Google Cloud

Last updated October 2022

Background information	Google Commentary
BAIT No. 3 Clause 3.1 Information processing and dissemination in business and service processes is supported by data-processing IT systems and associated IT processes. The scope and quality of these must be based in particular on internal operational requirements, business activities and the risk situation (see AT 7.2 para. 1 MaRisk). IT systems, the associated IT processes and other components of the information network must ensure the integrity, availability, authenticity and confidentiality of the data (see AT 7.2 para. 2 MaRisk). The institution must define and coordinate the tasks, competencies, responsibilities, controls and communication channels associated with the management of information risks (see AT 4.3.1 para. 2 MaRisk). To this end, the institution shall establish appropriate monitoring and control processes (cf. AT 7.2 para. 4 MaRisk) and define related reporting obligations (cf. BT 3.2 para. 1 MaRisk).	The Infrastructure Security Overview whitepaper provides an overview of how security is designed into Google's technical infrastructure. It is intended for security executives, security architects, and auditors. Google maintains a robust and up-to-date Information Security Management System (ISMS) 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. Google performs risk assessments as required to support its ISMS. Google takes into account regulatory, legal, statutory or location restrictions of data, including data retention, classification and protection, in its risk assessments. Google has demonstrated adherence to this control by way of ISO/IEC 27001, ISO/IEC 27018 certification, as well as the annual external third party audits conducted for SOC 2/3 compliance. Information Security policies and procedures are communicated to all internal employees that must undergo and attest to yearly training. Google provides customers (under NDA) a copy of the SOC 2/3 report that demonstrates compliance with these controls. Please note in particular the following sections of the SOC 2+ CSA Star Type II Report outlining the control design: - Section III/C. ¨Policies¨ for description of design of Google´s risk management - Section III/D. ¨"Communication to ensure operating performance & controls" - Section III/E. ¨Control Processes - Section III/F. ¨Monitoring¨ For control effectiveness please refer to the Section ¨Controls, Criteria, Tests and Results of Tests¨. Please also note that the SOC 2+ CSA Star Type II Report provides a mapping to the Cloud Control Matrix (CCM) criteria. Google provides customers (under NDA) a copy of i.a. the SOC 2+ CSA Star Type II Report via the Compliance Reports Manager that demonstrates compliance with these controls.

BAIT No. 3 Clause 3.2 The components of a system for managing information risks shall be implemented with the involvement of all relevant bodies and functions in a competent manner and free of conflicts of interest.	At the higested level, Alphabet has board committees responsible for the governance of the organization. Please see our Investor Relations page for more information. When it comes to risk management, Google follows a 3 lines of defense principle to make sure risks are managed appropriately across the organization and are free of conflicts of interests. Google has documented its risk management procedures as part of its ISMS that underlies our ISO/IEC 27001 certification. Google provides customers (under NDA) a copy of i.a. the SOC 2+ CSA Star Type II Report via the Compliance Reports Manager that demonstrates compliance with these controls. Please note in particular the following sections of the SOC 2+ CSA Star Type II Report outlining the control design: - Section III/C. ¨Policies¨ for description of design of Google´s risk management For control effectiveness please refer to the Section ¨Controls, Criteria, Tests and Results of Tests¨. Please also note that the SOC 2+ CSA Star Type II Report provides a mapping to the Cloud Control Matrix (CCM) criteria.

BAIT No. 3 Clause 3.3 The institution shall have an up-to-date overview of the components of the defined information network as well as their interdependencies and interfaces. In this regard, the institution should be guided in particular by internal operational requirements, business activities and the risk situation.	Google maintains a centralized inventory system for all managed endpoints which ingests data from various inventory systems to prevent duplicates. This is covered in greater detail in Section 10 ¨System Environment and Inventory¨ of the FedRAMP SSP. Google provides customers (under NDA) a copy of i.a. the FedRAMP SSP via the Compliance Reports Manager that demonstrates compliance with these controls. Google utilizes barcodes and asset tags to track the status and location of data center equipment from acquisition to installation, retirement, and destruction. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. Google hard drives leverage technologies, like Full Disk Encryption (FDE) and drive locking, to protect data at rest. Personally Identifiable Information (PII) on removable media leaving Google facilities is approved and encrypted.
BAIT No. 3 Clause 3.4 The protection needs assessment and the associated documentation must be reviewed by information risk management.	Google executive management reviews and approves all information security policies and sets applicable commitment and direction to achieve the agreed upon Information Security goals. Google reviews its security policies at least annually. Google's cross functional security policy team meets periodically throughout the year to address emerging issues and risks and issue new or amend existing policies or guidelines, as needed. Google performs risk assessments as required by ISO/IEC 27001. Google has documented its risk management procedures as part of its ISMS that underlies our ISO/IEC 27001 certification. Documentation is made available to all individuals that may participate in or need to be informed of risk management and assessment programs.

BAIT No. 3 Clause 3.5 The owner of the information is responsible for determining the need for protection.	Google executive management reviews and approves all information security policies and sets applicable commitment and direction to achieve the agreed upon Information Security goals. Google reviews its security policies at least annually. Google's cross functional security policy team meets periodically throughout the year to address emerging issues and risks and issue new or amend existing policies or guidelines, as needed. Google performs risk assessments as required by ISO/IEC 27001. Google has documented its risk management procedures as part of its ISMS that underlies our ISO/IEC 27001 certification. Documentation is made available to all individuals that may participate in or need to be informed of risk management and assessment programs. Please note in particular the following sections of the SOC2 + CSA Star Type II Report outlining the control design: - Section III/E. ¨Procedures / Storage Media Security¨ For control effectiveness please refer to the Section ¨Controls, Criteria, Tests and Results of Tests¨. Please also note that the SOC 2+ CSA Star Type II Report provides a mapping to the Cloud Control Matrix (CCM) criteria. Google provides customers (under NDA) a copy of i.a. the SOC 2+ CSA Star Type II Report via the Compliance Reports Manager that demonstrates compliance with these controls.

