CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
The information described in this paper is detailed as of the time of authorship. The information in this document does not amend or in any way alter Google's security obligations as part of its contractual agreement with Customer. Google may discontinue or change the processes, procedures and controls described in this document at any time without notice as we regularly innovate with new features and products within Google Cloud. Google's security obligations are described in its contractual agreement with Customer which may include our Data Processing Amendment and/or Data Processing and Security Terms if opted-in to by Customer.									
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Google maintains and implements comprehensive internal and external audit plans that are performed semi-annually to test the efficiency and effectiveness of implemented security controls against recognized standards such as PCI-DSS, NIST 800-53, AICPA Trust Services Criteria (SOC2), and ISO/IEC 27001 security objectives.		A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	Audit and Assurance Policy and Procedures	Audit & Assurance
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?	Yes	CSP-owned	Google reviews audit and assurance policies and procedures annually.					
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Yes	CSP-owned	Google conducts independent audits on a semi-annual basis to determine whether the information protection program is approved by executive management, communicated to stakeholders, adequately resourced, conforms to relevant legislation or regulations and other business requirements, and adjusted as needed to ensure the program continues to meet defined objectives. For a full list of available certificates and compliance materials, please refer to: https://cloud.google.com/security/compliance		A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Independent Assessments	
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	Yes	CSP-owned	Google's independent audit and assurance assessments are performed according to the risk environment across the organization to enable effective risk management.		A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	Risk Based Planning Assessment	
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	Yes	CSP-owned	Google maintains and implements comprehensive internal and external audit plans that are performed at least annually to test the efficiency and effectiveness of implemented security controls against recognized standards such as PCI-DSS, NIST 800-53, AICPA Trust Services Criteria (SOC2), and ISO/IEC 27001 security objectives.		A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	Requirements Compliance	
A&A-05.1	Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports and supporting evidence?	Yes	CSP-owned	Google maintains and implements comprehensive internal and external audit plans which include audit planning, risk analysis, control assessments, remediations, reporting, and reviews of past reports/evidence that are performed at least annually to test the efficiency and effectiveness of implemented security controls against recognized standards.		A&A-05	Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	Audit Management Process	
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Google uses a formal methodology with defined criteria for determining risk-based treatments and ensuring that corrective action plans for the security program and the associated organizational information systems are prioritized and maintained; and the remedial information security actions necessary to mitigate risk to organizational operations and assets, individuals, and other organizations are documented.		A&A-06	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders.	Remediation	
A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?	Yes	CSP-owned	Google continually communicates remediation status of audit findings to relevant stakeholders.					
AIS-01.1	Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to guide appropriate planning, delivery, and support of the organization's application security capabilities?	Yes	CSP-owned	Google has an Applications, Systems, and Services Security Policy, which supports the system development lifecycle.		AIS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organization's application security capabilities. Review and update the policies and procedures at least annually.	Application and Interface Security Policy and Procedures	
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Google has processes in place to review and update Security & Privacy policies annually. The policies for application security fall under this category.					
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Yes	Shared CSP and CSC	Google has a policy for both Device Security Configuration Guidelines and Corporate Services Security. It outlines the baseline requirements for devices and applications deployed within the organization.	Customers are responsible for establishing baseline requirements to secure applications within the customer's GCP instance.	AIS-02	Establish, document and maintain baseline requirements for securing different applications.	Application Security Baseline Requirements	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	Yes	CSP-owned	Google's security engineering organization ensures effectiveness of the information protection program through program oversight. As part of the program oversight, the organization establishes and communicates Objective Key Results (OKRs) and updates of Google's security plan. The organization also ensures organizational compliance with the security plan, and evaluates risks through annual risk assessments performed and accepts security risks on behalf of Google.		AIS-03	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.	Application Security Metrics	Application & Interface Security
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	Yes	CSP-owned	Google has a policy for security design in applications, systems, and services to ensure that security is accounted for in all stages of the development process. Google uses a continuous build and release process informed by industry practices.		AIS-04	Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization.	Secure Application Design and Development	
AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?	Yes	CSP-owned	Google has guidelines to perform fuzz testing, sandboxing, third-party library monitoring, source code analysis, and vulnerability scanning to detect, mitigate, and resolve security issues as part of the software testing lifecycle.		AIS-05	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible.	Automated Application Security Testing	
AIS-05.2	Is testing automated when applicable and possible?	Yes	CSP-owned	Google engineering's continuous build system utilizes an automated testing platform which runs tests automatically at every changelist.					
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Yes	CSP-owned	Google follows a structured code development and release process that includes considerations for security defects and all code is peer reviewed. Google makes purpose built code analysis tools available for engineers to deploy against application code.		AIS-06	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	Automated Secure Application Deployment	
AIS-06.2	Is the deployment and integration of application code automated where possible?	Yes	CSP-owned	Google follows a structured code development and release process that includes considerations for security defects and all code is peer reviewed. Google makes purpose built code analysis tools available for engineers to deploy against application code and performs continuous post-production monitoring based on real-time threats.					
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	Yes	Shared CSP and CSC	Google has implemented a vulnerability management program to detect and remediate system vulnerabilities. Google also performs periodic application-layer vulnerability scans using commercial and proprietary tools. Vulnerability management is also discussed in the security whitepaper: https://cloud.google.com/security/overview/whitepaper	Customers are responsible for remediation of application security vulnerabilities within customer's GCP instance.	AIS-07	Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.	Application Vulnerability Remediation	
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	Yes	Shared CSP and CSC	Google has implemented a vulnerability management program to track and remediate system vulnerabilities in accordance with established benchmarks. Google also performs periodic application-layer vulnerability scans using commercial and proprietary tools. Google has a team dedicated to automated vulnerability management. Vulnerability management is also discussed in the security whitepaper: https://cloud.google.com/security/overview/whitepaper	Customers are responsible for establishing automated remediation of application security vulnerabilities within customer's GCP instance, when possible.				
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Google implements a business continuity plan for our Services, reviews and tests it at least annually and ensures it remains current with industry standards. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide https://cloud.google.com/solutions/dr-scenarios-planning-guide		BCR-01	Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually.	Business Continuity Management Policy and Procedures	
BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Google's business and systems resilience policy is reviewed annually.					

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	Yes	CSP-owned	Google has established criteria for the business continuity plan to identify and take into consideration potential risk areas, likelihood and intensity of business disruptions, and the impact of these disruptions.		BCR-02	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities.	Risk Assessment and Impact Analysis	Business Continuity Management and Operational Resilience
BCR-03.1	Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?	Yes	CSP-owned	Google routinely performs impact analysis for possible disruptions to cloud services and performs post-mortems to understand the root cause, and mitigate future disruptions.		BCR-03	Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.	Business Continuity Strategy	
BCR-04.1	Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan?	Yes	CSP-owned	Google routinely performs impact analysis for possible disruptions to cloud services and performs post-mortems to understand the root cause, and mitigate future disruptions. These strategies are incorporated into the organization's business continuity management plans.		BCR-04	Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities.	Business Continuity Planning	
BCR-05.1	Is relevant documentation developed, identified, and acquired to support business continuity and operational resilience plans?	Yes	CSP-owned	The detailed business continuity and redundancy plans are internal to Google. However, the existence and operating effectiveness of the same, is verified as part of our SOC 2/3 audit reports.		BCR-05	Develop, identify, and acquire documentation that is relevant to support the business continuity and operational resilience programs. Make the documentation available to authorized stakeholders and review periodically.	Documentation	
BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	Yes	CSP-owned	The detailed business continuity and redundancy plans are internal to Google. However, the existence and operating effectiveness of the same, is verified as part of our SOC 2/3 audit reports.					
BCR-05.3	Is business continuity and operational resilience documentation reviewed periodically?	Yes	CSP-owned	Google implements a business continuity plan for our Services, reviews and tests it at least annually and ensures it remains current with industry standards.					
BCR-06.1	Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?	Yes	CSP-owned	Google performs annual testing of its business continuity plans to simulate disaster scenarios that model catastrophic events that may disrupt Google operations.		BCR-06	Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.	Business Continuity Exercises	
BCR-07.1	Do business continuity and resilience procedures establish communication with stakeholders and participants?	Yes	CSP-owned	Google has processes during the business continuity procedure to list out teams and key contacts across Google Cloud infrastructure and services to work collaboratively with when identifying potential risks, disruptions, and impact.		BCR-07	Establish communication with stakeholders and participants in the course of business continuity and resilience procedures.	Communication	
BCR-08.1	Is cloud data periodically backed up?	Yes	Shared CSP and CSC	Google's geographically dispersed storage services provide replication to backup system software and data so that user data is written to at least two other clusters. A combination of synchronous and asynchronous replication methods are used. Google's highly available solution is discussed in the security whitepaper: https://cloud.google.com/security/overview/whitepaper	Customers are responsible for backups of data stored in their GCP instance.	BCR-08	Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency.	Backup	
BCR-08.2	Is the confidentiality, integrity, and availability of backup data ensured?	Yes	Shared CSP and CSC	Google's backup data is subject to the same logical and physical security controls as other data to protect the confidentiality, availability, and integrity of data.	Customers are responsible for ensuring confidentiality, integrity, and availability of backups of data stored in their GCP instance.				
BCR-08.3	Can backups be restored appropriately for resiliency?	Yes	Shared CSP and CSC	Google's geographically dispersed storage services provide replication to backup system software and data so that user data is written to at least two other clusters. A combination of synchronous and asynchronous replication methods are used. Google's highly available solution is discussed in the security whitepaper: https://cloud.google.com/security/overview/whitepaper	Customers are responsible for ensuring backups of data stored in their GCP instance can be restored appropriately for resiliency.				
BCR-09.1	Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?	Yes	CSP-owned	Google automatically replicates to and serves data from multiple data centers to provide seamless access to end-users should a datacenter not be available. This ensures recovery from natural and man-made disasters.		BCR-09	Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes.	Disaster Response Plan	
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	Yes	CSP-owned	Google performs annual testing of its business continuity plans to simulate disaster scenarios that model catastrophic events that may disrupt Google operations. As part of this annual testing, playbooks are also tested and refined.					

