UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

This document is designed to help UK telecoms providers supervised by Ofcom (providers of public electronic communications networks and/or services) to consider the UK Telecommunications Security Code Of Practice 2022 under the UK Telecoms Security Act 2021 (“**framework**”) in the context of Google Cloud IaaS & PaaS services. This information is relevant for telecoms providers wishing to host “Security Critical Functions” (SCFs) and/or “Network Oversight Functions” (NOFs) and/or related “sensitive data” (as defined by the Electronic Communications Security Measures Regulations 2022) in Google Cloud IaaS/PaaS platforms (e.g. Google Compute Engine, Google Kubernetes Engine, Google Cloud Storage, Google BigQuery and similar services).

For each measure in the Telecoms Security Code Of Practice, we provide commentary to help you understand how you can use Google Cloud services in a way that we believe supports your compliance. Note that according to the framework, responsibility for assessing compliance with these regulations (and providing related evidence to Ofcom) remains with the telecoms providers. For additional information, please contact your Google Cloud account team.

Measure	Description	Google Cloud Commentary	Google Cloud Reference
M1.01	Providers shall maintain accurate records of all externally-facing systems.	Google maintains an automated asset register and assigns ownership for managing its critical resources (not just externally-facing systems). Customers are responsible for maintaining accurate inventory records of their information system components. **Cloud Asset Inventory** provides inventory services based on a time series database.	Introduction to Cloud Asset Inventory
M1.02	Security testing on externally-facing systems should normally be performed at least every two years, and in any case shortly after a significant change occurs.	Google conducts regular testing of Google's production network, including coordination of external 3rd party penetration testing using qualified and certified penetration testers at least annually. Google maintains a Security Red Team and also offers a Vulnerability Reward Program for anyone that discovers a bug in Google Cloud software Customers may also conduct security audits as described in Google's **Cloud Data Processing Addendum**.	Attacking Google to Defend Google: How Google Does Red Team Google's Bug Hunting community Cloud Data Processing Addendum
M1.03	Equipment in the exposed edge shall not host sensitive data or security critical functions.	Google Cloud does not deploy equipment within the "exposed edge" (as defined by the Telecoms Security Code Of Practice).	N/A
M1.04	Physical and logical separation shall be implemented between the exposed edge and security critical functions. (Note that this requirement may not be necessary once datasets and functions can be cryptographically-protected from compromise)	Refer to **M1.03**	N/A
M1.05	Security boundaries shall exist between the exposed edge and critical or sensitive functions which implement protective measures.	Refer to **M1.03**	N/A
M1.06	Equipment in the exposed edge shall not be able to impact operation or routing within the core network. As an example, the exposed edge shall not be a PE-node within the provider's IP core.	Refer to **M1.03**	N/A
M2.01	Privileged user access rights shall be regularly reviewed and updated as part of business as usual management. This shall include updating privileged user rights in line with any relevant changes to roles and responsibilities within the organisation.	For Google Cloud employees, this is covered by Google internal security controls, evidenced by compliance to standards such as **ISO 27001**. Google's Access Control systems are also continuously synchronized with HR data to check for any changes in roles. For customer workloads, **Identity and Access Management (IAM)** access rights should be	ISO/IEC 27001 Identity and Access Management (IAM) Policy Intelligence

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
		reviewed in line with customer security policies. **Policy Intelligence** can also be used to quickly identify who has access to which resources and to flag excess permissions.	
