European Medicines Agency (EMA) - Eudralex Annex 11

Google Cloud Mapping

This document is designed to help regulated customers supervised by the European Medicines Agency (EMA) (“**regulated entity**”) to consider Eudralex Annex 11 (“**framework**”) in the context of Google Cloud.

We focus on the requirements of the framework for computerised systems. For each paragraph, we provide commentary to help you understand how you can address the requirements using the Google Cloud services and the Google Cloud Compliance Reports and Certificates.

NOTE:
**Google Responsibilities vs Customer Responsibilities - Google Cloud is responsible for controls for the Google Cloud and customers retain ownership and control of the systems/workloads they set-up on Google Cloud, in alignment with the Google Cloud Shared Responsibility model in the Google Cloud Security Foundations whitepaper.

#	Framework reference	**Google	**Customer	Google Cloud commentary	Google Cloud Compliance Reports / Certificates reference
1	**Risk Management** Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.	☑	☑	Google has documented its risk management procedures as part of its ISMS that underlies our ISO/IEC 27001 certification. Documentation is made available to all individuals that may participate in or need to be informed of risk management and assessment programs. Customers retain control and ownership over risk management processes for their regulated systems.	CSA CCM v4: GRC-02 SOC 2 Type II: CC3.1, CC3.3 ISO 27001: 5.2(c), 5.3(a), 5.3(b), 7.5.3(b), 7.5.3(d), 8.2, 9.2(g), A.8.2.24.2(b), 6.1.1, 6.1.1(e)(2), 6.1.2, 6.1.2(a)(1), 6.1.2(a)(2), 6.1.2(b), 6.1.2 (c), 6.1.2(c)(1), 6.1.2(c)(2), 6.1.2(d), 6.1.2(d)(1), 6.1.2(d)(2), 6.1.2(d)(3), 6.1.2(e), 6.1.2(e)(1), 6.1.2(e)(2), 6.1.3, 6.1.3(a), 6.1.3(b), 8.1, 8.3, 9.3(a), 9.3(b), 9.3(b)(f), 9.3(c), 9.3(c)(1), 9.3(c)(2), 9.3(c)(3), 9.3(d), 9.3(e), 9.3(f), A.12.6.1, A.17.1.1, A.18.2.2, A.18.2.3, A.18.1.1 ISO 27017: 8.2.2, 18.1.1, 18.1.3, 12.6.1, 15.1.1, 15.1.3 ISO 27018: None NIST SP800-53 R3: PL-5, RA-2, RA-3, AC-4, CA-2, CA-3, CA-6, MP-8, PM-9, RA-1, SI-12 BSI C5:2020: RB-03, RB-06, AM-05, IDM-01, OIS-06, OIS-07
2	**Personnel** There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.	☑	☑	All Google employees undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new employees agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.	CSA CCM v4: HRS-10, HRS-11, HRS-12 SOC 2 Type II: CC2.2, CC2.3, CC5.5, CC5.6 ISO 27001: 7.2(a), 7.2(b), A.7.2.2, A.11.1.5, A.9.3.1, A.11.2.8, A.11.2.9 ISO 27017: 7.2.2