BAIT No. 3 Clause 3.6 The institution shall define requirements that are appropriate for achieving the respective protection requirement and document them in a suitable form (catalog of target measures).	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. 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. Please note in particular the following sections of the SOC 2+ CSA Star Type II Report outlining the control design: - Section III/C. ¨Policies / Risk Management¨ For control effectiveness please refer to the Section ¨Controls, Criteria, Tests and Results of Tests¨. Please also note that the SOC 2+ CSA Star Type II Report provides a mapping to the Cloud Control Matrix (CCM) criteria. Google provides customers (under NDA) a copy of i.a. the SOC 2+ CSA Star Type II Report via the Compliance Reports Manager that demonstrates compliance with these controls.

BAIT No. 3 Clause 3.7 The institution must perform a comparison of the target measures with the respective effectively implemented measures (the actual state) on the basis of the defined risk criteria.	Google has documented its risk management procedures as part of its ISMS that underlies our ISO/IEC 27001 certification. 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. 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. 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 on our Service Level Agreements web page. Google's highly available solution is discussed in the security whitepaper. Please note in particular the following of the C5:2021 report: - Section 4, Section 6.1 ¨Organization of Informtation Security¨ (OIS) - Section 4, Section 6.14 ¨Business Continuity Management¨ (BCM) - Section 4, Section 6.15 ¨Compliance¨ (COM) Google provides customers (under NDA) a copy of i.a. the C5:2021 report via the Compliance Reports Manager that demonstrates compliance with these controls.

BAIT No. 3 Clause 3.8 Other risk-reducing measures due to incompletely implemented target measures must be effectively coordinated, documented, monitored and controlled.	Google's independent audit and assurance assessments are performed according to the risk environment across the organization to enable effective risk management.
BAIT No. 3 Clause 3.9 Information risk management shall coordinate and monitor the risk analysis and transfer its results to the operational risk management process. The treatment of risks is to be approved in accordance with competencies.	Google has documented its risk management procedures as part of its ISMS that underlies our ISO/IEC 27001 certification. Additionally, the FedRamp report in Section RA-3 outlines the Security Assessment Report and the System Security Plan. Google provides customers (under NDA) a copy of i.a. the ISO/IEC 27001 certification via the Compliance Reports Manager and the FedRamp Report (please contact sales contact) that demonstrates compliance with these controls.

BAIT No. 3 Clause 3.10 The institution shall keep itself informed about threats to its information network, review their relevance, assess their impact and, if necessary, take appropriate technical and organizational measures.	The Threat Analysis Group at Google monitors threat actors and the evolution of their tactics and techniques. The goals of this group are to help improve the safety and security of Google products and share this intelligence for the benefit of the online community. For Google Cloud, you can use Google Cloud Threat Intelligence for Chronicle and VirusTotal to monitor and respond to many types of malware. Google Cloud Threat Intelligence for Chronicle is a team of threat researchers who develop threat intelligence for use with Chronicle. VirusTotal is a malware database and visualization solution that you can use to better understand how malware operates within your enterprise. 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. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Monthly infrastructure and web application scans are performed. Google conducts 3rd party security penetration tests on a regular basis.
BAIT No. 3 Clause 3.11 The management shall be informed regularly, but at least quarterly, in particular about the results of the risk analysis as well as changes in the risk situation.	Google has multiple levels of risk management reviews happening at the continuous basis. Google's 3 lines of defense perform their respective continous risk analysis, inform the risk to management and changes the risk situation based upon risk identified. We have risk management teams embedded in product groups, compliance organizations, risk management organizations and internal audit organizations to create the awareness at the management level. Customer is informed by risk analysis via multiple avenues: - We share our attestation reports with the customers - We perform regular workshops, briefings and QBRs with the customers
BAIT No. 4 Clause 4.1 Information security management specifies information security requirements, defines processes and manages their implementation (see AT 7.2 para. 2 MaRisk). Information security management follows an ongoing process comprising the phases of planning, implementation, performance review, and optimization and improvement. The content of the information security officer's reporting duties to the management and the reporting cycle are based on BT 3.2. para. 1 MaRisk.	Google executive management reviews and approves all information security policies and sets applicable commitment and direction to achieve the agreed upon Information Security goals. Also Google reviews its Information Security Management System documentation annually as part of its required due diligence and it is ISO/IEC 27001 - Compliant. Please note in particular the following of the C5:2021 report: - Section 4, Section 6.1 ¨Organization of Informtation Security (OIS) Google provides customers (under NDA) a copy of i.a. the C5:2021 report via the Compliance Reports Manager that demonstrates compliance with these controls.

BAIT No. 4 Clause 4.2 The management shall adopt an information security guideline and communicate it within the institution. The information security guideline shall be consistent with the strategies of the institution. The guideline shall be reviewed in the event of significant changes in the framework conditions and adjusted promptly if necessary.	Google has a well established information security organization with well-defined roles and responsibilities, managed by an executive who is dedicated to Security and Privacy, is independent of Information Technology responsibility, and may escalate to the board level concerning security issues. Google Cloud operates at a scale where a singled named Information Security Manager is insufficient. Instead we operate a dedicated Cloud CISO (chief information security officer) office, which has a named Leader. Information Security policies and procedures are communicated to all internal employees that must undergo and attest to yearly training. Please note in particular the following of the C5:2021 report: - Section 3 ¨Description of the Internal Control System[...] / Procedures¨ Google provides customers (under NDA) a copy of i.a. the C5:2021 report via the Compliance Reports Manager that demonstrates compliance with these controls.
BAIT No. 4 Clause 4.3 Based on the information security guideline, concretizing information security guidelines and information security processes that take into account the state of the art are to be defined with the sub-processes identification, protection, detection, response and recovery.	Google employs security and privacy professionals, who are part of our software engineering and operations division. Our team includes some of the world's foremost experts in information, application and network security. This team is tasked with maintaining the company's defense systems, developing security review processes, building security infrastructure and implementing Google's security policies. Google's dedicated security team actively scans for security threats using commercial and custom tools, penetration tests, quality assurance (QA) measures and software security reviews. Within Google, members of the information security team review security plans for all networks, systems and services. They provide project-specific consulting services to Google's product and engineering teams. They monitor for suspicious activity on Google's networks, address information security threats, perform routine security evaluations and audits, and engage outside experts to conduct regular security assessments. We specifically built a full-time team, known as Project Zero, that aims to prevent targeted attacks by reporting bugs to software vendors and filing them in an external database. The security team also takes part in research and outreach activities to protect the wider community of Internet users, beyond just those who choose Google solutions. Some examples of this research would be the discovery of the POODLE SSL 3.0 exploit and cipher suite weaknesses. The security team also publishes security research papers, available to the public. The security team also organizes and participates in open-source projects and academic conferences.
BAIT No. 4 Clause 4.4 The management shall establish the function of information security officer. This function shall include responsibility for the performance of all information security matters within the Institute and vis-à-vis third parties. It shall ensure that the objectives and measures set out in the IT strategy, the information security guideline and the information security guidelines of the institute with regard to information security are made transparent both internally and vis-à-vis third parties, and that compliance with these objectives and measures is reviewed and monitored on a regular and ad hoc	Google has a well established information security organization with well-defined roles and responsibilities, managed by an executive who is dedicated to Security and Privacy, is independent of Information Technology responsibility, and may escalate to the board level concerning security issues.