M2.02	All privileged access shall be logged.	**Audit Logs** are enabled by default in Google Cloud (logging of customer admin access). For sensitive customer workloads and data, customers can turn on **Access Transparency** (logging of Google admin access).	Cloud Audit Logs Google Cloud services with audit logs Access Transparency
M2.03	Privileged access shall be via secure, encrypted and authenticated protocols whenever technically viable.	Google Cloud APIs accept only secure requests using TLS encryption. OAuth 2.0 is used for API authentication. Google Cloud also encrypts all data in transit. Customer workloads are typically accessed via SSH. For sensitive workloads, it is recommended to use Private IP and to connect via **Identity-Aware Proxy (IAP).**	Google Cloud APIs Authentication methods at Google Encryption in transit Building internet connectivity for private VMs
M2.04	Management protocols that are not required shall be disabled on all network functions and equipment.	By default, Google Cloud blocks all external traffic except SSH, RDP and ICMP. Customers can modify **Cloud Firewall** rules as required.	VPC firewall rules
M2.05	Default passwords shall be changed upon initialisation of the device or service and before its use for the provision of the relevant network of service.	Google Cloud does not make use of default passwords. Customers can use **Cloud Identity** to manage password rules, multi-factor authentication and single sign on.	Cloud Identity
M2.06	The infrastructure used to support a provider's network shall be the responsibility of the provider, or another entity that adheres to the regulations, measures and oversight as they apply to the provider (such as a third party supplier with whom the provider has a contractual relationship). Where the provider or other entity adhering to the regulations has responsibility, this responsibility shall include retaining oversight of the management of that infrastructure (including sight of management activities, personnel granted management access, and management processes).	Google has an extensive set of security controls and audited management practices covering areas such as personnel security, access control, asset management, information security, confidentiality, physical & environmental security, encryption, network security, operational security, supplier management, incident management, change management, business continuity. Evidence of these controls is via Google's compliance to international security standards such as ISO 27001, ISO 27017, ISO 27018, AICPA SOC 1, SOC 2, SOC 3 as well as UK specific standards such as NCSC Cyber Essentials Plus, NCSC Cloud Security Guidelines. US federal standards such as FedRAMP and NIST 800-53 may also be relevant. Google Cloud has a well-documented model of "shared responsibilities and shared fate" and operates against well defined SLAs. Google maintains the integrity, security and performance of the shared platform. For example, security patches will be applied to the underlying infrastructure to protect against emerging exploits, new features are introduced to maintain competitiveness and maintenance activities are carried out in the event of component failures. Google Cloud customers are responsible for the security of their workloads running in Google Cloud and have many controls available to facilitate this, including identity and access management, key management, network security controls, API security controls, backup & disaster recovery solutions and many other things. Google helps customers to maintain security by providing best-practices, templates and security products & features, as described elsewhere in this document.	Compliance resource center Shared responsibilities and shared fate on Google Cloud Google Cloud Platform Service Level Agreements

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
M3.01	Providers shall understand how incoming signalling arrives into their network, and outgoing signalling leaves their network. Specifically, the interfaces over which signalling enters and leaves the network, and the equipment which sends and processes external signalling.	Not applicable to Google Cloud.	N/A
M3.02	Providers shall understand what network equipment could be impacted by malicious signalling.	Not applicable to Google Cloud.	N/A
M3.03	Providers shall understand what network and user data could be compromised through malicious signalling.	Not applicable to Google Cloud.	N/A
M3.04	Providers shall understand who they directly connect with over the signalling network and operate on the principle that incoming signals are from untrusted networks.	Not applicable to Google Cloud.	N/A
M3.05	At edge signalling nodes, providers shall block any incoming message using any source address internal to the provider's network.	Not applicable to Google Cloud.	N/A
M3.06	Trust shall not be assumed based on the source of any incoming message. For example, 'UK' source addresses (e.g. +44 global titles in SS7) shall not be assumed to be trusted and allowed by default.	Not applicable to Google Cloud.	N/A
M3.07	Where the signalling message is protected by end-to-end authentication, risk decisions and associated security controls may be determined based upon the authenticated source	Not applicable to Google Cloud.	N/A
M3.08	Where providers allow others to use numbers ranges that have been allocated to them (e.g. GTs, IMSIs), they remain responsible for the activity related to that number range, and any further security implications. This does not apply in the case of MSISDNs shared through MNP.	Not applicable to Google Cloud.	N/A
M3.09	Any outgoing message that uses a source address that should not transit or leave the provider's network shall not be permitted to leave the provider's network.	Not applicable to Google Cloud.	N/A
M3.10	Networks shall only send outgoing signalling in support of services permitted by the recipient. Guidance on what the GSMA has defined as permitted services is set out within Section 5 of GSMA's charging and accounting principles44 and Section 10 of GSMA's interconnection and interworking charging principles	Not applicable to Google Cloud.	N/A
M3.11	External BGP updates shall be monitored for evidence of misuse.	Not applicable to Google Cloud.	N/A
M3.12	Any BGP misuse that impacts their network or services shall be mitigated in a timely manner, and at least within 12 hours whenever technically possible	Not applicable to Google Cloud.	N/A
M3.13	Providers shall ensure that contact details are current and accurate on all the Regional Internet Registries (e.g. RIPE) and should endeavour to keep other	Not applicable to Google Cloud.	N/A

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
	data sources accurate.		