European Medicines Agency (EMA) - Eudralex Annex 11

Google Cloud Mapping

#	Framework reference	**Google	**Customer	Google Cloud commentary	Google Cloud Compliance Reports / Certificates reference
				Google maintains a robust and up-to-date Information Security Management System that is audited at least yearly and signed off by business leadership. As part of the ISO/IEC 27001 certified ISMS, roles and responsibilities are documented and authorized by leadership. Customers retain control and ownership over training of their personnel including maintaining appropriate sign-offs and records.	ISO 27018: None NIST SP800-53 R3: AT-1, AT-2, AT-3, AT-4, AC-11, MP-2, MP-3, MP-4 BSI C5:2020: HR-03
3	**Suppliers and Service Providers** 3.1 When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous. 3.2 The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment. 3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled. 3.4 Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request. Project Phase	☑	☐	Google has a robust compliance program, designed to meet emerging requirements from our customers and regulators. We work with regulators, government bodies, and third-party auditors globally to comply with regional, country or industry specific requirements. Google undergoes a number of independent third party audits and internal audits on a regular basis to verify and provide assurance of our quality, security, privacy and compliance controls. Our certifications include many internationally accepted independent quality, security and privacy standards including ISO/IEC9001, CSA STAR, HITRUST CSF, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 1/2/3 and NIST 800-53. Google Cloud also supports compliance with industry and country specific regulations (such as PCI DSS) and we continue to expand our list of certifications to assist our customers with their compliance obligations, including the “right to audit” Google Cloud. For more information on our compliance, visit the Compliance Resource Center and Compliance Reports Manager to download reports and certifications. Google maintains a public website that details all current compliance, regulatory, and privacy standards Google either complies or aligns with. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Google Cloud, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide.Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms. Google agrees contractually with third party providers on adherence to Google's security and privacy policies and has a vendor audit program to verify compliance. Google has a dedicated team which performs an annual information security	CSA CCM v4: A&A-02, A&A-04 SOC 2 Type II: CC3.2, CC1.2, CC2.3, CC4.1 ISO 27001: 4.3, 5, 4.4, 4.2(b), 6.1.2(a)(1), 6.2, 6.2(a), 6.2(d), 7.1, 7.4, 9.3, 10.2, 7.2(a), 7.2(b), 7.2(c), 7.2(d), 7.3(b), 7.3(c), A5.1.1, A.7.2.2, 18.2.1, 4.3(a), 4.3(b), 5.1(e), 5.1(f), 9.1, 9.2, 9.3(f) ISO 27017: 5.1.1, 7.2.2, 15.1.1, 15.1.3, 18.1.2 ISO 27018: None NIST SP800-53 R3: AC-1, AT-1, AU-1, CA-1, CM-1, IA-1, IR-1, MA-1, MP-1, MP-1, PE-1, PL-1, PS-1, SA-1, SC-1, SI-1, CA-2, CA-6 , RA-5 BSI C5:2020: SA-01, COM-03

European Medicines Agency (EMA) - Eudralex Annex 11

Google Cloud Mapping

#	Framework reference	**Google	**Customer	Google Cloud commentary	Google Cloud Compliance Reports / Certificates reference
				assessment on Cloud Subprocessors that support the delivery of Cloud products and services. The audit includes an evaluation of the controls in place at the subprocessor site to safeguard the confidentiality, availability, and integrity of Google's customer data. Google undergoes a number of independent third party audits and internal audits on a regular basis to verify and provide assurance of these security, privacy and compliance controls. Refer to the Cloud Data Processing Addendum in section 11 Subprocessors. Customers retain control and ownership over their QMS, including procedures for quality audits and conduct such audits to assure that the quality system is in compliance with the established quality system requirements and to determine the effectiveness of the quality system. Quality audits shall be conducted by individuals who do not have direct responsibility for the matters being audited. Corrective action(s), including a re-audit of deficient matters, shall be taken when necessary. A report of the results of each quality audit, and reaudit(s) where taken, shall be made and such reports shall be reviewed by management having responsibility for the matters audited. The dates and results of quality audits and re-audits shall be documented.	
4	**Validation** 4.1 The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment. 4.2 Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process. 4.3 An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software prerequisites, and security measures should be available. 4.4 User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle. 4.5 The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance	☐	☑	Customers retain control and ownership over all systems validation documentation and testing of their applications, systems and workloads.	N/A