BAIT No. 4 Clause 4.5 The function of the information security officer must be independent in terms of organization and processes in order to avoid potential conflicts of interest.	Google has a well established information security organization with well-defined roles and responsibilities, managed by an executive who is dedicated to Security and Privacy, is independent of Information Technology responsibility, and may escalate to the board level concerning security issues.
BAIT No. 4 Clause 4.6 Each institution shall, as a matter of principle, maintain the function of information security officer in-house. BAIT No. 4 Para. 4.6 Comment With regard to regionally active institutions (in particular those belonging to an association) as well as small institutions (in particular those belonging to a group) without significant in-house IT with a similar business model and joint IT service providers for the handling of banking processes, it is	Google has a well established information security organization with well-defined roles and responsibilities, managed by an executive who is dedicated to Security and Privacy, is independent of Information Technology responsibility, and may escalate to the board level concerning security issues.
BAIT No. 4 Clause 4.7 After an information security incident, the effects on information security must be analyzed promptly and appropriate follow-up measures must be initiated.	Google's incident response program is managed by teams of expert incident responders across many specialized functions to ensure each response is well-tailored to the challenges presented by each incident. Depending on the nature of the incident, the professional response team may include: Cloud incident management, Product engineering, Site reliability engineering, Cloud security and privacy, Digital forensics, Global, investigations, Signals detection, Security, privacy, and product counsel, Trust and safety, Counter abuse technology and Customer support. Subject matter experts from these teams are engaged in a variety of ways. Every data incident is unique, and the goal of the data incident response process is to protect customers' data, restore normal service as quickly as possible, and meet both regulatory and contractual compliance requirements. Google's incident response program has the following process: Identification, Coordination, Resolution, Closure. Google will notify customers promptly and without undue delay after becoming aware of a Data Incident, and promptly take reasonable steps to minimize harm and secure Customer Data. Following the successful remediation and resolution of a data incident, the incident response team evaluates the lessons learned from the incident. When the incident raises critical issues, the incident commander may initiate a post-mortem analysis. During this process, the incident
BAIT No. 4 Clause 4.8 The institution shall implement a policy on testing and reviewing the information security protection measures and review them regularly and on an ad hoc basis and adjust them as necessary. BAIT No. 4 Clause 4.8 Comment. The guideline shall take into account, among other things: - the general threat situation - the individual risk situation of the institution	Yes. Google reviews its ISMS documentation annually as part of its required due diligence. 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. Please note in particular the following of the C5:2021 report: - Section 4, Section 6.1 ¨Organization of Informtation Security (OIS)

BAIT No. 4 Clause 4.9 The institution shall establish a continuous and appropriate information security awareness and training program. The success of the defined awareness and training measures shall be reviewed. BAIT No. 4 Clause 4.9 Comment: The program should address at least the following aspects in a target group-oriented manner: - personal responsibility for one's own actions and omissions as well as general responsibilities for protecting information - basic information security procedures (such as reporting of information security incidents) and generally applicable security measures (e.g., on passwords, social engineering, prevention from malware, and what to do if malware is suspected).	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. Additional information is also available in the C5:2021 report: - Section 4, Section 6.3 ¨Personnel (HR)¨ Google provides customers (under NDA) a copy of i.a. the C5:2021 report via the Compliance Reports Manager that demonstrates compliance with these controls.
BAIT No. 4 Clause 4.10 The information security officer shall report to the management regularly, at least quarterly, on the status of information security and on an ad hoc basis.	Information security is managed by an executive who is dedicated to Security and Privacy, is independent of Information Technology responsibility, and may escalate to the board level concerning security issues. 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.
BAIT No. 5 Clause 5.1 Operational information security implements the requirements of information security management. IT systems, the associated IT processes and other components of the information group must ensure the integrity, availability, authenticity and confidentiality of the data. For these purposes, the design of the IT systems and the associated IT processes must be based on common standards (see AT 7.2 para. 2 MaRisk). Appropriate monitoring and management processes must be established for IT risks, including in particular the definition of IT risk criteria, the identification of IT risks, the definition of the need for protection, the resulting protective measures for IT operations, and the definition of appropriate measures for risk treatment and	Google has a well established information security organization with well-defined roles and responsibilities, managed by an executive who is dedicated to Security and Privacy, is independent of Information Technology responsibility, and may escalate to the board level concerning security issues. 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.