M3.14	All address space and autonomous system number (ASN) resources allocated to a service provider shall be correctly recorded in such a way that it is simple to identify and contact the ‘owner’ to assist in resolving issues.	Not applicable to Google Cloud.	N/A
M3.15	Providers shall implement ingress and egress route filtering.	Not applicable to Google Cloud.	N/A
M3.16	Providers shall adopt and implement mechanisms that prevent IP address spoofing.	Not applicable to Google Cloud.	N/A
M3.17	The provider shall share such details, as are appropriate and proportionate, of any BGP misuse with other providers where it may cause a connected security compromise.	Not applicable to Google Cloud.	N/A
M3.18	An external path update that includes a prefix owned by the provider shall not be accepted.	Not applicable to Google Cloud.	N/A
M3.19	End-users shall not be able to spoof IPs over the data plane (e.g. in line with BCP38).	Not applicable to Google Cloud.	N/A
M4.01	The provider shall ensure the risks included in Regulation 7(3) are assessed prior to contract, and this assessment is documented. This assessment shall inform both risk management and procurement processes.	Google Cloud assumes this measure is applicable to providers only (no flow down to suppliers).	N/A
M4.02	During procurement of equipment, prior to contract award, providers should, as a minimum, use the guidance contained in NCSC’s vendor security assessment to assess third party suppliers.	Google Cloud provides extensive documentation of its security practices and capabilities. Google Cloud also maintains and publishes compliance with a wide range of security standards and regulations. All external parties that provide tools, components or support to Google Cloud must be qualified under Google’s Vendor Security Assessment program. The VSA is leveraged by Google as a method of mitigating supply chain risks, and serves as an assessment and review of risks associated with suppliers or contractors. Vendors are re-evaluated at least annually.	Security overview Compliance resource center Google Cloud risk assessment resources
M4.03	The provider shall record all equipment that remains in use but has reached the vendor's end-of-life date. Providers shall regularly review their use of this equipment, with a view to reducing the risk of a security compromise occurring as a result of unsupported equipment remaining in use.	Software services provided by Google Cloud are typically upgraded automatically to remain in support. As per our **Service Terms**, Google Cloud will provide customers with at least 12 months notice before discontinuing support for any generally available service Customers are responsible for Operating Systems deployed to Google Cloud Virtual Machines. Google Cloud provides tools such as VM Manager to help customers track their OS inventory and ensure they can upgrade OS components to remain in support from a software perspective. From a hardware perspective, Google Cloud services are abstracted from the underlying hardware layer. Google has internal policies to ensure that any systems that are reaching end of life are tracked and prioritized for replacement.	Google Cloud Platform Terms of Service About VM Manager
M4.04	The provider shall produce a plan to replace the unsupported equipment at an appropriate time, dependent on the level of risk.	Refer to **M4.03**	N/A

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
M4.05	The provider shall record all risk management processes undertaken. Guidance on risk management processes can be found on the NCSC website.	Information about Google's approach to risk management is available in Google's security documentation, certifications and audit reports. Google undergoes independent third-party audits on at least an annual basis to provide independent verification of our operations and internal controls. Google collaborates with third-party risk management (TPRM) providers to support provider risk assessments. TPRM providers perform regular assessments of Google Cloud's platform and services—they inspect hundreds of security, privacy, business continuity, and operational resiliency controls aligned with industry standards and regulations such as ISO 27001, SOC2, CSA STAR, NIST SP 800-53, NIST CSF and more. Based on their observations and assessments, TPRM providers develop independent audit reports that can help inform provider risk assessment processes. Google Cloud also supports UK specific standards such as NCSC Cyber Essentials Plus, NCSC Cloud Security Guidelines	Security overview Compliance resource center NCSC - Cloud Security (UK) Google Cloud risk assessment resources
M4.06	Providers shall only store SIM credentials and SIM transport keys within secured systems that ensure data integrity and prevent 'read' access to key material.	Not applicable to Google Cloud.	N/A
M4.07	Providers shall review the security of existing SIM cards on an annual basis, including the supplier, the protection of keys, the algorithms used by the SIM, and the applets provisioned and running on SIMs.	Not applicable to Google Cloud.	N/A
M4.08	Providers shall phase out the use of SIMs which present an unmitigatable security risk, such as the use of deprecated security algorithms.	Not applicable to Google Cloud.	N/A
M5.01	The provider shall implement appropriate business processes. In order to achieve this, providers shall have regard to implementing the parts of the CAF that define the provider's business processes. These are contained within Annex C. These are: A1-Governance; A2-Risk Management; A3-Asset Management; B5-Resilient Networks and Systems; B6-Staff Awareness and Training; D1-Response and Recovery Planning; D2-Lessons Learned.	Google Cloud has achieved NCSC Cyber Essentials Plus certification and supports compliance with NCSC Cloud Security Principles, as well as ISO 27001, NIST 800-53 and the NIST Cyber Security Framework, which can be closely mapped to the NCSC Cyber Assessment Framework (CAF).	NCSC - Cyber Essentials (UK) NCSC - Cloud Security (UK) National Cyber Security Centre (NCSC) Cloud Security Principles Google Cloud Mapping ISO/IEC 27001 NIST SP 800-53 NIST Cybersecurity Framework & Google Cloud
