes	*Partial*	*Cloudticity Oxygen*	*No*	*For all AWS service configuration*
1801.08b1Organizational.124	08.b Physical Entry Controls	18 Physical & Environmental Security	1	Visitor and third-party support access is recorded and supervised unless previously approved.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1802.08b1Organizational.3	08.b Physical Entry Controls	18 Physical & Environmental Security	1	Areas where sensitive information (e.g., covered information, payment card data) is stored or processed are controlled and restricted to authorized individuals only.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1803.08b1Organizational.5	08.b Physical Entry Controls	18 Physical & Environmental Security	1	Repairs or modifications to the physical components of a facility which are related to security (e.g., hardware, walls, doors and locks) are documented and retained in accordance with the organization's retention policy.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1804.08b2Organizational.12	08.b Physical Entry Controls	18 Physical & Environmental Security	2	A visitor log containing appropriate information is reviewed monthly and maintained for at least two years.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1805.08b2Organizational.3	08.b Physical Entry Controls	18 Physical & Environmental Security	2	Physical authentication controls are used to authorize and validate access.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1806.08b2Organizational.4	08.b Physical Entry Controls	18 Physical & Environmental Security	2	An audit trail of all physical access is maintained.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1807.08b2Organizational.56	08.b Physical Entry Controls	18 Physical & Environmental Security	2	Visible identification that clearly identifies the individual is required to be worn by employees, visitors, contractors and third parties.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1808.08b2Organizational.7	08.b Physical Entry Controls	18 Physical & Environmental Security	2	Physical access rights are reviewed every ninety (90) days and updated accordingly.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1809.08b3Organizational.1	08.b Physical Entry Controls	18 Physical & Environmental Security	3	Doors to internal secure areas lock automatically, implement a door delay alarm, and are equipped with electronic locks.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1810.08b3Organizational.2	08.b Physical Entry Controls	18 Physical & Environmental Security	3	Inventories of physical access devices are performed every ninety (90) days.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
18108.08j1Organizational.1	08.j Equipment Maintenance	18 Physical & Environmental Security	1	The organization formally addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance requirements for its equipment maintenance program (e.g., through policy, standards, guidelines, and procedures).	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
18109.08j1Organizational.4	08.j Equipment Maintenance	18 Physical & Environmental Security	1	The organization maintains a list of authorized maintenance organizations or personnel, ensures that non-escorted personnel performing maintenance on the information system have required access authorizations, and designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1811.08b3Organizational.3	08.b Physical Entry Controls	18 Physical & Environmental Security	3	Combinations and keys for organization-defined high-risk entry/exit points are changed when lost or stolen or combinations are compromised.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
18110.08j1Organizational.5	08.j Equipment Maintenance	18 Physical & Environmental Security	1	The organization monitors and controls nonlocal maintenance and diagnostic activities; and prohibits nonlocal system maintenance unless explicitly authorized, in writing, by the CIO or his/her designated representative.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
18111.08j1Organizational.6	08.j Equipment Maintenance	18 Physical & Environmental Security	1	The organization obtains maintenance support and/or spare parts for defined key information system components (defined in the applicable security plan) within the applicable Recovery Time Objective (RTO) specified in the contingency plan.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1812.08b3Organizational.46	08.b Physical Entry Controls	18 Physical & Environmental Security	3	Intrusion detection systems (e.g., alarms and surveillance equipment) are installed on all external doors and accessible windows, the systems are monitored, and incidents/alarms are investigated.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
18127.08l1Organizational.3	08.l Secure Disposal or Re-Use of Equipment	18 Physical & Environmental Security	1	Surplus equipment is stored securely while not in use, and disposed of or sanitized when no longer required.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1813.08b3Organizational.56	08.b Physical Entry Controls	18 Physical & Environmental Security	3	The organization actively monitors unoccupied areas at all times and sensitive and/or restricted areas in real time as appropriate for the area.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
18130.09p1Organizational.24	09.p Disposal of Media	18 Physical & Environmental Security	1	The organization ensures the risk of information leakage to unauthorized persons during secure media disposal is minimized. If collection and disposal services offered by other organizations are used, care is taken in selecting a suitable contractor with adequate controls and experience.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
18131.09p1Organizational.3	09.p Disposal of Media	18 Physical & Environmental Security	1	Disposal methods are commensurate with the sensitivity of the information contained on the media.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1814.08d1Organizational.12	08.d Protecting Against External and Environmental Threats	18 Physical & Environmental Security	1	Fire extinguishers and detectors are installed according to applicable laws and regulations.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
18145.08b3Organizational.7	08.b Physical Entry Controls	18 Physical & Environmental Security	3	The organization regularly tests alarms to ensure proper operation.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