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	Yes	CSP-owned	Google performs annual testing of its business continuity plans to simulate disaster scenarios that model catastrophic events that may disrupt Google operations.		BCR-10	Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities.	Response Plan Exercise	
BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	No	CSP-owned	Google has an internal security operations team to act as a liaison with emergency personnel.					
BCR-11.1	Is business-critical equipment supplemented with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards?	Yes	CSP-owned	Google does not rely on any one specific data center for its continued operation and allocates redundant equipment, applications, services and data across multiple data centers. Google's production services are designed with hardware redundancy, multi-homing and automatic failover. This is discussed in Google's security whitepaper: https://cloud.google.com/security/overview/whitepaper		BCR-11	Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards.	Equipment Redundancy	
CCC-01.1	Are risk management policies and procedures associated with changing organizational assets including applications, systems, infrastructure, configuration, etc., established, documented, approved, communicated, applied, evaluated and maintained (regardless of whether asset management is internal or external)?	Yes	CSP-owned	Google has established change management policies and procedures which integrate the risk management process with the change management process. Google's change management process 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.		CCC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually.	Change Management Policy and Procedures	Change Control and Configuration Management
CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Google has processes in place to review Security & Privacy policies annually. The policies for change management fall under this category.					
CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	Yes	CSP-owned	Google maintains policy and procedures to ensure consideration of security, quality and availability throughout the SDLC (Software Development Lifecycle). In addition, Google develops, documents, and maintains a current baseline for all machines and network device hardware. System changes are code reviewed by a separate technical resource to evaluate quality and accuracy of changes.		CCC-02	Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.	Quality Testing	
CCC-03.1	Are risks associated with changing organizational assets (including applications, systems, infrastructure, configuration, etc.) managed, regardless of whether asset management occurs internally or externally (i.e., outsourced)?	Yes	CSP-owned	Google's risk management process is integrated with the change management process within the organization.		CCC-03	Manage the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced).	Change Management Technology	
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted?	Yes	CSP-owned	Google has change management policies and procedures in place to restrict unauthorized changes to Google's applications, services, and systems.		CCC-04	Restrict the unauthorized addition, removal, update, and management of organization assets.	Unauthorized Change Protection	
CCC-05.1	Are provisions to limit changes that directly impact CSC-owned environments and require tenants to authorize requests explicitly included within the service level agreements (SLAs) between CSPs and CSCs?	Yes	CSP-owned	Google provides customers an advance notice for all system changes having an impact on their environment. Audit logs are made to customers for all system changes and support activities performed by GCP teams in the customer environment. Google's agreements regarding modifications are discussed below: https://cloud.google.com/terms/ Google's agreements regarding changes to subprocessors are discussed below: https://cloud.google.com/terms/data-processing-terms		CCC-05	Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs.	Change Agreements	
CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	Yes	CSP-owned	Google develops, documents, and maintains under configuration control, a current baseline configuration of the information system.		CCC-06	Establish change management baselines for all relevant authorized changes on organization assets.	Change Management Baseline	

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	Yes	CSP-owned	Google maintains configuration management tools to detect and automatically correct deviations from its baseline configuration and collects and secures audit records.		CCC-07	Implement detection measures with proactive notification in case of changes deviating from the established baseline.	Detection of Baseline Deviation	
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Yes	CSP-owned	Google's change management policies and procedures include an exception process for relevant use cases which require approvals, and an emergency process to be used by authorized personnel only which require emergency changes and tests to be reviewed in a timely manner.		CCC-08	Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. Align the procedure with the requirements of GRC-04: Policy Exception Process.	Exception Management	
CCC-08.2	Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?	Yes	CSP-owned	Google has a policy exception process (which also applies to change management exceptions) which aligns business needs with associated level of risk and requires multiple layers of approval. In addition, Google has automated mechanisms to detect deviations from the desired security configuration of its infrastructure.					
CCC-09.1	Is a process to proactively roll back changes to a previously known "good state" defined and implemented in case of errors or security concerns?	Yes	CSP-owned	Google has processes in place to roll back changes or manage operational impact in case the changes have an adverse impact on the production environment.		CCC-09	Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns.	Change Restoration	
CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Google has established policies and procedures that govern the use of cryptographic controls. Google has an established key management process in place to support the organization's use of cryptographic techniques.		CEK-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually.	Encryption and Key Management Policy and Procedures	
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Google has processes in place to review Security & Privacy policies annually. The policies for cryptography, encryption, and key management fall under this category.					
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Yes	CSP-owned	Google has policies in place that outline cryptography, encryption, and key management protocols and specific requirements. Policies on cryptographic guidelines include roles and responsibilities. Google's key management operates as a service for engineering teams to use in their application code.		CEK-02	Define and implement cryptographic, encryption and key management roles and responsibilities.	CEK Roles and Responsibilities	
CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	Yes	Shared CSP and CSC	Google uses a combination of open source and proprietary encryption formats and algorithms validated by Google security engineers. Google has security whitepapers on encryption at rest and in transit: https://cloud.google.com/security/encryption-in-transit https://cloud.google.com/security/encryption/default-encryption	Customers may opt to use the Cloud Key Management Service which allows customers to manage encryptions for their GCP cloud instance the same way they do in their local environment.	CEK-03	Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.	Data Encryption	
CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	Yes	Shared CSP and CSC	Google has established policies and procedures that govern the use of cryptographic controls. Google has an established key management process in place to support the organization's use of cryptographic techniques. Google uses a combination of open source and proprietary encryption formats and algorithms validated by Google security engineers.	Customers may opt to use the Cloud Key Management Service which allows customers to manage encryptions for their GCP cloud instance the same way they do in their local environment.	CEK-04	Use encryption algorithms that are appropriate for data protection, considering the classification of data, associated risks, and usability of the encryption technology.	Encryption Algorithm	
CEK-05.1	Are standard change management procedures established to review, approve, implement and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources?	Yes	CSP-owned	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.		CEK-05	Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes.	Encryption Change Management	

CAIQ

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
CEK-06.1	Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?	Yes	CSP-owned	Google has processes in which the encryption system and policy are centrally managed. The changes to policy are reviewed by the compliance/security team. Any changes or updates to the system are reviewed by different stakeholders and considered backward compatible when updated. The change is rolled out step by step to allow different stakeholders to adapt the changes.		CEK-06	Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis.	Encryption Change Cost Benefit Analysis	Cryptography, Encryption & Key Management
CEK-07.1	Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions?	Yes	CSP-owned	Google performs a risk assessment for its offerings and the supporting infrastructure in which assets are identified and threats, vulnerabilities, impact, and likelihood are assessed.		CEK-07	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.	Encryption Risk Management	
CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	Yes	CSP-owned	Google provides capabilities to encrypt data by tenant for a subset of products. Customers can manage their own encryption keys on Google Cloud using Cloud Key Management Services. https://cloud.google.com/security/encryption-at-rest/		CEK-08	CSPs must provide the capability for CSCs to manage their own data encryption keys.	CSC Key Management Capability	
CEK-09.1	Are encryption and key management systems, policies, and processes audited with a frequency proportional to the system's risk exposure, and after any security event?	Yes	CSP-owned	Google uses a proprietary Key Management Service to manage the distribution, generation and rotation of cryptographic keys. In addition, Google's cryptography policy includes guidance on the rotation of keys at regular intervals automatically. This policy also includes requirements on key rotation in case of compromise or other security issues. The existence and operating effectiveness of Google's encryption and key management, is verified as part of our SOC 2 audit report.		CEK-09	Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and after any security event(s).	Encryption and Key Management Audit	
CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	Yes	CSP-owned	Google uses a proprietary Key Management Service to manage the distribution, generation and rotation of cryptographic keys. In addition, Google's cryptography policy includes guidance on the rotation of keys at regular intervals automatically. This policy also includes requirements on key rotation in case of compromise or other security issues. The existence and operating effectiveness of Google's encryption and key management, is verified as part of our SOC 2 audit report.					
CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	Yes	CSP-owned	Google follows formal practices for key generation, distribution, storage, access and destruction that are informed by industry best practices and NIST SP 800-57 - Recommendation for Key Management. Google uses a combination of open source and proprietary code to develop its encryption solutions. The libraries and algorithms used are discussed in the security whitepapers below: https://cloud.google.com/security/encryption-in-transit https://cloud.google.com/security/encryption/default-encryption		CEK-10	Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.	Key Generation	
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	Yes	CSP-owned	Google uses a proprietary Key Management Service for storage of cryptographic keys and secrets. Google also maintains guidelines on key/secret storage. The existence and operating effectiveness of Google's encryption and key management, is verified as part of our SOC 2 audit report.		CEK-11	Manage cryptographic secret and private keys that are provisioned for a unique purpose.	Key Purpose	
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	Yes	CSP-owned	Google uses a proprietary system to periodically generate and rotate an encryption key used to protect user data at rest on average at least every 90 days.		CEK-12	Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.	Key Rotation	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
CEK-13.1	Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions?	Yes	CSP-owned	Google uses a proprietary Key Management Service to manage key revocation. Key revocation, including in emergency situations, is a built in component to the rotation mechanism.		CEK-13	Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements.	Key Revocation	
CEK-14.1	Are processes, procedures and technical measures to destroy unneeded keys defined, implemented and evaluated to address key destruction outside secure environments, revocation of keys stored in hardware security modules (HSMs), and include applicable legal and regulatory requirement provisions?	Yes	CSP-owned	Google uses a proprietary Key Management Service to manage the distribution, generation and rotation of cryptographic keys. In addition, Google's cryptography policy includes guidance on the rotation of keys at regular intervals automatically. The existence and operating effectiveness of Google's encryption and key management, is verified as part of our SOC 2 audit report.		CEK-14	Define, implement and evaluate processes, procedures and technical measures to destroy keys stored outside a secure environment and revoke keys stored in Hardware Security Modules (HSMs) when they are no longer needed, which include provisions for legal and regulatory requirements.	Key Destruction	
CEK-15.1	Are processes, procedures, and technical measures to create keys in a pre-activated state (i.e., when they have been generated but not authorized for use) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSP-owned	Google uses a proprietary Key Management Service to manage the distribution, generation and rotation of cryptographic keys. In addition, Google's cryptography policy includes guidance on the rotation of keys at regular intervals automatically. The existence and operating effectiveness of Google's encryption and key management, is verified as part of our SOC 2 audit report.		CEK-15	Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements.	Key Activation	
CEK-16.1	Are processes, procedures, and technical measures to monitor, review and approve key transitions (e.g., from any state to/from suspension) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSP-owned	Google uses a proprietary Key Management Service to manage the distribution, generation and rotation of cryptographic keys. In addition, Google's cryptography policy includes guidance on the rotation of keys at regular intervals automatically. The existence and operating effectiveness of Google's encryption and key management, is verified as part of our SOC 2 audit report.		CEK-16	Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements.	Key Suspension	
CEK-17.1	Are processes, procedures, and technical measures to deactivate keys (at the time of their expiration date) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSP-owned	Google uses a proprietary Key Management Service to manage the distribution, generation and rotation of cryptographic keys. In addition, Google's cryptography policy includes guidance on the rotation of keys at regular intervals automatically. The existence and operating effectiveness of Google's encryption and key management, is verified as part of our SOC 2 audit report.		CEK-17	Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements.	Key Deactivation	
CEK-18.1	Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSP-owned	Google has technical mechanisms in which its proprietary Key Management System has a built in feature to keep inactive keys for archival purposes. The existence and operating effectiveness of Google's encryption and key management, is verified as part of our SOC 2 audit report.		CEK-18	Define, implement and evaluate processes, procedures and technical measures to manage archived keys in a secure repository requiring least privilege access, which include provisions for legal and regulatory requirements.	Key Archival	
CEK-19.1	Are processes, procedures, and technical measures to encrypt information in specific scenarios (e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSP-owned	Google has policies in place for scenarios in which data must be encrypted, along with additional legal, compliance, or security requirements.		CEK-19	Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstance, and thereafter exclusively for decrypting data and never for encrypting data, which include provisions for legal and regulatory requirements.	Key Compromise	
CEK-20.1	Are processes, procedures, and technical measures to assess operational continuity risks (versus the risk of losing control of keying material and exposing protected data) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSP-owned	Google performs a risk assessment for its offerings and the supporting infrastructure in which assets are identified and threats, vulnerabilities, impact, and likelihood are assessed.		CEK-20	Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost, which include provisions for legal and regulatory requirements.	Key Recovery	
CEK-21.1	Are key management system processes, procedures, and technical measures being defined, implemented, and evaluated to track and report all cryptographic materials and status changes that include legal and regulatory requirements provisions?	Yes	CSP-owned	Google has an established key management process in place to support the organization's use of cryptographic techniques. Google uses a proprietary Key Management Service to manage the distribution, generation and rotation of cryptographic keys. Only authorized Google services and users are allowed access to a key. Auditing is enabled.		CEK-21	Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and report all cryptographic materials and changes in status, which include provisions for legal and regulatory requirements.	Key Inventory Management	