M5.02	Security changes shall be prioritised and postponements of security changes shall be minimised. Where security changes are postponed, these may need to be recorded as a business risk as appropriate.	Refer to **M8.08**	N/A
M5.03	Providers shall maintain read-only backups of their infrastructure and information and shall be able to restore them. The backups should contain the information necessary to maintain the normal operation of the public electronic communications network or public electronic communications service.	Google Cloud has robust internal backup, disaster recovery and business continuity management procedures in place. This is evidenced by compliance with **ISO 22301**. Google Cloud offers a **Backup and DR** service which is customer configurable. Backup and DR can be used with Cloud Storage, which supports immutable storage via the **Bucket Lock** feature.	Data and Security ISO 22301:2019 & BS EN ISO 22301:2019 Disaster recovery planning guide Backup and DR Service Bucket Lock
M5.04	Providers shall have clear, exercised and implemented processes for managing security incidents, at varying levels of severity.	Google Cloud maintains a well-defined and well-practiced **Incident Response Process** to help ensure prompt notification and investigation of incidents. These procedures include guidelines on prioritization based on severity.	Data incident response process

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
		In addition to our published policy, further evidence is provided via our compliance to international security standards such as ISO 27001 etc (refer to **M2.06**).	
M5.05	Providers shall perform a root-cause analysis of all security incidents. Outcomes of this analysis shall be escalated to an appropriate level, which may include the provider's board.	Google Cloud maintains an **Incident Response Process** which includes root-cause analysis and remediation, as well as notification and escalation procedures.	Data incident response process
M5.06	For significant incidents, providers shall share the high-level lessons learned with other providers, so far as is appropriate and proportionate	Not applicable to Google Cloud.	N/A
M5.07	Lessons learned from previous security incidents shall be used to inform the security of new products and services.	Google Cloud maintains an **Incident Response Process** which includes a Continuous Improvement and Lessons Learned phase.	Data incident response process
M6.01	Non-persistent credentials (e.g. username and password authentication) shall be stored in a centralised service with appropriate role-based access control which shall be updated in line with any relevant changes to roles and responsibilities within the organisation.	All access to Google Cloud requires a globally unique Google Account. Customers can also use **Cloud Identity** to manage password rules, multi-factor authentication and single sign on. **Cloud IAM** is used to implement role-based access control. Google Cloud also supports **Secret Manager** for secure storage of customer API Keys, Passwords, Certificates and other sensitive data.	Cloud Identity Identity and Access Management (IAM) Secret Manager
M6.02	Privileged access shall be via accounts with unique user ID and authentication credentials for each user and these shall not be shared.	Refer to **M6.01**	N/A
M6.03	For accounts capable of making changes to security critical functions, the following measures shall be adopted relating to multifactor authentication: (a) the second factor shall be locally generated, and not be transmitted; and (b) the multi-factor authentication mechanism shall be independent of the provider's network and PAW. Soft tokens (e.g. authenticator apps) may be used.	For Google Cloud employees, all network access requires multi-factor authentication, including the use of a local physical security key. Customers can also use Cloud Identity to enforce multi-factor authentication. MFA options such as physical security keys or software-based authenticators can also be enforced.	Set up 2-Step Verification Titan Security Key
M6.04	All break-glass privileged user accounts must have unique, strong credentials per network equipment.	By default, remote access to Google Cloud VMs is controlled via **SSH Keys** that are unique to each VM (in addition to network-level security). Customers can also choose to implement **OS Login**, which ties VM Linux account management to Google identity and enables fine-grained authorization via Google Cloud IAM.	Create SSH keys About OS Login
M6.05	Default and hardcoded accounts shall be disabled.	Google Cloud does not make use of hard-coded accounts. Every Google Cloud project has a default service account, used for interaction with Google Cloud APIs. For enhanced security, it is recommended that custom service accounts should be created, with least privilege access rights (in preference to sharing the default service account between multiple workloads). This can be enforced globally via Organization Policies.	Best practices for using service accounts Restricting service account usage
M7.01	Any incoming or outgoing message type that should not be sent over	Not applicable to Google Cloud.	N/A

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
	international signalling networks shall be blocked at the logical edge of the provider's network. For example, GSMA CAT 1 messages42 shall be blocked for SS7 networks, and equivalent messages shall be blocked for other signalling protocols such as Diameter, GTP, Interconnect and SS7/SIGTRAN.		