European Medicines Agency (EMA) - Eudralex Annex 11

Google Cloud Mapping

#	Framework reference	**Google	**Customer	Google Cloud commentary	Google Cloud Compliance Reports / Certificates reference
	with an appropriate quality management system. The supplier should be assessed appropriately. 4.6 For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system. 4.7 Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy. 4.8 If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process. Operational Phase				
5	**Data** Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.	☑	☑	All Google Cloud user interfaces are designed with secure coding practices to prevent web attacks such as cross site scripting or other popular input based attacks. If a user attempts to input data that does not meet system parameters, the system will reject the input. Users will not be able to execute commands without correcting that input. Users can input information in the Google Cloud Console, however the user interface is designed to only allow responses that meet specific parameters that can be processed by Google Cloud. If a user inputs invalid data that isn't within the parameters the system automatically rejects the data. Customers retain control and ownership over ensuring that checks to determine, as appropriate, the validity of the source of data input or operational instruction are in place for the devices, systems and applications that they build and host on Google Cloud.	CSA CCM v4: AIS-03 SOC 2 Type II: PI1.2, PI1.3, PI1.5 ISO 27001: A.10.9.2, A.10.9.3, A.12.2.1, A.12.2.2, A.12.2.3, A.12.2.4, A.12.6.1, A.15.2.1 ISO 27017: None ISO 27018: None NIST SP800-53 R3: SI-10, SI-11, SI-2, SI-3, SI-4, SI-6, SI-7, SI-9 BSI C5:2020: None
6	**Accuracy Checks** For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.	☑	☑	All Google Cloud user interfaces are designed with secure coding practices to prevent web attacks such as cross site scripting or other popular input based attacks. If a user attempts to input data that does not meet system parameters, the system will reject the input. Users will not be able to execute commands without correcting that input. Users can input information in the Google Cloud Console, however the user interface is designed to only allow responses that meet specific parameters that can be processed by Google Cloud. If a user inputs invalid data that isn't within the parameters the system automatically rejects the data.	CSA CCM v4: AIS-03 SOC 2 Type II: PI1.2, PI1.3, PI1.5 ISO 27001: A.10.9.2, A.10.9.3, A.12.2.1, A.12.2.2, A.12.2.3, A.12.2.4, A.12.6.1, A.15.2.1 ISO 27017: None ISO 27018: None

European Medicines Agency (EMA) - Eudralex Annex 11

Google Cloud Mapping

#	Framework reference	**Google	**Customer	Google Cloud commentary	Google Cloud Compliance Reports / Certificates reference
				Customers retain control and ownership over ensuring that checks to determine, as appropriate, the validity of the source of data input or operational instruction are in place for the devices, systems and applications that they build and host on Google Cloud.	NIST SP800-53 R3: SI-10, SI-11, SI-2, SI-3, SI-4, SI-6, SI-7, SI-9 BSI C5:2020: None
7	**Data Storage** 7.1 Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. 7.2 Regular back-ups of all relevant data should be done. Integrity and accuracy of back-up data and the ability to restore the data should be checked during validation and monitored periodically.	☑	☑	Policies and procedures are established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness. Refer to the Cloud Data Processing Addendum in Appendix 2: Security Measures which include data backup and redundancy measures. Customers retain control and ownership over their content. Customers are responsible for managing their data retention policies. Customers may leverage the features of our storage services. Please see product documentation for examples of such services: • Google Cloud online storage products • Retention policies and retention policy locks	CSA CCM v4: DSP-18, LOG-09 SOC 2 Type II: A1.2, A1.3, I3.21 ISO 27001: 9.2(g), 7.5.3(b), 5.2 (c), 7.5.3(d), 5.3(a), 5.3(b), 8.1, 8.3, A.12.3.1, A.8.2.3 ISO 27017: 12.3.1, 15.1.1, 15.1.3 ISO 27018: None NIST SP800-53 R3: CP-2, CP-6, CP-7, CP-8, CP-9, SI-12, AU-11 BSI C5:2020: RB-06, RB-08
8	**Printouts** 8.1 It should be possible to obtain clear printed copies of electronically stored data. 8.2 For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.	☐	☑	Customers do not need Google's assistance to port their data. Google will enable you to access and export your data throughout the duration of our contract. You can export your data from the Services in a number of industry standard formats (e.g. .doc, .xls, .pdf, logs, and flat files). Google offers solutions to support customers in data export and migration such as: • Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. • Migrate to Containers allows you to move and convert workloads directly into containers in Google Kubernetes Engine. • You can export/import an entire VM image in the form of a .tar archive. Find more information on images and on storage options. Google provides documentation regarding how customers may port data. Our GDPR resource site provides an entry point for information regarding portability and interoperability of data. Further, Google Cloud storage and database solutions offer fine-grained IAM permissions to control which employees can export data. In addition, Google Cloud	CSA CCM v4: IPY-01, IPY-02, IPY-04, IPY-05 SOC 2 Type II: None ISO 27001: 6.1.1, 6.1.1(e)(2), 6.1.2, 6.1.2(a)(1), 6.1.2(a)(2), 6.1.2(b), 6.1.2 (c), 6.1.2(c)(1), 6.1.2(c)(2), 6.1.2(d), 6.1.2(d)(1), 6.1.2(d)(2), 6.1.2(d)(3), 6.1.2(e), 6.1.2(e)(1), 6.1.2(e)(2), 6.1.3, 6.1.3(a), 6.1.3(b), 8.1, 8.3, 9.3(a), 9.3(b), 9.3(b)(f), 9.3(c), 9.3(c)(1), 9.3(c)(2), 9.3(c)(3), 9.3(d), 9.3(e), 9.3(f), A.14.2.3, A.12.6.1, A.18.1.1, A.18.2.2, A.18.2.3 ISO 27017: 12.6.1, 18.1.1 ISO 27018: None NIST SP800-53 R3: SC-8, SC-8(1)