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
DCS-01.1	Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?	Yes	CSP-owned	Google has strict policies and procedures to govern the management of the equipment lifecycle within its production data centers. Any disk that did, at any point in its lifecycle, contain customer data is subject to a series of data destruction processes before leaving Google's premises, and would need to be authorized by appropriate operations manager before release. For more information, please see: https://cloud.google.com/security/deletion		DCS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually.	Off-Site Equipment Disposal Policy and Procedures	
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Yes	CSP-owned	Google describes its logical deletion methods in the security whitepaper below. Overwriting or cryptographic erasure are the 2 methods used for rendering information unreadable, depending on the product. https://cloud.google.com/security/deletion					
DCS-01.3	Are policies and procedures for the secure disposal of equipment used outside the organization's premises reviewed and updated at least annually?	Yes	CSP-owned	Google has data destruction guidelines and a media erase policy which are both reviewed and updated at least annually.					
DCS-02.1	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained?	Yes	CSP-owned	Google has strict policies and procedures for the offsite storage of encrypted backup tapes and decommissioned hardware. Software and other data is not relocated or transferred offsite.		DCS-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location.The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually.	Off-Site Transfer Authorization Policy and Procedures	
DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	Yes	CSP-owned	Google has strict policies and procedures for the offsite storage of encrypted backup tapes and decommissioned hardware. Software and other data is not relocated or transferred offsite. Any disk that did, at any point in its lifecycle, contain customer data is subject to a series of data destruction processes before leaving Google's premises, and would need to be authorized by appropriate operations manager before release.					
DCS-02.3	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location reviewed and updated at least annually?	Yes	CSP-owned	Google has guidelines on shipping tapes offsite which are reviewed and updated at least annually.					
DCS-03.1	Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?	Yes	CSP-owned	Google maintains a physical security policy that describes the requirements for maintaining a safe and secure work environment.		DCS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually.	Secure Area Policy and Procedures	
DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	Yes	CSP-owned	Google has processes in place to review Security & Privacy policies annually. The policies specific to safe and secure workspaces within the data center fall under this category.					
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	Yes	CSP-owned	Google has policies and procedures in place for the data security of tapes which discusses off site transportation. Requirements for encrypting data are outlined, in addition to guidelines on the use of a case during transport.		DCS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually.	Secure Media Transportation Policy and Procedures	
DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?	Yes	CSP-owned	Google has a data security of tapes policy which is reviewed and updated at least annually.					
DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	Yes	CSP-owned	Google considers all digital media contains the highest classification of data and must be destroyed according to the data destruction guidelines for the highest classification.		DCS-05	Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk.	Assets Classification	
DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	Yes	CSP-owned	Google maintains asset inventories and assigns ownership for managing its critical resources.		DCS-06	Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured system.	Assets Cataloguing and Tracking	
DCS-07.1	Are physical security perimeters implemented to safeguard personnel, data, and information systems?	Yes	CSP-owned	Google implemented a combination of CCTV cameras, ID cards, retina scans, mantraps, and gate checkpoints which are used to monitor ingress and egress at the various physical security zones in a Data Center.		DCS-07	Implement physical security perimeters to safeguard personnel, data, and information systems. Establish physical security perimeters between the administrative and business areas and the data storage and processing facilities areas.	Controlled Access Points	
DCS-07.2	Are physical security perimeters established between administrative and business areas, data storage, and processing facilities?	Yes	CSP-owned	Google implemented a combination of CCTV cameras, ID cards, retina scans, mantraps, and gate checkpoints which are used to monitor ingress and egress at the various physical security zones in a Data Center.					

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
DCS-08.1	Is equipment identification used as a method for connection authentication?	Yes	CSP-owned	Google uses certificates and ACLs to achieve authentication integrity.		DCS-08	Use equipment identification as a method for connection authentication.	Equipment Identification	Datacenter Security
DCS-09.1	Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms?	Yes	CSP-owned	Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system that are linked to a system alarm. Only authorized employees, contractors, and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request (which is followed by proper approval process) electronic card key access to these facilities. Access to perimeter doors, shipping and receiving, and other critical areas is logged, including unauthorized activity. Failed access attempts are logged by the access control system and investigated as appropriate. Authorized access throughout the business operations and data centers is restricted based on an individual's job responsibilities. The fire doors at the data centers are alarmed and can only be opened from the inside. CCTV cameras are in operation both inside and outside the data centers. Security operations personnel manage the CCTV monitoring, recording and control equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week.		DCS-09	Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization.	Secure Area Authorization	
DCS-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	Yes	CSP-owned	Google logs all physical access of its data center employees and retains them according to Google's retention policy.					
DCS-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	Yes	CSP-owned	Google Data centers maintain secure external perimeter protections. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to help cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. Security operations personnel manage the CCTV monitoring, recording and control equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week.		DCS-10	Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts.	Surveillance System	
DCS-11.1	Are datacenter personnel trained to respond to unauthorized access or egress attempts?	Yes	CSP-owned	Google's data center security training program contains training to respond to unauthorized access and disruptive person as well as an alarm training on how to respond to alarm alerts.		DCS-11	Train datacenter personnel to respond to unauthorized ingress or egress attempts.	Unauthorized Access Response Training	
DCS-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms?	Yes	CSP-owned	Google's data centers rely on hardware redundancy which includes power supplies and cables. Google's security whitepaper explains the redundancy of our data centers in more detail: https://cloud.google.com/security/overview/whitepaper		DCS-12	Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication cables from a threat of interception, interference or damage at all facilities, offices and rooms.	Cabling Security	
DCS-13.1	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?	Yes	CSP-owned	Google has mechanisms in place to monitor and maintain data center temperatures and humidity through the use of smart temperature controls and "free-cooling" techniques like using outside air or reused water for cooling. Cooling systems maintain a constant operating temperature for servers and other hardware. Processes are tested as part of annual disaster recovery testing. Google's security whitepaper explains the environmental impact of our data centers in more detail;: https://cloud.google.com/security/overview/whitepaper		DCS-13	Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.	Environmental Systems	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
DCS-14.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	Yes	CSP-owned	Google has mechanisms in place to address utility outages through the implementation of a primary and alternative power source, each with equal power, for every critical component. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Processes are tested as part of annual disaster recovery testing. Google's security whitepaper explains the redundancy of our data centers in more detail: https://cloud.google.com/security/overview/whitepaper		DCS-14	Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals.	Secure Utilities	
DCS-15.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?	Yes	CSP-owned	Google has processes in place during data center design to consider security and environmental factors when determining locations for critical rooms and equipment floor plans within the data center. Google carefully selects the locations of its data centers to avoid exposure to high-impact environmental risks to the extent possible.		DCS-15	Keep business-critical equipment away from locations subject to high probability for environmental risk events.	Equipment Location	
DSP-01.1	Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?	Yes	CSP-owned	Google maintains policies and procedures on data classification, protection, and handling throughout its lifecycle according to legal and regulatory requirements.		DSP-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually.	Security and Privacy Policy and Procedures	
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Google has processes in place to review Security & Privacy policies annually. The policies specific to data security and privacy fall under this category.					
DSP-02.1	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?	Yes	CSP-owned	Google's process for data deletion upon termination is described in our DPST and DPA. https://cloud.google.com/terms/data-processing-terms Google also has a security whitepaper on data deletion and backup deletion: https://cloud.google.com/security/deletion#overview		DSP-02	Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.	Secure Disposal	
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	Yes	CSP-owned	Google maintains a data security policy which requires data to be managed consistent with Google's standards and policies regarding data classification, categorization, and the lifecycle of data through destruction.		DSP-03	Create and maintain a data inventory, at least for any sensitive data and personal data.	Data Inventory	
DSP-04.1	Is data classified according to type and sensitivity levels?	Yes	CSP-owned	Google has data classification policies in place to describe how data should be classified and handled according to type of data and sensitivity levels to ensure its confidentiality, integrity, and availability.		DSP-04	Classify data according to its type and sensitivity level.	Data Classification	
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	Yes	CSP-owned	Google maintains an internal launch system to document, review, and approve launches, and this process requires teams to submit design documents including data flow in order for Google to meet the data commitments to its customers. Google's respective product teams create and maintain data flow documentation.		DSP-05	Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, and after any change.	Data Flow Documentation	
DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	Yes	CSP-owned	Google has processes for product teams to review data flow documentation at least annually.					
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	Yes	CSP-owned	Google's data security policy requires data to have an owner, defined as the person or group responsible for managing and protecting the data.		DSP-06	Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.	Data Ownership and Stewardship	
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	Yes	CSP-owned	Google has processes in place to review Security & Privacy policies annually. The policies specific to data ownership and stewardship fall under this category.					