M7.02	When sent over signalling networks, the external exposure of customer data, customer identifiers and network topology information shall be minimised.	Not applicable to Google Cloud.	N/A
M7.03	Providers shall have in place the means for recipients of their BGP routing updates to validate that the BGP routing update originated from the legitimate owner.	Not applicable to Google Cloud.	N/A
M7.04	Where the necessary information is available, providers shall validate that any BGP route updates they receive have originated from the legitimate owner	Not applicable to Google Cloud.	N/A
M8.01	During procurement of equipment, prior to contract award, providers shall ensure the security functionality of all equipment has been tested.	Security code reviews and automated security testing are included in Google's software development process. Google security teams also conduct regular testing of Google's production network. Google maintains a Security Red Team and also offers a Vulnerability Reward Program for anyone that discovers a bug in Google Cloud software. Further evidence of our secure software development process is provided via our compliance certifications (refer to **M2.06**). Customers may also conduct security audits as described in Google's **Cloud Data Processing Addendum**.	Attacking Google to Defend Google: How Google Does Red Team Google's Bug Hunting community Compliance resource center Cloud Data Processing Addendum
M8.02	During procurement of equipment, prior to contract award, providers shall ensure negative testing and fuzzing of equipment interfaces has been performed.	Google Cloud makes use of many security testing techniques, including fuzzing and negative testing.	Fuzzing PCI express: security in plaintext Google infrastructure security design overview
M8.03	Any third party testing shall only be accepted as evidence by the provider if it is repeatable, performed independently of the network equipment supplier and is clearly applicable to the provider's deployment (e.g. relates to the hardware, software and configuration that is being supplied).	Google Cloud undergoes independent third-party audits on a regular basis audited against multiple security standards. Results and certifications are available via our compliance website.	Compliance resource center Google Cloud risk assessment resources
M8.04	Providers shall ensure that security considerations are a significant factor in determining the procurement outcome, considering available evidence from testing, recognising the benefit of any security features that will provide measurable improvement to the security of the network	Google Cloud assumes this measure is applicable to providers only (no flow down to suppliers).	N/A
M8.05	Providers shall record all equipment deployed in their networks, and proactively assess, at least once a year, their exposure should the third party supplier be unable to continue to support that equipment.	Refer to **M1.01** for information about Google's approach to maintaining an automated asset inventory. Google also has a Supply Chain Risk Management program to proactively assess and reduce risk related to both software and hardware supply chains. This plan, which is reviewed at least once a year, includes measures to diversify supply, to ensure continuity of supply against potential supply chain disruption and to assess supplier business continuity plans.	N/A

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
M8.06	Providers shall remove or change default passwords and accounts for all devices in the network, and should disable unencrypted management protocols. Where unencrypted management protocols cannot be disabled, providers shall limit and mitigate the use of these protocols as far as possible.	Refer to **M2.04, M2.05, M6.05**	N/A
M8.07	Providers shall ensure that all security relevant logging is enabled on all network equipment and sent to the network logging systems.	**Audit Logs** are enabled by default in Google Cloud (logging of customer admin access). Customers can also enable the following optional log types that may be relevant for security. **VPC Flow Logs** **Firewall Rule Logs** **Access Transparency Logs**	Cloud Audit Logs Configure VPC Flow Logs Firewall Rules Logging Access Transparency and Access Approval
M8.08	Providers shall prioritise critical security patches over functionality upgrades wherever possible.	Google Cloud implements a **vulnerability management** process that actively scans for security threats across all technology stacks. Security patches are deployed across the Google Cloud estate within a time period that is appropriate to the level of risk. Information is shared with customers via **security bulletins**. Google Cloud also offers automated updates for customer environments in Google Cloud, for example via **Compute Engine OS Patch Management**,**GKE Security Patching** and **Cloud SQL Maintenance.**	Google security overview Security Bulletins About Patch Security patching Understanding Cloud SQL Maintenance: how long does it take?