18146.08b3Organizational.8	08.b Physical Entry Controls	18 Physical & Environmental Security	3	The organization maintains an electronic log of alarm system events and regularly reviews the logs, no less than monthly.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1815.08d2Organizational.123	08.d Protecting Against External and Environmental Threats	18 Physical & Environmental Security	2	Fire prevention and suppression mechanisms, including workforce training, are provided.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1816.08d2Organizational.4	08.d Protecting Against External and Environmental Threats	18 Physical & Environmental Security	2	Any security threats presented by neighboring premises are identified.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1819.08j1Organizational.23	08.j Equipment Maintenance	18 Physical & Environmental Security	1	Maintenance and service are controlled and conducted by authorized personnel in accordance with supplier-recommended intervals, insurance policies and the organizations maintenance program, taking into account whether this maintenance is performed by personnel on site or external to the organization.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1820.08j2Organizational.1	08.j Equipment Maintenance	18 Physical & Environmental Security	2	Covered information is cleared from equipment prior to maintenance unless explicitly authorized.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1821.08j2Organizational.3	08.j Equipment Maintenance	18 Physical & Environmental Security	2	Following maintenance, security controls are checked and verified.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1822.08j2Organizational.2	08.j Equipment Maintenance	18 Physical & Environmental Security	2	Records of maintenance are maintained.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1825.08l1Organizational.12456	08.l Secure Disposal or Re-Use of Equipment	18 Physical & Environmental Security	1	Electronic and physical media containing covered information is securely sanitized prior to reuse, or if it cannot be sanitized, is destroyed prior to disposal.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1826.09p1Organizational.1	09.p Disposal of Media	18 Physical & Environmental Security	1	The organization securely disposes of media containing sensitive information.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1827.09p2Organizational.1	09.p Disposal of Media	18 Physical & Environmental Security	2	The organization takes measures to minimize the aggregation effect, which may cause a large quantity of non-covered information to become covered through accumulation of media for disposal.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1844.08b1Organizational.6	08.b Physical Entry Controls	18 Physical & Environmental Security	1	The organization develops, approves and maintains a list of individuals with authorized access to the facility where the information system resides; issues authorization credentials for facility access; reviews the access list and authorization credentials periodically but no less than quarterly; and removes individuals from the facility access list when access is no longer required.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1845.08b1Organizational.7	08.b Physical Entry Controls	18 Physical & Environmental Security	1	For facilities where the information system resides, the organization enforces physical access authorizations at defined entry/exit points to the facility where the information system resides, maintains physical access audit logs, and provides security safeguards that the organization determines necessary for areas officially designated as publicly accessible.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1846.08b2Organizational.8	08.b Physical Entry Controls	18 Physical & Environmental Security	2	Visitors are only granted access for specific and authorized purposes and issued with instructions on the security requirements of the area and on emergency procedures.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1847.08b2Organizational.910	08.b Physical Entry Controls	18 Physical & Environmental Security	2	The organization ensures onsite personnel and visitor identification (e.g., badges) are revoked, updated when access requirements change, or terminated when expired or when access is no longer authorized, and all physical access mechanisms, such as keys, access cards and combinations, are returned, disabled or changed.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1848.08b2Organizational.11	08.b Physical Entry Controls	18 Physical & Environmental Security	2	A restricted area, security room, or locked room is used to control access to areas containing covered information, and is controlled accordingly.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1862.08d1Organizational.3	08.d Protecting Against External and Environmental Threats	18 Physical & Environmental Security	1	Fire authorities are automatically notified when a fire alarm is activated.	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1863.08d1Organizational.4	08.d Protecting Against External and Environmental Threats	18 Physical & Environmental Security	1	The organization formally addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance requirements for its physical and environmental protection program (e. g., through policy, standards, guidelines, and procedures).	Yes	*Provided by AWS*	*N/A*	*N/A*	*N/A*
1903.06d1Organizational. 3456711	06.d Data Protection and Privacy of Covered Information	19 Data Protection & Privacy	1	The confidentiality and integrity of covered information at rest is protected using an encryption method appropriate to the medium where it is stored; where the organization chooses not to encrypt covered information, a documented rationale for not doing so is maintained or alternative compensating controls are used if the method is approved and reviewed annually by the CISO.	No	*Partial*	*Infrastructure Orchestration (Encryption-at-rest on secondary EBS volumes, RDS, S3, DynamoDB)*	*No*	
19145.06c2Organizational.2	06.c Protection of Organizational Records	19 Data Protection & Privacy	2	Specific controls for record storage, access, retention, and destruction have been implemented.	Yes	*Partial*	*Oxygen EC2 Backups, Infrastructure Orchestration (S3 Lifecycle Policies, Config Rules)*	*No*	*If using Cloudticity provided backups, a custom retention policy based on customer provided information is configured. This policy allows for only the number of backups necessary according to the customers policy.*

19242.06d1Organizational.14	06.d Data Protection and Privacy of Covered Information	19 Data Protection & Privacy	1	Covered information storage is kept to a minimum.	No	*Partial*	*Oxygen EC2 Backups*	*No*	*If using Cloudticity provided backups, a custom retention policy based on customer provided information is configured. This policy allows for only the number of instance backups necessary according to the customers policy.*
19243.06d1Organizational.15	06.d Data Protection and Privacy of Covered Information	19 Data Protection & Privacy	1	The organization specifies where covered information can be stored.	No	*Partial*	*Infrastructure Orchestration (Tagging, encrypted S3 Buckets, encrypted secondary EBS Volumes, encrypted RDS DB)*	*No*	*Cloudticity facilitates encryption-at-rest for all volumes, databases, or locations where sensitive information is stored or processed.*
19245.06d2Organizational.2	06.d Data Protection and Privacy of Covered Information	19 Data Protection & Privacy	2	The organization has implemented technical means to ensure covered information is stored in organization-specified locations.	No	*Partial*	*Infrastructure Orchestration (Tagging, encrypted S3 Buckets, encrypted secondary EBS Volumes, encrypted RDS DB)*	*No*	*Cloudticity facilitates encryption-at-rest for all volumes, databases, or locations where sensitive information is stored or processed.*