CAIQ

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	Yes	CSP-owned	Google has processes in place to ensure security is taken into account in all stages of the development lifecycle, including design. The security team is engaged to perform security reviews. Google also has a whitepaper on security design: https://cloud.google.com/security/infrastructure/design		DSP-07	Develop systems, products, and business practices based upon a principle of security by design and industry best practices.	Data Protection by Design and Default	Data Security and Privacy Lifecycle Management
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	Yes	CSP-owned	Google has processes in place to follow a privacy by design approach which includes awareness, training and education, privacy consulting and review, and development patterns that apply privacy protections.		DSP-08	Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.	Data Privacy by Design and Default	
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	Yes	CSP-owned	Google has processes in place to follow a privacy by design approach which includes privacy consulting and review and development patterns that apply privacy protections for all launches. Privacy settings' configuration by default according to applicable laws and regulations are taken into account during the privacy review in the privacy launch process.					
DSP-09.1	Is a data protection impact assessment (DPIA) conducted when processing personal data and evaluating the origin, nature, particularity, and severity of risks according to any applicable laws, regulations and industry best practices?	Yes	CSP-owned	Google has processes to perform Data Protection Impact Assessments to meet the GDPR's requirements around Privacy by Design and Privacy by Default. All DPIA needs to be approved by the security and privacy team.		DSP-09	Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data, according to any applicable laws, regulations and industry best practices.	Data Protection Impact Assessment	
DSP-10.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?	Yes	CSP-owned	Google details its security measures to protect against unauthorized personal or sensitive data access, and also details its data transfer agreements as permitted by respective laws and regulations in the Data Processing and Security Terms. https://cloud.google.com/terms/data-processing-terms		DSP-10	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.	Sensitive Data Transfer	
DSP-11.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?	Yes	CSP-owned	Google details its agreements to enable data subjects to fulfill requests per applicable laws and regulations in the Data Processing and Security Terms. https://cloud.google.com/terms/data-processing-terms		DSP-11	Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations.	Personal Data Access, Reversal, Rectification and Deletion	
DSP-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data subject)?	Yes	CSP-owned	Google details its agreements to ensure personal data is processed per applicable laws and regulations and for the purposes declared to the data subject in the Data Processing and Security Terms. https://cloud.google.com/terms/data-processing-terms		DSP-12	Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.	Limitation of Purpose in Personal Data Processing	
DSP-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)?	Yes	CSP-owned	Google details its agreements for the transfer and subprocessing of personal data within the service supply chain per applicable laws and regulations in the Data Processing and Security Terms. https://cloud.google.com/terms/data-processing-terms		DSP-13	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	Personal Data Sub-processing	
DSP-14.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation?	Yes	CSP-owned	Google details the disclosure of any personal or sensitive data by subprocessors prior to processing initiation through the Data Processing and Security Terms agreed upon by the customer and Google. https://cloud.google.com/terms/data-processing-terms		DSP-14	Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing.	Disclosure of Data Sub-processors	
DSP-15.1	Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?	Yes	CSP-owned	Google has established procedures which require that production data is not used in non-production systems without sanitization or approval from the privacy working group. Technical controls are in place to help ensure production data remains in the secure boundary of the production network.		DSP-15	Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments.	Limitation of Production Data Use	

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	Yes	CSP-owned	Google details its agreements for data deletion (including retention) and data export per applicable laws and regulations in the Data Processing and Security Terms. https://cloud.google.com/terms/data-processing-terms Google also has a whitepaper on data deletion: https://cloud.google.com/security/deletion		DSP-16	Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.	Data Retention and Deletion	
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	Yes	CSP-owned	Google details the security measures taken in its Data Processing and Security Terms under Appendix 2. https://cloud.google.com/terms/data-processing-terms Google also discusses this in its security whitepaper: https://cloud.google.com/security/overview/whitepaper		DSP-17	Define and implement, processes, procedures and technical measures to protect sensitive data throughout it's lifecycle.	Sensitive Data Protection	
DSP-18.1	Does the CSP have in place, and describe to CSCs, the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations?	Yes	CSP-owned	Google has a policy on how it handles government requests for user information. https://policies.google.com/terms/information-requests Google also discusses law enforcement data requests in the security whitepaper: https://cloud.google.com/security/overview/whitepaper		DSP-18	The CSP must have in place, and describe to CSCs the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations. The CSP must give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation.	Disclosure Notification	
DSP-18.2	Does the CSP give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation?	Yes	CSP-owned	Google has a policy on how it handles government requests for user information. This policy includes a section on notifying the user of the request. https://policies.google.com/terms/information-requests					
DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?	Yes	CSP-owned	Google's geographically dispersed storage services provide replication to backup system software and data so that user data is written to at least two other clusters. A combination of synchronous and asynchronous replication methods are used. Google's highly available solution is discussed in the security whitepaper: https://cloud.google.com/security/overview/whitepaper Google Cloud locations: https://cloud.google.com/about/locations		DSP-19	Define and implement, processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up.	Data Location	
GRC-01.1	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Google maintains an internal ISMS and evidence of its effectiveness is provided via ISO/IEC 27001 certification.		GRC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually.	Governance Program Policy and Procedures	Governance, Risk and Compliance
GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Google reviews its ISMS documentation annually as part of its required due diligence.					
GRC-02.1	Is there an established formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks?	Yes	CSP-owned	Google has documented its risk management procedures as part of its ISMS that underlies our ISO/IEC 27001 certification.		GRC-02	Establish a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks.	Risk Management Program	
GRC-03.1	Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?	Yes	CSP-owned	Google reviews its ISMS documentation annually as part of its required due diligence. Google also reviews its security and privacy policies annually.		GRC-03	Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization.	Organizational Policy Reviews	
GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	Yes	CSP-owned	Google has a policy exception process which aligns business needs with associated level of risk and requires multiple layers of approval. In addition, Google has automated mechanisms to detect deviations from the desired security configuration of its infrastructure.		GRC-04	Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs.	Policy Exception Process	
GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	Yes	CSP-owned	Google provides comprehensive external documentation and whitepapers detailing our security infrastructure and operational model. Google also maintains an internal ISMS and evidence of its effectiveness is provided via ISO/IEC 27001 certification.		GRC-05	Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM.	Information Security Program	

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	Yes	CSP-owned	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.		GRC-06	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.	Governance Responsibility Model	
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	Yes	CSP-owned	Google maintains a compliance strategic product roadmap where applicable standards, regulations, and requirements are identified. Legal teams are involved in identifying legal and statutory requirements.		GRC-07	Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization.	Information System Regulatory Mapping	
GRC-08.1	Is contact established and maintained with cloud-related special interest groups and other relevant entities?	Yes	CSP-owned	Google maintains contact with the security research community for identifying vulnerabilities. This is explained in the security whitepaper: https://cloud.google.com/security/overview/whitepaper		GRC-08	Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context.	Special Interest Groups	
HRS-01.1	Are background verification policies and procedures of all new employees (including but not limited to remote employees, contractors, and third parties) established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Google performs background checks on new hires and in accordance with applicable local labor law and statutory regulations. Google discusses background checks in its security whitepaper: https://cloud.google.com/security/overview/whitepaper		HRS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements, and acceptable risk. Review and update the policies and procedures at least annually.	Background Screening Policy and Procedures	
HRS-01.2	Are background verification policies and procedures designed according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk?	Yes	CSP-owned	Google performs background checks on new hires and in accordance with applicable local labor law and statutory regulations. The extent of these background checks is dependent on the desired position and whether it is classified as having access to need to know data. Google discusses background checks in its security whitepaper; https://cloud.google.com/security/overview/whitepaper					
HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Google's background verification documentation is reviewed and updated on a regular basis.					
HRS-02.1	Are policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Google has established a Code of Conduct which describes acceptable use expectations of Google's owned and managed assets.		HRS-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets. Review and update the policies and procedures at least annually.	Acceptable Use of Technology Policy and Procedures	
HRS-02.2	Are the policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets reviewed and updated at least annually?	Yes	CSP-owned	Google reviews the Code of Conduct on an annual basis.					
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Google has established formal security policies that requires all personnel to not leave sensitive materials unattended. In addition, workstations, laptops, and mobile devices are configured such that they lockout after a pre-defined period of time.		HRS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces to not have openly visible confidential data. Review and update the policies and procedures at least annually.	Clean Desk Policy and Procedures	
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	Yes	CSP-owned	Google has processes in place to review Security & Privacy policies annually. The policies for concealing confidential data on unattended workspaces fall under this category.					
HRS-04.1	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Google has policies in place for working remotely security guidelines which detail the required security and privacy practices for protecting Google data while working remotely.		HRS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information accessed, processed or stored at remote sites and locations. Review and update the policies and procedures at least annually.	Remote and Home Working Policy and Procedures	
HRS-04.2	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually?	Yes	CSP-owned	Google has processes in place to review Security & Privacy policies annually. The policies for protecting sensitive information at remote locations fall under this category.					
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established and documented?	Yes	CSP-owned	Google has a well defined exit process including equipment return procedures for terminated personnel. Exit checklists are provided to both personnel and their managers to inform them of their obligations for returning organizationally-owned assets.		HRS-05	Establish and document procedures for the return of organization-owned assets by terminated employees.	Asset returns	