European Medicines Agency (EMA) - Eudralex Annex 11

Google Cloud Mapping

#	Framework reference	**Google	**Customer	Google Cloud commentary	Google Cloud Compliance Reports / Certificates reference
				implements limitations, such as preventing the export of BigQuery tables to raw files or Google Sheets, the inability to export more than 1GB of table data, the inability to export data from multiple tables all at once, and others.	BSI C5:2020: IPI-02, IPI-04, IPI-05
9	**Audit Trails** Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated ""audit trail""). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.	☑	☑	Google maintains an automated log collection and analysis tool to review and analyse log events. Google restricts physical and logical access to audit logs. Google Cloud retains Google-generated customer data access audit logs for no longer than 30 days. It is the customer's responsibility to offload these audit log records from the Google Cloud Console and manage the retention of logs. Customers that have longer audit log retention requirements can export logs to Cloud Storage, BigQuery, or Cloud Pub Sub to stream log entries to other applications or repositories. Customers are also responsible for the retention of audit records for customer applications within Google Cloud. Admin Activity audit logs are retained by Google for 400 days. Admin Activity logs contain log entries for API calls or other administrative actions that modify the configuration or metadata of resources. For example, the logs record when VM instances and App Engine applications are created and when permissions are changed. Customers retain control and ownership over identity & access management to their systems hosted on Google Cloud including audit trails and logging management.	CSA CCM v4: LOG-01, LOG-02, LOG-03, LOG-04, LOG-05, LOG-06, LOG-07, LOG-08, LOG-09, LOG-10, LOG-11, LOG-12, LOG-13, LOG-14 SOC 2 Type II: CC6.2 ISO 27001: A.12.4.1, A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.3, A.12.4.1, A.9.2.3, A.9.4.4, A.9.4.1, A.16.1.2, A.16.1.7, A.18.2.3, A.18.1.3 ISO 27017: 12.4.1, 12.4.1, 12.4.3, 12.4.3, 12.4.1, 9.2.3, 9.4.4, 9.4.1, 15.1.1, 15.1.3, 16.1.2, 16.1.7, 18.1.3, CLD.9.5.1 , CLD12.4.5 ISO 27018: 9.2.3, 9.4.1, 9.4.4, 12.4.1 , 12.4.2, 12.4.3 , 16.1.2 , 16.1.7 , 18.2.3, 18.1.3 NIST SP800-53 R3: AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4 BSI C5:2020: RB-10, RB-13, RB-14
10	**Change and Configuration Management** Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure	☑	☑	**Change Management:** Google has a robust change management process and security policy that is documented and requires approvals from relevant stakeholders before being released into production. Google maintains policy and procedures to ensure consideration of security, quality and availability throughout the SDLC (Software Development Lifecycle). Every Google Cloud product maintains a well documented release and deployment process. This process is validated for each product during the semi-annual compliance audit cycle. **Configuration Management (Infrastructure Qualification)** Google's infrastructure is designed and purpose built for Google. Baseline configuration settings are defined for infrastructure components and Google maintains configuration management tools to detect and correct deviations from its security baselines and collects and secures audit records. Our configuration management controls are audited as part of our third party audit certifications and attestation reports.	CSA CCM v4: CCC-01, CCC-02, CCC-03, CCC-04, CCC-05, CCC-06, CCC-07, CCC-08, CCC-09, LOG-01, LOG-02, LOG-03, LOG-04, LOG-05, LOG-07, LOG-08, LOG-09, LOG-10, LOG-14 SOC 2 Type II: CC7.4, CC6.2 ISO 27001: A.12.1.4, 8.1* (partial) A.14.2.2, 8.1* (partial) A.14.2.3, A.12.1.2, A.12.4, A.12.4.1, A.12.4.2, A.12.4.3, A.12.6.1, A.12.6.2, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7, A.9.2.3, A.9.4.4, A.9.4.1, A.18.2.3, A.18.1.3 ISO 27017: CLD12.1.5, 14.1.1, 14.2.1, 15.1.1, 15.1.3, 12.1.2, 12.4, 12.4.1, 12.4.3, 12.6.1, 15.1.1,