BAIT No. 5 Clause 5.2 The Institute shall implement appropriate, state-of-the-art operational information security measures and processes on the basis of the information security policy and information security guidelines.	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. Security Health Analytics managed vulnerability assessment scanning for Google Cloud can automatically detect common vulnerabilities and misconfigurations. Google segregates its production environment from its corporate environment. Google's production network is separated from other networks. 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. We use several layers of encryption to protect data at rest. By default, the storage infrastructure encrypts all user data before the user data is written to physical storage. The infrastructure performs encryption at the application or storage infrastructure layer. Google employs several security measures to help ensure the authenticity, integrity, and privacy of data in transit. Google encrypts and authenticates data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. All VM-to-VM traffic within a VPC network and peered VPC networks is encrypted. Our data centers are protected with several layers of security to prevent any unauthorized access to your data. We use secure perimeter defense systems, comprehensive camera coverage, biometric authentication, and a 24/7 guard staff. In addition, we enforce a strict access and security policy at our data centers and ensure all staff is trained to be security minded.

BAIT No. 5 Clause 5.3 Threats to the information group must be identified as early as possible. Potentially security-relevant information must be evaluated centrally in an appropriately timely and rule-based manner. This information must be protected during transport and storage and must be available for later evaluation for an appropriate period of time. BAIT No. 5 Clause 5.3 Notes Potentially security-relevant information is, for example, log data, messages and faults that can provide indications of violations of the protection goals. The rule-based evaluation (e.g., via parameters, correlations of information, deviations or patterns) of large volumes of data usually requires the use of automated IT systems. Subsequent evaluations include forensic analysis and internal improvement measures. The timeframe should be commensurate with the threat level.	Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs.
BAIT No. 5 Clause 5.4 An appropriate portfolio of rules shall be defined to identify security-relevant events. Rules shall be tested before being put into operation. Rules shall be tested for effectiveness and further developed on a regular and ad hoc basis.	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 discussed in the Security Overview whitepaper. Additionally, the FedRamp report in Section RA-5 ¨Vulnerability Scanning¨ outlines Google´s approach to vulnerability management inlc. rule examples. Google provides customers (under NDA) a copy of i.a. the FedRamp Report via the Compliance Reports Manager that demonstrates compliance with these controls.
BAIT No. 5 Clause 5.5 Security-relevant events shall be analyzed in a timely manner, and resulting information security incidents shall be responded to appropriately under the responsibility of information security management. BAIT No. 5 Clause 5.5 Comment. Security-relevant events result, for example, from the rule-based evaluation of potentially security-relevant information. Prompt analysis and response may require a permanently staffed central	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 note in particular the following of the C5:2021 report:

BAIT No. 5 Clause 5.6 The security of the IT systems shall be reviewed regularly, on an ad hoc basis avoiding conflicts of interest. Results are to be analyzed with regard to necessary improvements and risks are to be controlled appropriately. BAIT No. 5 Clause 5.6 Note The frequency, type and scope of the review should be based in particular on the need for protection and the potential attack surface (e.g., accessibility from the Internet) of the IT system. Types of reviews include: - Deviation analyses (gap analyses) - Vulnerability scans - Penetration tests - Simulations of attacks.	Security Health Analytics is automatically enabled when you select the Security Command Center Standard or Premium tier. Security Health Analytics detectors monitor a subset of resources from Cloud Asset Inventory (CAI), using the following three scan modes to detect vulnerabilities: Batch scan: All detectors are scheduled to run for all enrolled organizations two or more times a day. Detectors run on different schedules to meet specific service level objectives (SLO). To meet 12- and 24-hour SLOs, detectors run batch scans every six hours or 12 hours, respectively. Real-time scan: Supported detectors start scans whenever CAI reports a change in an asset's configuration. Findings are immediately written to Security Command Center. Mixed-mode: Some detectors that support real-time scans may not detect changes in real time in all supported assets. In those cases, configuration changes for some assets are captured immediately and others are captured in batch scans. Google Cloud uses Forseti Security, a collection of community-driven, open-source tools to help you improve the security of your Google Cloud environments. Forseti consists of core modules (inventory, Scanner, Enforcer, Explain,) that you can enable, configure, and execute independently of each other. Google coordinates external 3rd party penetration testing using qualified and certified penetration testers at least annually. 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. Google Cloud Armor Managed Protection is the managed application protection service that helps protect IDS web applications and services from distributed denial-of-service (DDoS) attacks and other threats from the internet. Managed Protection helps protect applications deployed on Google Cloud, on-premises, or on other infrastructure providers. Google Cloud Armor Standard includes always-on protection from volumetric and protocol-based DDoS attacks across any globally load-balanced infrastructure, and access to Google Cloud Armor Web Application Firewall (WAF) rule capabilities, including preconfigured WAF rules for OWASP.
BAIT No. 6 Clause 6.1 Identity and rights management shall ensure that authorizations granted to users are designed and used in a manner that complies with the organizational and functional requirements of the institution. The identity and rights management system shall meet the requirements of AT 4.3.1 clause 2, AT 7.2 clause 2, and BTO clause 9 of MaRisk. All access rights to components of the information network should be subject to standardized processes and controls.	Google maintains policies and procedures that enforce data access permissions and maintains a central identity and authorization management system. Two factor authentication is required for all employee access to all company and customer resources. Access rights are based on a Google employee's job function and role—using the concepts of least-privilege and need-to-know—commensurate with the employee's defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources. How Google Secure the authorisation and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorised access is described in area Identity and Access Management (IDM) of the BSI C5 report.