CAIQ

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel?	Yes	CSP-owned	Google maintains personnel and data access policies that govern the administration of access controls including transfers and terminations. Additionally, Google removes access to corporate assets in a timely basis upon submission of a termination request.		HRS-06	Establish, document, and communicate to all personnel the procedures outlining the roles and responsibilities concerning changes in employment.	Employment Termination	Human Resources
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	Yes	CSP-owned	Google employees are required to complete Google's Code of Conduct training which addresses responsibilities and expected behavior with respect to the protection of information. Additionally, Google requires employees to sign the Google Confidentiality and Invention Assignment and Arbitration Agreements prior to their start date.		HRS-07	Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets.	Employment Agreement Process	
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	Yes	CSP-owned	Google employees are required to acknowledge the Code of Conduct and complete Google's Code of Conduct training which addresses responsibilities and expected behavior with respect to the protection of information. Additionally, Google requires employees to sign the Google Confidentiality and Invention Assignment and Arbitration Agreements.		HRS-08	The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies.	Employment Agreement Content	
HRS-09.1	Are employee roles and responsibilities relating to information assets and security documented and communicated?	Yes	CSP-owned	Google's Terms of Service outline the responsibilities of Google. In addition, Google maintains internal policies on security requirements for employees with access to corporate services. Google's employees also agree to the Code of Conduct which details commitments to information assets and security. This is further discussed in our security whitepaper: https://cloud.google.com/security/overview/whitepaper		HRS-09	Document and communicate roles and responsibilities of employees, as they relate to information assets and security.	Personnel Roles and Responsibilities	
HRS-10.1	Are requirements for non-disclosure/confidentiality agreements reflecting organizational data protection needs and operational details identified, documented, and reviewed at planned intervals?	Yes	CSP-owned	Google periodically reviews Non-Disclosure Agreement and confidentiality documents. Google personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Google's confidentiality and privacy policies.		HRS-10	Identify, document, and review, at planned intervals, requirements for non-disclosure/confidentiality agreements reflecting the organization's needs for the protection of data and operational details.	Non-Disclosure Agreements	
HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	Yes	CSP-owned	Google has established Code of Conduct training and Security and Privacy training which are required by all new hires and employees to be completed on an ongoing basis. This is further discussed in our security whitepaper: https://cloud.google.com/security/overview/whitepaper		HRS-11	Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates.	Security Awareness Training	
HRS-11.2	Are regular security awareness training updates provided?	Yes	CSP-owned	Google has processes in place for security training content reviews and refreshes annually, during which feedback from learners and partner teams are considered.					
HRS-12.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Yes	CSP-owned	Google has established a privacy and information security training program and requires all employees to complete this training upon hire and annually.		HRS-12	Provide all employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	Personal and Sensitive Data Awareness and Training	
HRS-12.2	Are all employees granted access to sensitive organizational and personal data provided with regular updates in procedures, processes, and policies relating to their professional function?	Yes	CSP-owned	Google requires all employees to retake the security and privacy awareness training on an annual basis. The content in these trainings is reviewed and updated accordingly on an annual basis.					

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
HRS-13.1	Are employees notified of their roles and responsibilities to maintain awareness and compliance with established policies, procedures, and applicable legal, statutory, or regulatory compliance obligations?	Yes	CSP-owned	Google maintains a security awareness program and has developed and documented formal policies and procedures for its personnel. This training is required by all employees upon hire and on an ongoing annual basis. Google employees are required to acknowledge the Code of Conduct and complete Google's Code of Conduct training which addresses responsibilities and expected behavior with respect to the protection of information.		HRS-13	Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.	Compliance User Responsibility	
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSP-owned	Google has identity and access management policies and procedures in place. Google restricts access based on need-to-know and job function. Google also discusses administrative access in the security whitepaper: https://cloud.google.com/security/overview/whitepaper		IAM-01	Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually.	Identity and Access Management Policy and Procedures	
IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Google has processes in place to review Security & Privacy policies annually. The policies specific to identity and access management fall under this category.					
IAM-02.1	Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSP-owned	Google maintains a strong password guidelines policy regarding the use and protection of passwords. Passwords have a minimum 8 character requirement and must meet the requirements automatically enforced such as dictionary and complexity checks.		IAM-02	Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually.	Strong Password Policy and Procedures	
IAM-02.2	Are strong password policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Google has processes in place to review Security & Privacy policies annually. The policies specific to strong password guidelines fall under this category.					
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	Yes	CSP-owned	Google maintains a central identity and authorization management system. This system automatically updates group memberships based on continuous syncs with HR data to check for changes in roles.		IAM-03	Manage, store, and review the information of system identities, and level of access.	Identity Inventory	
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	Yes	CSP-owned	Google restricts access based on need-to-know and job function, using the concept of separation of duties to match access privileges to defined responsibilities. Google also discusses administrative access in the security whitepaper: https://cloud.google.com/security/overview/whitepaper		IAM-04	Employ the separation of duties principle when implementing information system access.	Separation of Duties	
IAM-05.1	Is the least privilege principle employed when implementing information system access?	Yes	CSP-owned	Google restricts access based on need-to-know and job function, using the concept of least privilege to match access privileges to defined responsibilities. Google also discusses administrative access in the security whitepaper: https://cloud.google.com/security/overview/whitepaper		IAM-05	Employ the least privilege principle when implementing information system access.	Least Privilege	
IAM-06.1	Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	Yes	CSP-owned	Google has processes in place which define the steps of user access provisioning. For Google personnel, authorization is required prior to access being granted. Google maintains automated log collection and analysis tools. All account actions are recorded.		IAM-06	Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.	User Access Provisioning	
IAM-07.1	Is a process in place to de-provision or modify the access, in a timely manner, of movers / leavers or system identity changes, to effectively adopt and communicate identity and access management policies?	Yes	CSP-owned	Google monitors its access lists carefully to minimize the potential for unauthorized account use. Google periodically reviews access lists and removes access that is no longer required. This system automatically updates group memberships based on continuous syncs with HR data to check for changes in roles or terminations. All account actions are recorded.		IAM-07	De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner in order to effectively adopt and communicate identity and access management policies.	User Access Changes and Revocation	

CAIQ

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
IAM-08.1	Are reviews and revalidation of user access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance?	Yes	CSP-owned	Google requires access reviews at least semi-annually for critical access groups. Google maintains a central identity and authorization management system. This system automatically updates group memberships based on continuous syncs with HR data to check for changes in roles.		IAM-08	Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance.	User Access Review	Identity & Access Management
IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate?	Yes	CSP-owned	Google maintains a separation of duties matrix to document the organizational roles established within the organization. Various roles within the matrix are responsible for administrative data access, encryption, key management, and logging. Google employs the principle of least privilege, allowing only authorized access for users necessary to accomplish their job functions.		IAM-09	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and separated.	Segregation of Privileged Access Roles	
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	Yes	CSP-owned	Google's HR system automatically updates machine ACL systems based on continuous syncs with HR data to check for changes in roles. This ensures accounts with access to production are still valid and appropriate in the HR system. In addition, machine ACL system accounts with access to production and network administrator accounts are reviewed at least semi-annually.		IAM-10	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the culmination of segregated privileged access.	Management of Privileged Access Roles	
IAM-10.2	Are procedures implemented to prevent the culmination of segregated privileged access?	Yes	CSP-owned	Google maintains a separation of duties matrix to document the organizational roles established within the organization.					
IAM-11.1	Are processes and procedures for customers to participate, where applicable, in granting access for agreed, high risk as (defined by the organizational risk assessment) privileged access roles defined, implemented and evaluated?	NA	CSP-owned	Google restricts access based on need-to-know and job function.		IAM-11	Define, implement and evaluate processes and procedures for customers to participate, where applicable, in the granting of access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles.	CSCs Approval for Agreed Privileged Access Roles	
IAM-12.1	Are processes, procedures, and technical measures to ensure the logging infrastructure is "read-only" for all with write access (including privileged access roles) defined, implemented, and evaluated?	Yes	CSP-owned	Google ensures access to audit management information is restricted from unauthorized access through the use of ACLs within the log repository. Access to logging infrastructure is limited to authorized Google engineers only. Access may vary by levels and must be approved by the resource owner. Log analysts are granted read only access to log data in the repository.		IAM-12	Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures.	Safeguard Logs Integrity	
IAM-12.2	Is the ability to disable the "read-only" configuration of logging infrastructure controlled through a procedure that ensures the segregation of duties and break glass procedures?	Yes	CSP-owned	Google ensures access to audit management information is restricted from unauthorized access through the use of ACLs within the log repository based on least privilege and separation of duties and logs within the repository are read only. There is a team dedicated to enforcing appropriate access. Changes to the logging infrastructure configuration cannot be made without approval as per our change management procedures.					
IAM-13.1	Are processes, procedures, and technical measures that ensure users are identifiable through unique identification (or can associate individuals with user identification usage) defined, implemented, and evaluated?	Yes	CSP-owned	Google has processes to ensure new Google employees (including vendors, contractors, and temporary employees) are assigned a username to uniquely identify an individual. There are automated mechanisms in place during the accounts workflow to verify the uniqueness of the username.		IAM-13	Define, implement and evaluate processes, procedures and technical measures that ensure users are identifiable through unique IDs or which can associate individuals to the usage of user IDs.	Uniquely Identifiable Users	
IAM-14.1	Are processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multifactor authentication for a least-privileged user and sensitive data access defined, implemented, and evaluated?	Yes	CSP-owned	Google has processes in place which require two factor authentication and machine certificates for all employees. In addition, Google provides the capability for domain administrators to enforce Google's 2-step verification. The 2nd factor could be a code generated by Google's Authenticator application or via a supported hardware key.		IAM-14	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	Strong Authentication	
IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	Yes	CSP-owned	Google uses machine certificates to establish device identity.					