European Medicines Agency (EMA) - Eudralex Annex 11

Google Cloud Mapping

#	Framework reference	**Google	**Customer	Google Cloud commentary	Google Cloud Compliance Reports / Certificates reference
				Logging: Google maintains an automated log collection and analysis tool to review and analyse log events.	15.1.3, 16.1.1, 16.1.2, 16.1.7, 9.2.3, 9.4.4, 9.4.1,18.1.3, CLD.9.5.1, CLD12.4.5 ISO 27018: 9.2.3, 9.4.1, 9.4.4, 12.4.1 , 12.4.2, 12.4.3 , 16.1.2 , 16.1.7 , 18.2.3, 18.1.3 NIST SP800-53 R3: CA-1, CA-6, CA-7, CM-2, CM-3, CM-5, CM-6, CM-9, PL-2, PL-5, SI-2, SI-6, SI-7, AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4 BSI C5:2020: BEI01, BEI02, BEI03, BEI04, BEI05, BEI06, BEI07
11	**Periodic evaluation** Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.	☑	☑	Google has a robust compliance program, designed to meet emerging requirements from our customers and regulators. We work with regulators, government bodies, and third-party auditors globally to comply with regional, country or industry specific requirements. Google undergoes a number of independent third party audits and internal audits on a regular basis to verify and provide assurance of our quality, security, privacy and compliance controls. Our certifications include many internationally accepted independent quality, security and privacy standards including ISO/IEC9001, CSA STAR, HITRUST CSF, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 1/2/3 and NIST 800-53. Google Cloud also supports compliance with industry and country specific regulations (such as PCI DSS) and we continue to expand our list of certifications to assist our customers with their compliance obligations, including the “right to audit” Google Cloud. Customers retain control and ownership over all systems validation documentation and testing of their applications and workloads.	For more information on our compliance, visit the Compliance Resource Center and Compliance Reports Manager to download reports and certifications. Google maintains a public website that details all current compliance, regulatory, and privacy standards Google either complies or aligns with.
12	**Security** 12.1 Physical and/or logical controls should be in place to restrict access to computerised systems to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal	☑	☑	Customers retain control and ownership over identity & access management to their systems hosted on Google Cloud. Customers can customize access to data by organization and user and assign administrative access profiles based on roles. Google provides customers with solutions which helps to prevent unauthorized access by controlling access rights and roles for Google Cloud resources and to implement more granular control over access. For example: • Cloud Identity and Access Management	CSA CCM v4: IAM-01, IAM-02, IAM-03, IAM-04, IAM-05, IAM-06, IAM-07 SOC 2 Type II: CC5.1, CC7.4, CC3.1, CC3.3, CC5.3 ISO 27001: A.9.1.1, A.9.2.1, A.9.2.2, A.9.2.5, A.9.1.2, A.9.4.1, A.13.1.1, A.9.4.4,, A.9.2, A.9.2.3,