BAIT No. 6 Clause 6.2 Authorization concepts shall define the scope and conditions of use of authorizations for IT systems (access to IT systems and access to data) and access rights to rooms consistently with the identified need for protection and in a complete and traceable manner for all authorizations provided. Authorization concepts must ensure that authorizations are granted in accordance with the principle of economy ("need-to-know" and "least privilege" principles), that the separation of functions is also maintained across authorization concepts, and that conflicts of interest are avoided. Authorization concepts must be reviewed regularly and on an ad hoc basis and updated if necessary.	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. Please note in particular the following sections of the SOC 2+ CSA Star Type II Report outlining the control design: - Section E, ¨Procedures / Authentication, Authorization and Administration¨ For control effectiveness please refer to the Section ¨Controls, Criteria, Tests and Results of Tests¨. Please also note that the SOC 2+ CSA Star Type II Report provides a mapping to the Cloud Control Matrix (CCM) criteria. Google provides customers (under NDA) a copy of i.a. the SOC 2+ CSA Star Type II Report via the Compliance Reports Manager that demonstrates compliance with these controls How Google Secure the authorisation and authentication of users of the Cloud Service Provider (typically privileged users) to prevent
BAIT No. 6 Clause 6.3 Accesses and accesses must at all times be able to be assigned without doubt to an acting or responsible person (automated if possible).	An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud products. 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. All account actions are recorded for audit purposes.
BAIT No. 6 Clause 6.4 The procedures for setting up, changing, deactivating or deleting authorizations for users must use approval and control processes to ensure that the requirements of the authorization concept are met. In doing so, the department responsible for the subject must be appropriately involved so that it can fulfill its technical responsibility.	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. Please note in particular the following of the C5:2021 report: - Section 4, 6.7 Identity and Access Management (IDM) Google provides customers (under NDA) a copy of i.a. the C5:2021 report via the Compliance Reports Manager that demonstrates compliance with these controls.

BAIT No. 6 Clause 6.5 When checking whether the authorizations granted are still required and whether they comply with the specifications of the authorization concept (recertification), the control authorities responsible for setting up, changing, deactivating or deleting authorizations must be involved.	Google requires access reviews at least semi-annually for critical access groups. Customers are responsible for configuring the access by their users to the service. For Google personnel, authorization is required prior to access being granted.
BAIT No. 6 Clause 6.6 The establishment, modification, deactivation as well as deletion of authorizations and recertification shall be documented in a traceable and evaluable manner.	Google restricts access based on need-to-know and job function. Google maintains automated log collection and analysis tools. Multi-factor authentication is required for any connections to our production environment.
BAIT No. 6 Clause 6.7 The institution shall establish logging and monitoring processes in accordance with the protection needs and target requirements that make it verifiable that the authorizations are only used as intended. Due to the far-reaching intervention options involved, the institution must set up appropriate logging and monitoring processes, especially for activities with privileged (particularly critical) user and access rights.	Cloud Audit Logs provides the following audit logs for each Cloud project, folder and organisation: Admin activity audit logs, data access audit logs, system event audit logs and policy denied audit logs. Google Cloud services write audit log entries to these logs to help you answer the questions of "Who did what, where and when?" within your Google Cloud resources. Cloud IAM provides built-in auditing to ease compliance processes.
BAIT No. 6 Clause 6.8 Accompanying technical and organizational measures must be taken to prevent circumvention of the requirements of the authorization concepts.	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. Please note in particular the following of the C5:2021 report: - Section 4, 6.7 Identity and Access Management (IDM) Google provides customers (under NDA) a copy of i.a. the C5:2021 report via the Compliance Reports Manager that demonstrates compliance with these controls.

BAIT No. 7 Clause 7.1 Significant changes in IT systems as part of IT projects, their impact on the IT structure and IT process organization as well as the associated IT processes must be assessed as part of an impact analysis (cf. AT 8.2 para. 1 MaRisk). The requirements of AT 7.2 (in particular paragraph 3 and paragraph 5) MaRisk, AT 8.2 paragraph 1 MaRisk and AT 8.3 paragraph 1 MaRisk must be met with regard to the initial use of and significant changes to IT systems.	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. Please note in particular the following of the C5:2021 report: - Section 4, 6.11 ¨¨ Procurement, Development, and Modification of Information Systems (DEV)¨ Google provides customers (under NDA) a copy of i.a. the C5:2021 report via the Compliance Reports Manager that demonstrates compliance with these controls.
BAIT No. 7 Clause 7.2 The organizational basis for IT projects and the criteria for their application shall be regulated.	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. The SDLC comprises the following phases: - Inception - Requirements - Design - Test - Custover/Hypercare Please note in particular the C5:2021 report. Google provides customers (under NDA) a copy of i. a. the C5:2021 report via the Compliance Reports Manager that demonstrates compliance with these controls.
BAIT No. 7 Clause 7.3 IT projects must be managed appropriately in terms of duration, resources and quality, taking into account their objectives and risks. Procedure models are to be defined for this purpose, and compliance with them is to be monitored.	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. Please note in particular the C5:2021 report. Google provides customers (under NDA) a copy of i. a. the C5:2021 report via the Compliance Reports Manager that demonstrates compliance with these controls.

BAIT No. 7 Clause 7.4 The portfolio of IT projects must be monitored and managed appropriately. It must be taken into account that risks can also result from dependencies of different projects on each other. BAIT No. 7 Clause 7.4 Note The portfolio view provides an overview of the IT projects with the corresponding project data, resources, risks and dependencies.	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. Please note in particular the following of the C5:2021 report: - Section 4, 6.6 ¨ Operations (OPS) and 6.11 and ¨Procurement, Development, and Modification of Information Systems (DEV)¨ Google provides customers (under NDA) a copy of i.a. the C5:2021 report via the Compliance Reports Manager that demonstrates compliance with these controls.
BAIT No. 7 Clause 7.5 Significant IT projects and IT project risks are reported to the management on a regular basis and as required. Significant project risks are to be taken into account in risk management.	Google has a robust change management process and security policy that is documented and requires approvals from relevant stakeholders before being released into production. Google maintains policy and procedures to ensure consideration of security, quality and availability throughout the SDLC (Software Development Lifecycle). Every Google Cloud product maintains a well documented release and deployment process. This process is validated for each product during the semi-annual compliance audit cycle.
BAIT No. 7 Clause 7.6 Appropriate processes shall be defined for application development, including specifications for requirements elicitation, development objective, (technical) implementation (including programming guidelines), quality assurance, and testing, acceptance, and release. BAIT No. 7 Clause 7.6 Notes Application development includes, among other things, the creation of software for business and support processes (including individual data processing). The design of the processes is risk-oriented.	Google maintains policy and procedures to ensure consideration of security, quality and availability throughout the SDLC (Software Development Lifecycle). Google uses a continuous build and release process informed by industry practices. 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. Google follows a structured code development and release process. As part of this process, code is peer reviewed. Google makes proprietary code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats Please note in particular the following of the C5:2021 report: - Section 4, 6.11 ¨Procurement, Development, and Modification of Information Systems (DEV)¨ Google provides customers (under NDA) a copy of i.a. the C5:2021 report via the Compliance Reports Manager that demonstrates compliance with these controls.