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
IAM-15.1	Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?	Yes	CSP-owned	Google has policies in place defining the secure use of passwords. In addition, passwords are cryptographically protected in storage using a salted hash and passwords are encrypted in transmission.		IAM-15	Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords.	Passwords Management	
IAM-16.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	Yes	CSP-owned	Google restricts access based on need-to-know and job function in accordance with applicable legal and compliance requirements. Google also has policies on validating and verifying identity for access to Google systems. Google provides (under NDA) customers with a SOC 2 report that includes testing of Google's access controls.		IAM-16	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.	Authorization Mechanisms	
IPY-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g., APIs)?	Yes	CSP-owned	Google makes detailed information available on the use and function of its APIs. Terms of Service for APIs are located on their respective pages.		IPY-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: a. Communications between application interfaces b. Information processing interoperability c. Application development portability d. Information/Data exchange, usage, portability, integrity, and persistence Review and update the policies and procedures at least annually.	Interoperability and Portability Policy and Procedures	Interoperability & Portability
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	Yes	CSP-owned	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. https://cloud.google.com/security/gdpr/					
IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	Yes	CSP-owned	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. https://cloud.google.com/security/gdpr/					
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	Yes	CSP-owned	Google maintains policies for data exchange, usage, portability, integrity, and persistence. https://cloud.google.com/security/gdpr/ https://cloud.google.com/terms/data-processing-terms					
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Google has processes in place to review Security & Privacy policies annually. The policies specific to interoperability and portability fall under this category.					
IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	Yes	CSP-owned	Customers do not need Google's assistance to port their data. Customers can export their data from Google Workspace using Google Takeout. https://takeout.google.com/settings/takeout Customers can export their Google Cloud Platform data in a number of industry standard formats.		IPY-02	Provide application interface(s) to CSCs so that they programmatically retrieve their data to enable interoperability and portability.	Application Interface Availability	
IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?	Yes	CSP-owned	Network traffic is encrypted using industry standard protocols.		IPY-03	Implement cryptographically secure and standardized network protocols for the management, import and export of data.	Secure Interoperability and Portability Management	
IPY-04.1	Do agreements include provisions specifying CSC data access upon contract termination, and have the following? a. Data format b. Duration data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Yes	CSP-owned	Google's Data Processing and Security Terms define deletion on termination and data export agreements. . https://cloud.google.com/terms/data-processing-terms		IPY-04	Agreements must include provisions specifying CSCs access to data upon contract termination and will include: a. Data format b. Length of time the data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Data Portability Contractual Obligations	
IVS-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Google maintains device configuration policies on security requirements for the configuration and management of devices connecting to corporate services. The policies also apply to infrastructure and virtual instances.		IVS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually.	Infrastructure and Virtualization Security Policy and Procedures	
IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Google has processes in place to review Security & Privacy policies annually. The policies specific to device configuration fall under this category.					
IVS-02.1	Is resource availability, quality, and capacity planned and monitored in a way that delivers required system performance, as determined by the business?	Yes	CSP-owned	Google maintains an effective resource economy with internal Service Level Agreements between engineering teams that provide for capacity planning and provisioning decisions. Google's external SLAs are documented here: https://cloud.google.com/terms/sla		IVS-02	Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.	Capacity and Resource Planning	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
IVS-03.1	Are communications between environments monitored?	Yes	CSP-owned	In Google's production environment, traffic is required to flow through defined proxies in order to connect to the external environment. The defined proxies are spread across internal services managed by Google's Traffic team. They have RPC policy limitations enforced and they are limited at the network edge ACLs to permit return of traffic to specific sets of ports and protocols. Google has a security whitepaper which discusses defense in depth: https://cloud.google.com/security/overview/whitepaper		IVS-03	Monitor, encrypt and restrict communications between environments to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls.	Network Security	Infrastructure & Virtualization Security
IVS-03.2	Are communications between environments encrypted?	Yes	CSP-owned	Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. Google has a security whitepaper on encryption in transit: ttps://cloud.google.com/security/encryption-in-transit/					
IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	Yes	CSP-owned	In Google's production environment, traffic is required to flow through defined proxies in order to connect to the external environment. The defined proxies are spread across internal services managed by Google's Traffic team. They have RPC policy limitations enforced and they are limited at the network edge ACLs to permit return of traffic to specific sets of ports and protocols. Google has a security whitepaper which discusses defense in depth: https://cloud.google.com/security/overview/whitepaper					
IVS-03.4	Are network configurations reviewed at least annually?	Yes	CSP-owned	Google updates the baseline configuration for network devices at least annually or when a significant change occurs.					
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	Yes	CSP-owned	In Google's production environment, traffic is required to flow through defined proxies in order to connect to the external environment. The defined proxies are spread across internal services managed by Google's Traffic team. They have RPC policy limitations enforced and they are limited at the network edge ACLs to permit return of traffic to specific sets of ports and protocols.					
IVS-04.1	Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline?	Yes	Shared CSP and CSC	Google builds its own machines and deploys custom operating system images that only permit the necessary ports, protocols, and services.	Customers are responsible for hardening their GCP instance.	IVS-04	Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline.	OS Hardening and Base Controls	
IVS-05.1	Are production and non-production environments separated?	Yes	CSP-owned	Google separates its production environment from its corporate environment.		IVS-05	Separate production and non-production environments.	Production and Non-Production Environments	
IVS-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented, segregated, monitored, and restricted from other tenants?	Yes	CSP-owned	Customer environments are logically segregated to prevent users and customers from accessing resources not assigned to them. Customer data is logically segregated by domain to allow data to be produced for a single tenant.		IVS-06	Design, develop, deploy and configure applications and infrastructures such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented and segregated, monitored and restricted from other tenants.	Segmentation and Segregation	
IVS-07.1	Are secure and encrypted communication channels including only up-to-date and approved protocols used when migrating servers, services, applications, or data to cloud environments?	Yes	Shared CSP and CSC	Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. Google has a security whitepaper on encryption in transit: https://cloud.google.com/security/encryption-in-transit/	Customers are responsible for using secure and encrypted communication channels including up to date and approved protocols when migrating servers, services, applications, or data to cloud environments within customer managed systems and networks.	IVS-07	Use secure and encrypted communication channels when migrating servers, services, applications, or data to cloud environments. Such channels must include only up-to-date and approved protocols.	Migration to Cloud Environments	
IVS-08.1	Are high-risk environments identified and documented?	NA	Shared CSP and CSC	Within Google's production environment, there are high trust environments considered to as privileged access environments and enforced by access controls.	Customers are responsible for identifying and documenting high-risk environments within customer managed instances.	IVS-08	Identify and document high-risk environments.	Network Architecture Documentation	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
IVS-09.1	Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks?	Yes	CSP-owned	Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google's intrusion detection involves: 1. Tightly controlling the size and make-up of Google's attack surface through preventative measures; 2. Employing intelligent detection controls at data entry points; and 3. Employing technologies that automatically remedy certain dangerous situations. Please review https://cloud.google.com/security/infrastructure/design/ regarding defense-in-depth techniques deployed across our infrastructure.		IVS-09	Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.	Network Defense	
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Google has policies and procedures in place for security logging requirements, rules on log data usage, and monitoring alerts. Google also discusses monitoring in the security whitepaper: https://cloud.google.com/security/overview/whitepaper		LOG-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually.	Logging and Monitoring Policy and Procedures	
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Google has processes in place to review Security & Privacy policies annually. The policies specific to security logging and monitoring processes fall under this category.					
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	Yes	Shared CSP and CSC	Google maintains an automated log collection and analysis tool to review and analyse log events. Google also maintains policies on log retention and log security requirements.	Customers are responsible for managing their own audit log security and retention within their GCP instance.	LOG-02	Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.	Audit Logs Protection	
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	Yes	CSP-owned	Google maintains a security monitoring program to detect and report security related events in our infrastructure and applications. Google discusses monitoring in the security whitepaper: https://cloud.google.com/security/overview/whitepaper		LOG-03	Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.	Security Monitoring and Alerting	
LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?	Yes	CSP-owned	Google uses a proprietary event management tool to identify and alert on unauthorized use of the information system and assets and takes timely appropriate action when unauthorized use is detected.					
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	Yes	CSP-owned	Google restricts physical and logical access to audit logs to authorized users only through the use of access control lists within the logging system.		LOG-04	Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability.	Audit Logs Access and Accountability	
LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	Yes	CSP-owned	Google uses a proprietary event management tool to identify and alert on atypical activity and takes timely appropriate action when unauthorized use is detected.		LOG-05	Monitor security audit logs to detect activity outside of typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies.	Audit Logs Monitoring and Response	
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Yes	CSP-owned	Google uses a proprietary event management tool to identify and alert on atypical activity and takes timely appropriate action when unauthorized use is detected.					
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Yes	CSP-owned	Google uses a synchronized time-service protocol to ensure all systems have a common time reference. Google makes their NTP protocol public as well for use by customers. https://developers.google.com/time/		LOG-06	Use a reliable time source across all relevant information processing systems.	Clock Synchronization	
LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?	Yes	CSP-owned	Google has policies and procedures in place for security logging requirements and rules on log data usage. These policies include metadata.					