M8.09	When assessing the risk due to SIM card suppliers, providers shall consider the risk due to the loss of sensitive SIM card data.	Not applicable to Google Cloud.	N/A
M8.10	When transferring the provider's SIM key material from SIM card vendors, transport keys shall not be shared across multiple SIM vendors. Where possible, a range of transport keys shall be used with each SIM card vendor.	Not applicable to Google Cloud.	N/A
M8.11	When providers define new SIM authentication algorithm parameters (e.g. for MILENAGE), the default values shall not be used.	Not applicable to Google Cloud.	N/A
M8.12	For fixed-profile SIM cards, the provider shall ensure that sensitive SIM data is appropriately protected throughout its lifecycle, by both the SIM card manufacturer and within the operator network, given the risk to network resilience and confidentiality should this information be lost.	Not applicable to Google Cloud.	N/A
M8.13	For fixed-profile SIM cards, the confidentiality, integrity and availability of the sensitive SIM card data shared with the SIM card manufacturer shall be protected at every stage of their lifecycle.	Not applicable to Google Cloud.	N/A
M8.14	For fixed-profile SIM cards, providers shall ensure that the security of the SIM card vendor has been independently audited. For example, using the GSMA's SAS scheme provides a means to accredit the security of SAS suppliers	Not applicable to Google Cloud.	N/A
M8.15	For profile-modifiable SIM cards, the provider shall, within the first year of use, update with a new profile (including K/Ki, and OTA keys) that has not been provided externally, including to the SIM card manufacturer. Providers should	Not applicable to Google Cloud.	N/A

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
	aim to ensure that all new UICCs can be updated with new K/Ki and OTA keys after receipt from the SIM card manufacturer.		
M8.16	When under the provider's control, the provider shall ensure that the SIM card can only be modified by specifically allowed servers (for example, determined by IP address and certificate stored on the SIM card).	Not applicable to Google Cloud.	N/A
M9.01	Once the CPE has been configured at the customer site, it shall only contain credentials that are both unique to that CPE, and not guessable from CPE metadata.	Not applicable to Google Cloud.	N/A
M9.02	The provider shall ensure that all CPE provided to customers are still supported by the network equipment supplier. For any provider-provided CPE that go out of third party supplier support, customers shall be informed prior to, and once the equipment goes out of support, and proactively offered a replacement as soon as reasonably practicable. This shall apply only whilst the provider provides the associated service	Not applicable to Google Cloud.	N/A
M9.03	WAN CPE management interfaces shall only be accessible from specified management locations (e.g. URL or IP address)	Not applicable to Google Cloud.	N/A
M9.04	Management of the CPE shall use a secure protocol (e.g. TLS 1.2 or newer)	Not applicable to Google Cloud.	N/A
M9.05	By default, the CPE's customer-facing management interfaces shall only be accessible from within the customer's network.	Not applicable to Google Cloud.	N/A
M9.06	By default, all unsolicited incoming connections towards the customer's network shall be blocked by the CPE.	Not applicable to Google Cloud.	N/A
M10.01	The provider shall maintain records of third party supplier's details, including their thirdparties and the major components which are used in the provision of goods/services/facilities for the provider.	Google maintains lists of third party suppliers who are material to the provision of services to the provider.	Google Cloud Platform Subprocessors
M10.02	The provider shall clearly express the security needs placed on third party suppliers. These shall be defined and agreed in contracts.	Google Cloud's security commitments are defined in our standard **Service Terms** and in the **Cloud Data Processing Addendum.** Additionally, Google has a well defined **Supply Chain Risk Management** policy which includes security policies in relation to our supply chain and security requirements that our suppliers must commit to. Google Cloud's suppliers are required to make contractual commitments to Google regarding matters such as quality, confidentiality, compliance with security standards as well as complying with Google Cloud's **Supplier Code of Conduct**.	Google Cloud Platform Terms of Service Cloud Data Processing Addendum Google Supplier Code of Conduct
M10.03	There shall be a clear and documented shared-responsibility model between the provider and third party suppliers.	Google Cloud operates a well-defined model of **Shared Responsibility and Shared Fate**.	Shared responsibilities and shared fate on Google Cloud

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
M10.04	The provider's incident management process and that of their third party suppliers shall provide mutual support in the resolution of incidents.	Google Cloud maintains an **Incident Response Process,** which includes communication and coordination with any affected customers and third-parties.	Data incident response process
