	id	question
0	53148c6413ac11f0a90176c5cf2df9da	Where are your data centres located?
1	5314a7da13ac11f0a90176c5cf2df9da	Do you monitor and restrict the installation of unauthorized software?
2	5314c76a13ac11f0a90176c5cf2df9da	Is business continuity and operational resilience documentation available to authorized stakeholders?
3	5314e9de13ac11f0a90176c5cf2df9da	Are private keys provisioned for a unique purpose managed, and is cryptography secret?
4	5315006813ac11f0a90176c5cf2df9da	Are data center environmental control systems designed to monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards effectively implemented and maintained?
5	53151efe13ac11f0a90176c5cf2df9da	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?
6	53158f9c13ac11f0a90176c5cf2df9da	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?
7	5315dba013ac11f0a90176c5cf2df9da	Are asset management and malware protection policies and procedures reviewed and updated at least annually?

8	5315f40a13ac11f0a90176c5cf2df9da	Do transport containers protect against physical damage?
9	53163f0a13ac11f0a90176c5cf2df9da	Do administrative and file sharing interfaces for web server software run on non-standard ports (e.g., Not 21, 80 and 443)?
10	5316577e13ac11f0a90176c5cf2df9da	Does the Incident Response Plan include event reporting mechanism to support the reporting action, and to list all necessary actions in case of an information security Event?
11	5316781c13ac11f0a90176c5cf2df9da	Is there a dedicated sanctions compliance officer?
12	531692ac13ac11f0a90176c5cf2df9da	Is there a Quality Assurance or other organization that ensures software integrity and adherence to internal processes for software development for FDA-regulated systems?
13	5316e9dc13ac11f0a90176c5cf2df9da	Does the Wireless Security Policy prohibit wired and wireless network connections at the same time?
14	531716dc13ac11f0a90176c5cf2df9da	Does the Wireless Security Policy require continuous monitoring and alerting to security personnel, or quarterly scanning for rogue wireless access points?
15	53176ce013ac11f0a90176c5cf2df9da	Does the approved anti-malware policy or program mandate an interval between the availability of a new anti-malware signature update and its deployment no longer than 24 hours?
16	5317805413ac11f0a90176c5cf2df9da	Does the Hypervisor system lock accounts after 3-5 invalid login attempts?
17	5317966613ac11f0a90176c5cf2df9da	Do asset inventory and management processes include all physical objects with network connectivity (IoT Devices)?

18	53180a7e13ac11f0a90176c5cf2df9da	Does your organisation have an Identity and Access Management System in place used for the formal request, approval, and provisioning of access to a role?

answer
Our data centers are located in the US Central region, specifically hosted within Google Cloud Platform (GCP). All customer data is physically stored in the USA.
Yes, we monitor and restrict the installation of unauthorized software through various controls, including application whitelisting and blacklisting. We ensure that only approved applications can be installed on our systems, and we require security approval prior to implementing any freeware or shareware applications. Additionally, we log and monitor access to our information security management systems to prevent unauthorized installations.
Yes
Yes, private keys are provisioned for unique purposes and are managed securely. We ensure that cryptography is treated as a secret, adhering to industry standards for key management and encryption practices.
Yes, our data center environmental control systems are designed to effectively monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards. We have implemented robust HVAC systems and humidity controls to ensure optimal conditions.
Yes
Yes
Yes

Data-Not-Found

Yes

Yes, the Incident Response Plan includes an event reporting mechanism to support the reporting action and lists all necessary actions in case of an information security event.

No

N/A

N/A

N/A

N/A

No, the Hypervisor system does not lock accounts after 3-5 invalid login attempts. Instead, we prioritize multi-factor authentication (MFA) as a more effective control. However, some of our services may have account lockout features built in by default.

No, our asset inventory and management processes do not include IoT devices as we do not use them.

Yes, we have an Identity and Access Management System in place that facilitates the formal request, approval, and provisioning of access to roles. This system ensures that user access is managed effectively, including timely de-provisioning and modification of access as needed.

comments	confidence
We leverage GCP for our data hosting, ensuring that all data is managed within their secure data centers. You can find more details about GCP's data security at https://www.google.com/about/datacenters/data-security/.	high
You can find more details in our "Company_kb (1).json" document, which outlines our software installation policies and controls.	high
Business continuity and operational resilience documentation is available to authorized stakeholders. We ensure that this documentation is regularly reviewed and updated to maintain its relevance and effectiveness.	high
We leverage Google Cloud Platform for cryptographic key management, ensuring that all keys are generated using approved cryptographic libraries and are managed according to established policies and procedures. Our key management system tracks and reports all cryptographic materials and status changes, and we have a risk program in place to assess and treat risks associated with cryptography.	high
You can find more details about our environmental controls and security measures in our documentation at https://cloud.google.com/security. Additionally, we have processes in place for regular testing and maintenance of these systems to ensure their continual effectiveness.	high
We implement cryptographically secure and standardized network protocols for the management, import, and export of data. All data in transit is protected using TLS 1.2 or TLS 1.3, ensuring secure communication channels. Additionally, we utilize approved cryptographic libraries for data protection at rest and in transit.	high
We have established, documented, approved, communicated, applied, evaluated, and maintained comprehensive infrastructure and virtualization security policies and procedures. These policies ensure that our security measures are effective and aligned with best practices.	high
Our asset management and malware protection policies and procedures are reviewed and updated at least annually to ensure they remain effective and aligned with current security practices.	high

We do not have specific documentation regarding the physical protection capabilities of transport containers against physical damage. Our operations are fully hosted in the cloud, and we do not transport physical media.	low
We ensure that administrative and file sharing interfaces for our web server software operate on non-standard ports to enhance security. This practice helps mitigate the risk of unauthorized access and potential attacks on commonly used ports like 21, 80, and 443.	high
Our Incident Response Plan outlines specific procedures for reporting incidents, including the actions to be taken during an event. This ensures that all relevant stakeholders are informed and that appropriate measures are implemented.	high
We do not have a dedicated sanctions compliance officer; however, we have a compliance program in place that restricts activities with sanctioned countries. Our internal audit and compliance department oversees regulatory and compliance issues.	medium
FDA compliance does not apply to us, and therefore we do not have a Quality Assurance organization specifically for FDA-regulated systems.	high
We do not have an office wireless network, so the question of prohibiting wired and wireless connections simultaneously does not apply to our current setup.	high
We do not have an office wireless network, so the Wireless Security Policy does not require continuous monitoring or quarterly scanning for rogue wireless access points.	high
We operate as a 100% Mac environment, and our anti-malware strategy may differ from traditional Windows-based systems. Therefore, the specific interval for deploying new anti-malware signature updates may not apply in the same way.	medium
We believe that MFA provides a stronger layer of security compared to account locking, which can sometimes lead to user frustration and support overhead.	high
We maintain a comprehensive asset inventory for all physical and logical assets, but IoT devices are not part of our infrastructure. You can find more details in "Company_kb (1).json".	high

Our IAM policies and procedures are established, documented, and regularly reviewed to ensure compliance and effectiveness. We also implement multifactor authentication and conduct periodic reviews of access rights to maintain security.	high