BAIT No. 7 Clause 7.7 Requirements for application functionality must be determined, evaluated, documented, and approved in the same manner as non-functional requirements. Appropriate acceptance and test criteria must be defined for each requirement. The responsibility for determining, evaluating and approving the functional requirements (functional and non-functional) shall be borne by the departments with functional responsibility. BAIT No. 7 Clause 7.7 Notes Requirements documents can differ according to the process model and include, for example: - Business concept (requirements specification) - Technical concept (requirements specification) - User story/product back-log	Google maintains policy and procedures to ensure consideration of security, quality and availability throughout the SDLC (Software Development Lifecycle). Google uses a continuous build and release process informed by industry practices. 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. Google follows a structured code development and release process. As part of this process, code is peer reviewed. Google makes proprietary code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats. Google's global technical infrastructure is designed to provide security through the entire information processing lifecycle at Google. Additionally, information on security infrastructure can be extracted from the whitepaper ¨Google
BAIT No. 7 Clause 7.8 During application development, appropriate precautions must be taken, depending on the protection requirements appropriate precautions must be taken to ensure that the confidentiality, integrity, availability and authenticity of the data to be processed are traceable even after each application has gone live.	Google has a global scale technical infrastructure designed to provide security through the entire information processing life cycle at Google. This infrastructure provides secure deployment of services, secure storage of data with end user privacy safeguards, secure communications between services, secure and private communication with customers over the internet, and safe operation by administrators. Google uses this infrastructure to build its internet services, including both consumer services such as Search, Gmail, and Photos, and enterprise services such as Google Workspace and Google Cloud. The security of the infrastructure is designed in progressive layers starting from the physical security of data centers, continuing on to the security of the hardware and software that underlie the infrastructure, and finally, the technical constraints and processes in place to support operational security. Google invests heavily in securing its infrastructure with many hundreds of engineers dedicated to security and privacy distributed across all of Google, including many who are recognized industry authorities. Access control to functions provided by Google is covered in area PSS of the BSI C5 report. Additionally, information on security infrastructure can be extracted from the whitepaper ¨Google infrastructure security design overview¨

BAIT No. 7 Clause 7.9 The integrity of the application (especially the source code) must be adequately ensured. In addition, precautions must be taken to identify, among other things, whether an application has been inadvertently modified or intentionally tampered with. BAIT No. 7 Clause 7.9 Comment. A suitable precaution, taking into account the need for protection, may be the review of the source code. Source code review is a methodical investigation to identify risks.	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse. Google uses a continuous build and release process informed by industry practices. this includes secure source code repository and code signing These controls are mapped to the following audit report and standards framework references that Google holds certifications for: - CSA Guidance V3.0 - AICPA/SOC 2 Controls - ISO/IEC 27001:2013 - ISO/IEC 270017:2015 - ISO/IEC 270018:2015 - NIST SP800-53 R3 - PCI DSS v3.2 - Shared Assessments 2017 AUP Google provides customers (under NDA) a copy of i.a. the C5:2021 report via the Compliance Reports Manager that demonstrates compliance with these controls.
BAIT No. 7 Clause 7.10 The application and its development must be documented clearly and in a manner that is comprehensible to knowledgeable third parties. For example, versioning of the source code and requirements documents contributes to the traceability of the application development.	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. Please note in particular the following of the C5:2021 report: - Section 4, 6.11¨Procurement, Development, and Modification of Information Systems (DEV)¨ Google provides customers (under NDA) a copy of i.a. the C5:2021 report via the Compliance Reports Manager that demonstrates compliance with these controls.

BAIT No. 7 Clause 7.11 A methodology shall be defined and implemented for testing applications prior to their initial deployment and after significant changes. The tests shall include in their scope the functionality of the application, the implemented measures to protect the information and, if relevant, the system performance under different stress load scenarios. The functional responsible parties shall be responsible for the execution of acceptance tests. Test environments for the execution of acceptance tests shall have correspond to the production environment in aspects essential to the test. Test activities and test results must be documented. BAIT No. 7 Clause 7.11 Note Test execution requires relevant expertise on the part of the testers as well as an adequately designed independence from the application developers. The need to protect the data used for testing must be taken into account. In a risk-oriented manner, the measures for protecting the information also include penetration tests.	Google follows a structured code development and release process. As part of this process, all code is peer-reviewed. Google makes purpose built code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats. Google has guidelines to perform fuzz testing, sandboxing, third-party library monitoring, source code analysis; vulnerability scanning to detect, mitigate and resolve security issues as part of the software testing lifecycle. Please note in particular the following of the C5:2021 report: - Section 4, 6.4 ¨Asset Management (AM)¨ Google provides customers (under NDA) a copy of i.a. the C5:2021 report via the Compliance Reports Manager that demonstrates compliance with these controls.
BAIT No. 7 Clause 7.12 After the application has gone live, possible deviations from regular operation must be monitored, their causes investigated and, if necessary, remedial action initiated. BAIT No. 7 Clause 7.12 Comment Indications of significant deficiencies can be, for example, accumulations of deviations from regular operation.	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. Google maintains configuration management tools to detect and automatically correct deviations from its baseline configuration and collects and secures audit records. Please note in particular the following of the C5:2021 report: - Section 4, 6.6 ¨ Operations (OPS) and 6.11 and ¨Procurement, Development, and Modification of Information Systems (DEV)¨ Google provides customers (under NDA) a copy of i.a. the C5:2021 report via the Compliance Reports Manager that demonstrates compliance with these controls.