M10.05	Providers shall retain control and oversight of their network and user data.	Google Cloud is committed to clear principles of **security transparency and trust**. Google Cloud also implements many data security controls as standard (including **encryption at rest**, **encryption in transit, network segregation** and **default firewall rules**) to protect customer workloads and customer data. For particularly sensitive customer workloads and data, Google offers a number of optional controls to further enhance customer data security, including: **- Customer Managed Encryption Keys (Bring Your Own Key)** **- External Key Manager (Hold Your Own Key)** **- Access Transparency (logging of all Google Admin access)** **- Access Approval (customer approval for all Google Admin access)** **- Confidential Computing (Encryption-In-Use)** **- VPC Service Controls (Service Perimeter for API Access)** Refer to the whitepaper on Trusting Your Data With Google Cloud for additional details.	Creating trust through transparency Customer-managed encryption keys (CMEK) Cloud External Key Manager Access Transparency Access Approval documentation Confidential Computing VPC Service Controls Trusting your data with Google Cloud
M10.06	The provider shall define what information is made accessible to any third party supplier, ensuring that it is the minimum necessary to fulfil their function. Providers shall place controls on that information and limit third party access to the minimum required to fulfil the business function.	Google Cloud's data processing and data security commitments are documented in the **Cloud Data Processing Addendum**. Customers may also refer to Google Cloud's **Privacy Resource Center** for additional information. Google also provides customers with many tools to control and limit access to customer information stored within Google Cloud (refer to **M10.05**).	Cloud Data Processing Addendum Privacy Resource Center
M10.07	The environment used to hold the network and user data made available to third party suppliers shall be within a system segregated from the rest of the provider's internal systems and data.	Google Cloud assumes this measure is applicable to providers only (no flow down to suppliers).	N/A
M10.08	Providers shall prevent transfer of network and user data outside their environment, except where necessary. Where transfer is necessary, it shall be through a defined process.	Google Cloud assumes this measure is applicable to providers only (no flow down to suppliers).	N/A
M10.09	Where network or user data leaves a provider's control, providers shall contractually require and verify that the data is property protected as a consequence. This shall include assessing the third party supplier's controls to ensure provider data is only visible or accessible to appropriate employees and from appropriate locations	Google has security controls in place to limit and control access to customer data within the production network. For more details, refer to the whitepaper on **Privileged Access Management**. Customers also have the option to enable the following features for additional visibility and control over Google admin access to their services. **- Access Transparency (logging of all Google Admin access)** **- Access Approval (customer approval for all Google Admin access)**	Privileged Access Management in Google Cloud Platform Access Transparency Access Approval documentation
M10.10	All data sharing with third party suppliers shall be over an encrypted and authenticated channel.	Refer to **M2.03**	N/A

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
M10.11	Providers shall contractually oblige third party suppliers to notify the provider within 48 hours (or less), of becoming aware of any security incidents that may have caused or contributed to the occurrence of a security compromise, or where they identify an increased risk of such a compromise occuring. This includes, but is not limited to, incidents in the supplier's development network or their corporate network.	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. Google is reviewing the requirement for more specific incident reporting timelines, in line with evolving regulations in multiple jurisdictions.	Cloud Data Processing Addendum
M10.12	Providers shall contractually require third party suppliers to support the provider in investigations of incidents which cause or contribute to the occurrence of a security compromise in relation to the primary provider, or of an increased risk of such a compromise occurring.	Refer to **M10.04**	N/A
M10.13	Providers shall contractually require the third party suppliers to find and report on the root cause of any security incident that could result in a security compromise in the UK within 30 days, and rectify any security failings found.	Google Cloud maintains a well-defined Incident Response Process. At the resolution stage, the focus is on investigating the root cause, limiting the impact of the incident, resolving immediate security risks (if any), implementing necessary fixes as part of remediation, and recovering affected systems, data, and services. A key aspect of remediation is notifying customers when incidents impact their data. We strive to provide prompt, clear, and accurate notifications containing the known details of the data incident, steps that we have taken to mitigate the potential risks, and actions that we recommend customers take to address the incident. Google is reviewing the requirement for more specific root cause reporting timelines, in line with evolving regulations in multiple jurisdictions.	Data incident response process