European Medicines Agency (EMA) - Eudralex Annex 11

Google Cloud Mapping

#	Framework reference	**Google	**Customer	Google Cloud commentary	Google Cloud Compliance Reports / Certificates reference
	codes with passwords, biometrics, restricted access to computer equipment and data storage areas. 12.2 The extent of security controls depends on the criticality of the computerised system. 12.3 Creation, change, and cancellation of access authorisations should be recorded. 12.4 Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.			• Identity-Aware Proxy - identity and context to guard access to your applications and VMs. • BeyondCorp - a zero trust solution that enables secure access with integrated threat and data protection. • Access Transparency - enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). • Cloud Logging - fully managed service that performs at scale and can ingest application and system log data, as well as custom log data from GKE environments, VMs, and Google Cloud services. Cloud Logging allows you to analyze selected logs and accelerate application troubleshooting. • Cloud Monitoring - provides visibility into the performance, uptime, and overall health of cloud-powered applications. Google's internal data access policies and processes are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process your data. Access rights and levels are based on their job function and role. Google restricts access based on need-to-know and job function in accordance with applicable legal and compliance requirements. Google provides (under NDA) customers with a SOC 2 report that includes testing of Google's access controls. For more information, refer to Trusting your data with Google Cloud whitepaper. In the Cloud Data Processing Addendum, Google makes commitments to protect your data, including regarding access control and privilege management.	A.9.2.4, A.6.1.2, 5.2(c), 5.3(a), 5.3(b), 7.5.3(b), 7.5.3(d), 8.1, 8.3, 9.2(g), A.9.4.5, A.18.1.3, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 ISO 27017: 9.2.1, 9.2.2, 9.1.2, 9.4.1, 9.4.4, 9.2, 9.2.3, 9.2.4, 18.1.3, CLD12.4.5 ISO 27018: 9.2, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.4.5, 18.1.3, 9.1.1, 9.3.1, 9.4.1, 9.4.2, 9.4.3, 9.4.4 NIST SP800-53 R3: AC-1, IA-1, AU-9, AU-11, AU-14, CM-7, MA-3, MA-4, MA-5, AC-2, AC-5, AC-6, AU-1, AU-6, SI-1, SI-4, CM-5, CM-6, CA-3, RA-3, AC-3, IA-2, IA-4, IA-5, IA-8, PS-6, SA-7, SI-9, PM-10, PS-6, PS-7, PS-4, PS-5, , AC-11, AU-2, IA-6, SC-10, SC-3, SC-19 BSI C5:2020: RB-13, IDM-01, IDM-06, IDM-07, IDM-08, IDM-03, IDM-02, IDM-13, DLL-01, SPN-03, IDM-05, IDM-04, IDM-12
13	**Incident Management** All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.	☑	☑	Google has a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Google's security incident management program is structured around the NIST guidance on handling incidents (NIST SP 800–61). Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into	CSA CCM v4: SEF-02, SEF-03, SEF-04, SEF-05, SEF-07, SEF-08 SOC 2 Type II: CC5.5, CC6.2 ISO 27001: 5.3 (a), 5.3 (b), 7.5.3(b), 5.2 (c), 7.5.3(d), 8.1, 8.3, 9.2(g), Annex, A.16.1.1, A.16.1.2 ISO 27017: 16.1.1, 16.1.2, 6.1.1, 7.2.2, CLD.6.3.1, CLD12.4.5 ISO 27018: 16.1.1 , 16.1.2, 16.1.2.3,