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment?	Yes	CSP-owned	Google has processes in place to review Security & Privacy policies annually. The policies specific to security logging processes (which include defining the scope of the policy) fall under this category. Google discusses monitoring in the security whitepaper: https://cloud.google.com/security/overview/whitepaper		LOG-07	Establish, document and implement which information meta/data system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment.	Logging Scope	Logging and Monitoring
LOG-08.1	Are audit records generated, and do they contain relevant security information?	Yes	CSP-owned	Google maintains an automated log collection and analysis tool to review and analyse log events. Google's log requirements policy defines the minimum content required for log records.		LOG-08	Generate audit records containing relevant security information.	Log Records	
LOG-09.1	Does the information system protect audit records from unauthorized access, modification, and deletion?	Yes	CSP-owned	Google restricts physical and logical access to audit logs to authorized users only through the use of access control lists within the logging system. Audit information is protected from unauthorized modification and deletion through the use of checksums.		LOG-09	The information system protects audit records from unauthorized access, modification, and deletion.	Log Protection	
LOG-10.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	Yes	CSP-owned	Google maintains documentation for the use of its internal proprietary key management service. Google also has automated mechanisms in place for monitoring the key management server for modifications. Google also has whitepapers on encryption: Encryption at rest: https://cloud.google.com/security/encryption/default-encryption Encryption in transit: https://cloud.google.com/security/encryption-in-transit		LOG-10	Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls.	Encryption Monitoring and Reporting	
LOG-11.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	Yes	CSP-owned	Google maintains documentation on its key management process and provides controls to manage encryption keys through their lifecycle and protect against unauthorized use.		LOG-11	Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys.	Transaction/Activity Logging	
LOG-12.1	Is physical access logged and monitored using an auditable access control system?	Yes	CSP-owned	Google logs all physical access of its data center employees within its access control system. Data centers are monitored 24/7 by video cameras. Google discusses data center physical security in its security whitepaper: https://cloud.google.com/security/overview/whitepaper		LOG-12	Monitor and log physical access using an auditable access control system.	Access Control Logs	
LOG-13.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	Yes	CSP-owned	Google uses a proprietary event management tool to identify and alert on atypical activity and takes timely appropriate action when unauthorized use is detected.		LOG-13	Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party.	Failures and Anomalies Reporting	
LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	Yes	CSP-owned	Google has processes in place to perform alerting to relevant teams in the event manual intervention is required.					
SEF-01.1	Are policies and procedures for security incident management, e-discovery, and cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Google maintains incident response procedures to help ensure prompt notification and investigation of incidents. This includes the use of forensics in the resolution process. Google also has a data incident response whitepaper: https://cloud.google.com/security/incident-response		SEF-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and update the policies and procedures at least annually.	Security Incident Management Policy and Procedures	
SEF-01.2	Are policies and procedures reviewed and updated annually?	Yes	CSP-owned	Google has processes in place to review Security & Privacy policies annually. The policies for incident response fall under this category.					
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Google maintains incident response procedures to help ensure prompt notification and investigation of incidents. These procedures include guidelines on prioritization based on severity. Google also has a data incident response whitepaper: https://cloud.google.com/security/incident-response		SEF-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies and procedures at least annually.	Service Management Policy and Procedures	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually?	Yes	CSP-owned	Google has processes in place to review Security & Privacy policies annually. The policies for incident response (which include prioritization and timely management of incidents) fall under this category.					
SEF-03.1	Is a security incident response plan that includes relevant internal departments, impacted CSCs, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Google maintains incident response procedures to help ensure prompt notification and investigation of incidents. These procedures include roles and responsibilites along with stakeholders who may be impacted. Google also has a data incident response whitepaper: https://cloud.google.com/security/incident-response		SEF-03	Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: relevant internal departments, impacted CSCs, and other business critical relationships (such as supply-chain) that may be impacted.	Incident Response Plans	
SEF-04.1	Is the security incident response plan tested and updated for effectiveness, as necessary, at planned intervals or upon significant organizational or environmental changes?	Yes	CSP-owned	Google performs annual testing of its emergency response processes. In addition, the existence and operating effectiveness of the incident response plans, is verified as part of our SOC 2 report.		SEF-04	Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness.	Incident Response Testing	Security Incident Management, E-Discovery, & Cloud Forensics
SEF-05.1	Are information security incident metrics established and monitored?	Yes	CSP-owned	Google reviews and analyzes security incidents to determine impact, cause, and opportunities for corrective action.		SEF-05	Establish and monitor information security incident metrics.	Incident Response Metrics	
SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	Yes	CSP-owned	Google maintains processes for the Incident Management team to triage identified risks or security events/incidents.		SEF-06	Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events.	Event Triage Processes	
SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	Yes	CSP-owned	Google will respect the contractually agreed terms for customers in regards to incident notification. GCP: https://cloud.google.com/terms/data-processing-terms Workspace: https://workspace.google.com/terms/dpa_terms.html Google also has a data incident response whitepaper: https://cloud.google.com/security/incident-response		SEF-07	Define and implement, processes, procedures and technical measures for security breach notifications. Report security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations.	Security Breach Notification	
SEF-07.2	Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	Yes	CSP-owned	Google will respect the contractually agreed terms for customers in regards to incident notification. GCP: https://cloud.google.com/terms/data-processing-terms Workspace: https://workspace.google.com/terms/dpa_terms.html Google also has a data incident response whitepaper: https://cloud.google.com/security/incident-response					
SEF-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Yes	CSP-owned	Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents.		SEF-08	Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.	Points of Contact Maintenance	
STA-01.1	Are policies and procedures implementing the shared security responsibility model (SSRM) within the organization established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Google's policies and procedures establish the CSP's control ownership and responsibilities as it relates to the service offerings. Google provides its customers with information on subprocessors and outlines Google responsibilities/customer responsibilities in the Data Processing and Security Terms: https://cloud.google.com/terms/data-processing-terms		STA-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organization. Review and update the policies and procedures at least annually.	SSRM Policy and Procedures	
STA-01.2	Are the policies and procedures that apply the SSRM reviewed and updated annually?	Yes	CSP-owned	Google has processes to review policies and procedures related to the CSP's control ownership and responsibilities as it related to the service offerings on an annual basis.					

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	Yes	CSP-owned	Google's policies and procedures establish the CSP's control ownership and responsibilities as it relates to the service offerings. Google requires its subprocessors to sign the Subprocessor Data Processing Agreement which include their responsibilities to the data. More information on subprocessor security can be found here: https://cloud.google.com/terms/data-processing-terms		STA-02	Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering.	SSRM Supply Chain	
STA-03.1	Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	Yes	CSP-owned	Google provides its customers with information on subprocessors and outlines Google responsibilities/customer responsibilities in the Data Processing and Security Terms: https://cloud.google.com/terms/data-processing-terms Additionally, the public subprocessor listing provides guidance on the functions performed: Google Cloud Platform: https://cloud.google.com/terms/subprocessors Google Workspace: https://workspace.google.com/intl/en/terms/subprocessors.html Google also provides SRM relative to the following frameworks: PCI, HIPAA, and FedRamp.		STA-03	Provide SSRM Guidance to the CSC detailing information about the SSRM applicability throughout the supply chain.	SSRM Guidance	
STA-04.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering?	Yes	CSP-owned	Google's CAIQ v4 includes shared ownership information of all CSA CCM controls.		STA-04	Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering.	SSRM Control Ownership	
STA-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	Yes	CSP-owned	Google's CAIQ v4 goes through a review and validation process by appropriate internal teams before being made available to customers.		STA-05	Review and validate SSRM documentation for all cloud services offerings the organization uses.	SSRM Documentation Review	
STA-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	Yes	CSP-owned	Google undergoes periodic external audits for CSA STAR to test the efficiency and effectiveness of implemented security controls.		STA-06	Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for.	SSRM Control Implementation	
STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	Yes	CSP-owned	For Google Cloud, Google maintains public subprocessor lists for review. The lists are updated when subprocessors are added, modified, or removed. Google Cloud Platform: https://cloud.google.com/terms/subprocessors Google Workspace: https://workspace.google.com/intl/en/terms/subprocessors.html		STA-07	Develop and maintain an inventory of all supply chain relationships.	Supply Chain Inventory	Supply Chain Management, Transparency, and Accountability
STA-08.1	Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs?	Yes	CSP-owned	For Google Cloud, Google employs a vendor management process that includes contractual requirements and periodic review of vendors to ensure adherence to Google's requirements.		STA-08	CSPs periodically review risk factors associated with all organizations within their supply chain.	Supply Chain Risk Management	
STA-09.1	Do service agreements between CSPs and CSCs (tenants) incorporate at least the following mutually agreed upon provisions and/or terms? • Scope, characteristics, and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third-party assessment • Service termination • Interoperability and portability requirements • Data privacy	Yes	CSP-owned	Google maintains a directory with links to the Terms of Service and policies. This directory contains scope, characteristics, and location of business relationship and services, service termination, change management process, information security requirements (including customer responsibilities), right to audit and third party assessment, incident management and communication procedure, logging and monitoring capability, data export, and data privacy. . https://cloud.google.com/product-terms		STA-09	Service agreements between CSPs and CSCs (tenants) must incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope, characteristics and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third party assessment • Service termination • Interoperability and portability requirements • Data privacy	Primary Service and Contractual Agreement	
STA-10.1	Are supply chain agreements between CSPs and CSCs reviewed at least annually?	NA	CSP-owned	Google does not have supply chain agreements between us and customers. Google Cloud does maintain Service Level Agreements which can be found here: https://cloud.google.com/terms		STA-10	Review supply chain agreements between CSPs and CSCs at least annually.	Supply Chain Agreement Review	