BAIT No. 8 Clause 8.2 The components of the IT systems and their relationships to each other shall be managed in a suitable manner, and the inventory data recorded for this purpose shall be updated regularly and on an ad hoc basis.	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 maintains asset inventories and assigns ownership for managing its critical resources. Google uses a continuous build and release process informed by industry practices. Google Cloud uses Forseti Security, a collection of community-driven, open-source tools to help you improve the security of your Google Cloud Platform (GCP) environments. Forseti consists of core modules (inventory, Scanner,Enforcer, Explain,) that you can enable, configure, and execute independently of each other. Please note in particular the following of the C5:2021 report: - Section 4, 6.4 ¨Asset Management (AM)¨ Google provides customers (under NDA) a copy of i.a. the C5:2021 report via the Compliance Reports Manager that demonstrates compliance with these controls.
BAIT No. 8 Clause 8.3 The portfolio of IT systems requires management. IT systems should be updated on a regular basis. Risks from IT systems that are obsolete or no longer supported by the manufacturer must be managed (lifecycle management).	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. Please note in particular the following of the C5:2021 report: - Section 4, 6.4 ¨Asset Management (AM)¨ Google provides customers (under NDA) a copy of i.a. the C5:2021 report via the Compliance Reports Manager that demonstrates compliance with these controls.

BAIT No. 8 Clause 8.4 The processes for changing IT systems must be designed and implemented depending on the type, scope, complexity and risk content. This also applies to new or replacement IT systems as well as to security-relevant improvements (security patches).	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.
BAIT No. 8 Clause 8.5 Changes to IT systems must be recorded in an orderly manner, documented, evaluated taking into account possible implementation risks, prioritized, approved and implemented in a coordinated and secure manner. Suitable processes must also be established for time-critical changes to IT systems. BAIT No. 8 Clause 8.5 Note For low-risk configuration changes/parameter settings (e.g., changes to the layout of applications, replacement of defective hardware components, connection of processors), deviating procedural specifications/controls can be defined (e.g., dual control principle, documentation of changes or downstream control).	Changes to the Google Cloud Platform are delivered as software releases. Change Management policies, including security code reviews and emergency fixes, are in place, and procedures for tracking, testing, approving, and validating changes are documented. Each service has a documented release process that specifies the procedures to be used, including a definition of the scope of changes to be delivered, source code control, code review, building, testing, and record keeping. 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. Additionally, Google implements a business continuity plan for our Services, reviews and tests it at least annually and ensures it remains current with industry standards. Please note in particular the following of the C5:2021 report: - Section 4, 6.6 ¨ Operations (OPS) and 6.11 and ¨Procurement, Development, and Modification of Information Systems (DEV)¨ Google provides customers (under NDA) a copy of i.a. the C5:2021 report via the Compliance

BAIT No. 8 Clause 8.6 The reports of unplanned deviations from regular operation (incidents) and their causes must be recorded and evaluated in a suitable manner, prioritized in particular with regard to any resulting risks, and escalated in accordance with defined criteria. Standard procedures, e.g., for measures and communication, and responsibilities (e.g., for malicious code on end devices, malfunctions) must be defined for this purpose. Processing, root cause analysis and solution finding, including follow-up, must be documented. There must be an orderly process for analyzing possible correlations between faults and their causes. The processing status of open reports of malfunctions, as well as the appropriateness of the evaluation and prioritization, shall be monitored and controlled. The institution shall define appropriate criteria for informing stakeholders (e.g. management, competent supervisory authority) about incidents. BAIT No. 8 Para. 8.6 Notes	Google has a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Google's security incident management program is structured around the NIST guidance on handling incidents (NIST SP 800–61). Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. Incident response policies are in place, and procedures for handling incidents are documented. Please note in particular the following of the C5:2021 report: - Section 4, 6.13 ¨Security Incident Management (SIM)¨ Google provides customers (under NDA) a copy of i.a. the C5:2021 report via the Compliance Reports Manager that demonstrates compliance with these controls.
BAIT No. 8 Clause 8.7 The specifications for data backup procedures (excluding data archiving) shall be set out in writing in a data backup concept. The requirements set out in the data backup concept for the availability, readability and up-to-dateness of customer and business data and for the IT systems required to process them shall be derived from the requirements of the business processes and the business continuity plans. The procedures for restoring and ensuring the readability of data must be tested regularly, at least annually, as part of a random sample and on an ad hoc basis. BAIT No. 8 Clause 8.7 Notes The requirements for the measures to ensure the availability, readability and	Google has procedures in place to dispose of confidential information according to Google's data retention and deletion policy. Google details its agreements for data deletion (including retention) and data export per applicable laws and regulations in the Cloud Data Processing Addendum. Data retention and deletion is covered in the area Operations (OPS) of the BSI C5 report. See also whitepaper on data deletion.
BAIT No. 8 Clause 8.8 The current performance and capacity requirements of the IT systems shall be surveyed. Future performance and capacity requirements must be estimated. Service provision shall be planned and monitored, in particular to identify bottlenecks in a timely manner and to respond appropriately. The performance and capacity requirements of information security measures must be taken into account in planning.	Google collects capacity and use data on its infrastructure as needed to inform capacity planning and internal Service Level Agreement performance. Google maintains an effective resource economy with internal Service Level Agreements between engineering teams that provide for capacity planning and provisioning decisions. Also policies and procedures are in place for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities. The authorization to provision additional processing capacity is obtained through budget approvals and managed through internal Service Level Agreements SLAs as part of an effective resource economy. Google has established a resource management policy to monitor, maintain, and evaluate capacity demand. Google's availability monitoring dashboards provide details such as resource footprint, central processing unit capacity, and random-access memory availability to monitor resource availability across its data centers and allow Google to validate that data has been replicated to more than one location. Resource management is covered in the areas Physical Security (PS) and Organisation of