European Medicines Agency (EMA) - Eudralex Annex 11

Google Cloud Mapping

#	Framework reference	**Google	**Customer	Google Cloud commentary	Google Cloud Compliance Reports / Certificates reference
				consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. We outline Google's end-to-end data incident response process in our whitepaper. Customers retain control and ownership over the establishment and maintenance of procedures for implementing corrective and preventive action.	NIST SP800-53 R3: IR-1, IR-2, IR-3, IR-4, IR-5, IR-7, IR-8, SI-4, SI-5 BSI C5:2020: SIM-05, SIM-06, SIM-07
14	**Electronic Signature** Electronic records may be signed electronically. Electronic signatures are expected to: a. have the same impact as hand-written signatures within the boundaries of the company, b. be permanently linked to their respective record, c. include the time and date that they were applied.	☐	☑	Customers retain control and ownership over the establishment of, and adherence to digital/electronic signature management	N/A
15	**Batch release** When a computerised system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.	☐	☑	Customers retain control and ownership over the establishment of, and adherence to digital/electronic signature management	N/A
16	**Business Continuity** For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.	☑	☑	Google has a defined Business Continuity Plan (BCP) which is updated annually. Google performs annual testing of its business continuity plans to simulate disaster scenarios that model catastrophic events that may disrupt Google operations. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and Internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependent on a single server, data center, or network connection.	CSA CCM v4: BCR-01, BCR-02, BCR-03, BCR-04, BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11, BCR-12, BCR-13, BCR-14 SOC 2 Type II: CC1.3, CC1.4, CC2.1, CC4.1, A1.1, CC3.1, A1.2, A1.3, CC3.2 ISO 27001: A3.1.0, A3.3.0, A17.3.1, 9.2(g), A11.2.1, A.11.2.2, A.11.2.3, A.11.2.4, A.17.1.1, A.17.1.2, 5.1(h), A.6.1.1, A.7.2.1, A.7.2.2, A.12.1.1

European Medicines Agency (EMA) - Eudralex Annex 11

Google Cloud Mapping

#	Framework reference	**Google	**Customer	Google Cloud commentary	Google Cloud Compliance Reports / Certificates reference
				Google's data centers are geographically distributed to minimize the effects of regional disruptions on global products such as natural disasters and local outages. In the event of hardware, software, or network failure, platform services and control planes are automatically and instantly shifted from one facility to another so that platform services can continue without interruption. Google's highly redundant infrastructure also helps customers protect themselves from data loss. Google Cloud resources can be created and deployed across multiple regions and zones. Allowing customers to build resilient and highly available systems. Google's Business Continuity Plan and Disaster Recovery Test (DiRT) report can be provided upon request and under NDA. Customers retain control and ownership for the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system).	ISO 27017: CLD12.1.5, 6.1.1, 7.2.2, 15.1.1, 15.1.3 ISO 27018: None NIST SP800-53 R3: CP-1,CP-6, CP-7, PE-17, CP-2, CP-3, CP-4,PE-4, CP-9, CP-10,PE-1, PE-5,PE-15, PE-18, MA-2, MA-3, MA-4, MA-5, MA-6, CP-8, PE-1, PE-9, PE-10, PE-11, PE-12, PE-13, PE-14, RA-3, CM-2, CM-3, CM-4, CM-5, CM-6, CM-9, MA-4, SA-3, SA-4, SA-5, SA-8, SA-10, SA-11, SA-12 BSI C5:2020: AM-03, PS-05, SA-01, PS-01, PS-02, PS-03, PS-04, BCM-01,BCM-02, BCM-03, BCM-04, BCM-05
17	**Archiving** Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.	☑	☑	Policies and procedures are established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness. Customers retain control and ownership over their content. Customers are responsible for managing their data retention policies. Customers may leverage the features of our storage services. Please see product documentation for examples of such services: • Google Cloud online storage products • Retention policies and retention policy locks	CSA CCM v4: DSP-18, LOG-09 SOC 2 Type II: A1.2, A1.3, I3.21 ISO 27001: 9.2(g), 7.5.3(b), 5.2 (c), 7.5.3(d), 5.3(a), 5.3(b), 8.1, 8.3, A.12.3.1, A.8.2.3 ISO 27017: 12.3.1, 15.1.1, 15.1.3 ISO 27018: None NIST SP800-53 R3: CP-2, CP-6, CP-7, CP-8, CP-9, SI-12, AU-11 BSI C5:2020: RB-06, RB-08