CAIQ

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
STA-11.1	Is there a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities?	Yes	CSP-owned	Google maintains an internal program to assess ongoing conformance with relevant standards, policies, processes, and metrics. Google also maintains and implements comprehensive internal and external audit plans that are performed at least annually to test the efficiency and effectiveness of implemented security controls against recognized standards.		STA-11	Define and implement a process for conducting internal assessments to confirm conformance and effectiveness of standards, policies, procedures, and service level agreement activities at least annually.	Internal Compliance Testing	
STA-12.1	Are policies that require all supply chain CSPs to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented?	Yes	CSP-owned	Google has implemented data protection agreements required to be signed by supply chain CSPs to comply with privacy, security, access control, audit, personnel policy, SLA, and confidentiality commitments. Google vendor managers also perform quarterly performance reviews based on the agreements outlined in the vendor's service agreements.		STA-12	Implement policies requiring all CSPs throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy and service level requirements and standards.	Supply Chain Service Agreement Compliance	
STA-13.1	Are supply chain partner IT governance policies and procedures reviewed periodically?	Yes	CSP-owned	Google maintains an internal program to assess ongoing conformance with relevant policies and procedures. Google reviews and updates vendor IT governance policies and procedures as needed. Google also has its Data Processing and Security Terms for Partners: https://cloud.google.com/terms/data-processing-terms/partner		STA-13	Periodically review the organization's supply chain partners' IT governance policies and procedures.	Supply Chain Governance Review	
STA-14.1	Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented?	Yes	CSP-owned	Google has a well defined vendor management policy and process to select and monitor third party providers. Google has a dedicated team to conduct ongoing audits of subprocessors for compliance. Google conducts annual reviews and audits of its subprocessors to validate adherence with Google's security requirements to ensure they provide a level of privacy and security appropriate to their access to data and the scope of the services.		STA-14	Define and implement a process for conducting security assessments periodically for all organizations within the supply chain.	Supply Chain Data Security Assessment	
TVM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities to protect systems against vulnerability exploitation?	Yes	CSP-owned	Google's Vulnerability Priority Guidelines define how security vulnerability remediation timelines and prioritizations are based on level of risk. Google also provides ways to report vulnerabilities at: https://www.google.com/about/appsecurity/		TVM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually.	Threat and Vulnerability Management Policy and Procedures	
TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Google has processes in place to review Security & Privacy policies annually. The policies specific to vulnerability management fall under this category.					
TVM-02.1	Are policies and procedures to protect against malware on managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Google has policies and processes in place to protect against malware on managed assets. Malware prevention is further discussed in our security whitepaper: https://cloud.google.com/security/overview/whitepaper		TVM-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware on managed assets. Review and update the policies and procedures at least annually.	Malware Protection Policy and Procedures	
TVM-02.2	Are asset management and malware protection policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Google has processes in place to review Security & Privacy policies annually. The policies specific to asset management and malware protection fall under this category.					
TVM-03.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications (based on the identified risk)?	Yes	CSP-owned	Google's Vulnerability Priority Guidelines define response times and resolution expectations based on the vulnerability priority, including how high priority vulnerability remediations should be handled.		TVM-03	Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk.	Vulnerability Remediation Schedule	
TVM-04.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?	Yes	CSP-owned	Google's threat detection systems are continuously updated, at least weekly, based on attack signatures as new signatures are identified.		TVM-04	Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis.	Detection Updates	
TVM-05.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to identify updates for applications that use third-party or open-source libraries (according to the organization's vulnerability management policy)?	Yes	CSP-owned	Google has policies in place which define the technical and legal requirements for using third-party or open source libraries. This includes the guidelines around maintaining the libraries with newer versions and applying security patches in a timely manner.		TVM-05	Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy.	External Library Vulnerabilities	

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?	Yes	Shared CSP and CSC	Google coordinates external 3rd party penetration testing using qualified and certified penetration testers at least annually.	Customers are responsible for conducting penetration testing on their GCP instance.	TVM-06	Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties.	Penetration Testing	Threat & Vulnerability Management
TVM-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	Yes	Shared CSP and CSC	Google's vulnerability management process actively scans for security threats using a combination of commercially available and purpose-built in-house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. Monthly infrastructure and web application scans are performed. Vulnerability management is described in the security whitepaper: https://cloud.google.com/security/overview/whitepaper#vulnerability_management	Customers are responsible for implementing vulnerability detection on their GCP instance.	TVM-07	Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly.	Vulnerability Identification	
TVM-08.1	Is vulnerability remediation prioritized using a risk-based model from an industry-recognized framework?	Yes	Shared CSP and CSC	Google's Vulnerability Priority Guidelines define how security vulnerability remediation timelines and prioritizations are based on level of risk. Google uses the most up to date version of CVSS to determine reporting severity.	Customers are responsible for remediation of vulnerabilities identified within their GCP instance.	TVM-08	Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework.	Vulnerability Prioritization	
TVM-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	Yes	CSP-owned	Google's Vulnerability Management Program and Vulnerability Priority Guidelines define how to track vulnerabilities including identification and remediation updates with the responsible teams. External researchers are encouraged to submit identified risks via our Vulnerability Rewards Program. In addition, Google updates its security bulletin with new vulnerabilities as needed: https://cloud.google.com/support/bulletins Google also discusses its Vulnerability Reward Program and vulnerability management in the security whitepaper: https://cloud.google.com/security/overview/whitepaper		TVM-09	Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.	Vulnerability Management Reporting	
TVM-10.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	Yes	CSP-owned	Google has Vulnerability Priority Guidelines in place which establish timelines and procedures for responding to vulnerability reports in addition to assigning priorities based on the vulnerability. Through Google's Vulnerability Management Program, metrics are monitored and reported via internal dashboards.		TVM-10	Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals.	Vulnerability Management Metrics	
UEM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	Yes	CSP-owned	Google has policies and procedures in place for security requirements of Google owned and managed endpoints.		UEM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually.	Endpoint Devices Policy and Procedures	
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Google has processes in place to review Security & Privacy policies annually. The policies specific to endpoint management fall under this category.					
UEM-02.1	Is there a defined, documented, applicable and evaluated list containing approved services, applications, and the sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data?	Yes	CSP-owned	Google maintains an internal software solution with the approved list of applications that can be installed on managed endpoints based on OS. For Android and iOS, Google Device Policy restricts the user and device behavior on mobile devices including application installation. For advanced use, a work profile is required which includes a restricted apps store.		UEM-02	Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data.	Application and Service Approval	
UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	Yes	CSP-owned	Mobile operability is is part of our standard software engineering development lifecycle.		UEM-03	Define and implement a process for the validation of the endpoint device's compatibility with operating systems and applications.	Compatibility	
UEM-04.1	Is an inventory of all endpoints used and maintained to store and access company data?	Yes	CSP-owned	Google maintains a centralized inventory system for all managed endpoints which ingests data from various inventory systems to prevent duplicates.		UEM-04	Maintain an inventory of all endpoints used to store and access company data.	Endpoint Inventory	
UEM-05.1	Are processes, procedures, and technical measures defined, implemented and evaluated, to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data?	Yes	CSP-owned	Google has implemented technical measures in which all devices must have a trust tier designation. Each trust tier allows varying levels of access to corporate systems.		UEM-05	Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data.	Endpoint Management	

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1
Google Cloud (September 2021)

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	Yes	CSP-owned	Google's Device Configuration Guidelines requires that all devices must implement an automatic screen lock after a pre-defined period of time.		UEM-06	Configure all relevant interactive-use endpoints to require an automatic lock screen.	Automatic Lock Screen	Universal Endpoint Management
UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	Yes	CSP-owned	Google's endpoint devices are continuously patched through system management software as patches become available, which varies by OS and applications. Google's Device Policy Manager requires personnel to keep devices up to date with patches and requires a minimum O/S level. For OS updates, these are pushed to end devices once the vendor releases it and endpoint teams test and approve it.		UEM-07	Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes.	Operating Systems	
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	Yes	CSP-owned	Google requires all managed endpoints to be encrypted during the initial setup process and remain encrypted throughout the device's lifecycle. iOS and Android devices also require encryption in order to sync a corporate account to it.		UEM-08	Protect information from unauthorized disclosure on managed endpoint devices with storage encryption.	Storage Encryption	
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	Yes	CSP-owned	Google has mechanisms in which corporate issued machines have antivirus software preinstalled to help prevent, detect, and remove malware, depending on the OS.		UEM-09	Configure managed endpoints with anti-malware detection and prevention technology and services.	Anti-Malware Detection and Prevention	
UEM-10.1	Are software firewalls configured on managed endpoints?	Yes	CSP-owned	Google has mechanisms in which all Google managed Mac, Windows, and Linux computers have personal firewalls enabled and managed by an internal team. For CrOS devices, the functionality offered by personal firewalls is already built in.		UEM-10	Configure managed endpoints with properly configured software firewalls.	Software Firewall	
UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	Yes	CSP-owned	Google leverages the Google Workspace DLP functionalities; https://support.google.com/a/topic/7556687?hl=en&ref_topic=7558840		UEM-11	Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment.	Data Loss Prevention	
UEM-12.1	Are remote geolocation capabilities enabled for all managed mobile endpoints?	Yes	CSP-owned	Google has mechanisms in place to provide recent physical locations for employees based on corporate activity logs. This system is used for location based access restrictions.		UEM-12	Enable remote geo-location capabilities for all managed mobile endpoints.	Remote Locate	
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	Yes	CSP-owned	Google has policies and procedures in place for mobile device security guidelines which state Google reserves the right to remotely wipe mobile devices. Google also has technical implementations in place which require remote wipe capabilities for all mobile devices managed by Google. In addition to remote wipe capabilities, Google uses strong encryption modules on all highly privileged access mobile devices.		UEM-13	Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.	Remote Wipe	
UEM-14.1	Are processes, procedures, and technical and/or contractual measures defined, implemented, and evaluated to maintain proper security of third-party endpoints with access to organizational assets?	Yes	CSP-owned	Google maintains a personal computer policy and provides detailed instructions to personnel that wish to provision access to Google corporate services on their Android, iOS, or ChromeOS devices if the devices are managed by Google. The policy includes eligibility requirements and security policy requirements.		UEM-14	Define, implement and evaluate processes, procedures and technical and/or contractual measures to maintain proper security of third-party endpoints with access to organizational assets.	Third-Party Endpoint Security Posture	