BAIT No. 10 Clause 10.1 The institution shall define objectives for emergency management and, derived from these, establish an emergency management process. Precautions must be taken for emergencies in time-critical activities and processes (emergency concept). The measures defined in the emergency concept must be suitable for reducing the extent of possible damage (cf. AT 7.3 para. 1 MaRisk). The contingency plan must include business continuation and recovery plans. In the case of outsourcing of time-critical activities and processes, the outsourcing institution and the outsourcing company must have coordinated contingency plans (see AT 7.3 para. 2 MaRisk). The effectiveness and appropriateness of the contingency plan must be reviewed regularly. For time-critical activities and processes, it must be demonstrated for all relevant scenarios at least annually and on an ad hoc basis (see AT 7.3 para. 3 MaRisk).	Google performs annual testing of its emergency response processes. In addition, the existence and operating effectiveness of the incident response plans, are verified as part of our SOC 2 report. Google performs annual testing of its business continuity plans to simulate disaster scenarios that model catastrophic events that may disrupt Google operations. Google has an internal security operations team to act as a liaison with emergency personnel. 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. Please note in particular the following of the C5:2021 report: - Section 4, 6.14 ¨ Business Continuity Management (BCM)¨ Google provides customers (under NDA) a copy of i.a. the C5:2021 report via the Compliance Reports Manager that demonstrates compliance with these controls.
BAIT No. 10 Clause 10.2 The objectives and framework of IT emergency management shall be defined on the basis of the objectives of emergency management. BAIT No. 10 Clause 10.2 Comment. Framework conditions include, among other things, organizational aspects such as interfaces to other areas (including risk management or information security management).	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. Please note in particular the following of the C5:2021 report: - Section 4, 6.14 ¨ Business Continuity Management (BCM)¨ Google provides customers (under NDA) a copy of i.a. the C5:2021 report via the Compliance Reports Manager that demonstrates compliance with these controls.

BAIT No. 10 Clause 10.3 The institution shall prepare IT contingency plans based on the contingency concept for IT systems that support time-critical activities and processes. BAIT No. 10 Clause 10.3 Note IT contingency plans shall include restart, emergency operation and recovery plans and the parameters defined for them and shall take into account dependencies in order to restore the time-critical activities and processes.	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. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. Please note in particular the following of the C5:2021 report: - Section 4, 6.14 ¨ Business Continuity Management (BCM)¨ Google provides customers (under NDA) a copy of i.a. the C5:2021 report via the Compliance Reports Manager that demonstrates compliance with these controls
BAIT No. 10 Clause 10.4 The effectiveness of IT contingency plans shall be verified through IT contingency testing at least annually. The tests must fully cover IT systems that support time-critical activities and processes. Dependencies between IT systems or on shared IT systems shall be adequately considered. An IT test concept must be drawn up for this purpose. BAIT No. 10 Clause 10.4 Comment The IT test concept includes tests of individual IT systems (e.g., components, individual applications) as well as their combination into system networks (e. g., high-availability clusters) and processes (e.g., access management).	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
BAIT No. 10 Clause 10.5 The institution shall demonstrate that, in the event of a data center failure, the time-critical activities and processes can be provided from a sufficiently remote data center and for a reasonable time and for the subsequent restoration of IT normal operations.	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.

BAIT No. 12 Clause 12.2 The scope of critical infrastructures within the information system shall be clearly identified. All relevant interfaces shall be included in this context. All relevant requirements of the BAIT and other regulatory requirements shall also be comprehensibly applied to all components and areas of the critical service. Critical services shall be monitored appropriately. Possible effects of security incidents also on critical services shall be assessed. BAIT No. 12 Clause 12.2 Notes This can be done, for example, by additionally marking the components and areas of the information group belonging to the critical infrastructures in the inventory in accordance with 3.3. BAIT (for example, in a configuration management database CMDB). The reference to the respective asset categories of the CRITIS operator to be audited must be shown.	"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. In addtion, 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. Additionally, Google maintains BSCI C5 certification (Area: Physical Security (PS)) which outlines Google´s controls in relation to Physical Security. Please note in particular the following of the C5:2021 report: - Section 4, 6.5 Physical Security (PS) Google provides customers (under NDA) a copy of i.a. the C5:2021 report via the Compliance Reports Manager that demonstrates compliance with these controls.
BAIT No. 12 Clause 12.2 Notes Appropriate measures shall be taken to ensure that the systems relevant to the operation of the critical services are subject to a resilient architecture.	Google maintains BSCI C5 certification.
BAIT No. 12 Clause 12.4 The CRITIS protection objective must be taken into account at all times, from the identification of protection needs, through the definition of appropriate measures, to the effective implementation of these measures, including the implementation and regular testing of appropriate emergency preparedness measures. must always be taken into account. BAIT No. 12 Clause 12.4 Notes In particular, this shall be considered for the following aspects: - the KRITIS protection objective must also be taken into account in the case of outsourcing of services in accordance with sections 25a, 25b KWG in conjunction with AT 9 and AT 5 subsection 3. f) MaRisk as well as chapter 9. BAIT - Measures must be taken as part of emergency preparedness (AT 7.3 MaRisk and Chapter 10. BAIT) to ensure that critical services can be maintained in the event of an emergency.	Google maintains BSCI C5 certification.

BAIT No. 12 Clause 12.5 Evidence pursuant to Section 8a (3) BSIG regarding compliance with the requirements pursuant to Section 8a (1) BSIG can be provided as part of the annual audit. The CRITIS operator must submit the relevant verification documents to the BSI in a timely manner, in accordance with the applicable BSI requirements. BAIT No. 12 Clause 12.5 Notes When providing evidence as part of the annual audit, the following should be taken into account compliance with the requirements pursuant to Section 8a (1) BSIG by the CRITIS operator should be referenced to the 2018 annual financial statements for the first time and must subsequently be demonstrated to the BSI at least every two years. In addition to the audit as part of the annual financial statements, other options for providing evidence are permissible. Accordingly, the KRITIS operators should observe the "Guidance on evidence pursuant to Section 8a (3) BSIG" as amended from time to time.	Google maintains BSCI C5 certification.