M10.14	Where third party suppliers cannot quickly resolve weaknesses, the provider shall work with the third party supplier to ensure the issue is mitigated until resolved.	Refer to **M10.04**	N/A
M10.15	Where third party suppliers do not resolve weaknesses within a reasonable timeframe, the provider shall have a break clause with the third party supplier to allow exit from the contract without penalty	Google Cloud's standard terms include a "Termination for Breach" clause.	Google Cloud Platform Terms of Service
M10.16	Providers shall contractually require third party suppliers to support, as far as appropriate and reasonable, any security audits, assessments or testing required by the provider in relation to the security of the provider’s own network, including those necessary to evaluate the security requirements in this document.	Customers may conduct security audits as described in Google's **Cloud Data Processing Addendum**.	Cloud Data Processing Addendum
M10.17	Providers shall flow down appropriate security measures to the third party administrator. Providers shall ensure that the third party administrator applies controls that are at least as rigorous as the provider when the third party administrator has access to the provider’s network or service or to sensitive data.	Google Cloud has provided guidance on how we support security controls, equivalent to those that would be required from providers, for aspects of the Third Party Administrator role that are applicable to Google Cloud. However, some aspects of the Third Party Administrator role are not applicable or not relevant for Google Cloud, since Google does not have access to the provider's network.	N/A
M10.18	The provider shall retain the right to determine permissions of the accounts used to access its network by third party administrators.	Google Cloud does not have any access to the provider's physical networks.	N/A

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
M10.19	Providers shall ensure that they retain sufficient in-house expertise and technical ability to re-tender their managed services arrangements at any time and shall produce and maintain a plan for moving the provided services back in-house, or to another third party supplier.	Google Cloud assumes this measure is applicable to providers only (no flow down to suppliers). Note that Google Cloud does not charge any data fees for customers that have decided to exit Google Cloud.	Applying for free data transfer when exiting Google Cloud
M10.20	Providers shall maintain an up-to-date list of all third party administrator personnel that are able to access its network, including their roles, responsibilities and expected frequency of access.	Google Cloud does not have any access to the provider's physical networks.	N/A
M10.21	Providers shall have the contractual right to control the members of third party administrator personnel who are involved in the provision of the third party administrator services, including to require the third party administrator to ensure that any member of personnel no longer has access to the network.	Google Cloud does not have any access to the provider's physical networks.	N/A
M10.22	Providers shall not allow routine, direct access to network equipment by third party administrators. Access shall be via mediation points owned and operated by the provider.	Google Cloud does not have any access to the provider's physical networks.	N/A
M10.23	Providers shall implement and enforce security enforcing functions at the boundary between the third party administrator network and the provider network.	Google Cloud does not have any access to the provider's physical networks.	N/A
M10.24	Providers shall contractually require that the third party administrators implement technical controls to prevent one provider or their network from adversely affecting any other provider or their network.	Google Cloud does not have any access to the provider's physical networks.	N/A
M10.25	Providers shall contractually require that the third party administrators implement logical separation within the third party administrator network to segregate customer data and networks.	Google Cloud does not have any access to the provider's physical networks.	N/A
M10.26	Providers shall contractually require that the third party administrators implement separation between third party administrator management environments used for different provider networks.	Google Cloud does not have any access to the provider's physical networks.	N/A
M10.27	Providers shall contractually require that the third party administrators implement and enforce security enforcing functions at the boundary between the third party administrator network and the provider network.	Google Cloud does not have any access to the provider's physical networks.	N/A
M10.28	Providers shall contractually require that the third party administrators implement technical controls to limit the potential for users or systems to negatively impact more than one provider.	Google Cloud does not have any access to the provider's physical networks.	N/A
M10.29	Providers shall contractually require that the third party administrators implement logically-independent privileged access workstations per provider.	Google Cloud does not have any access to the provider's physical networks.	N/A
M10.30	Providers shall contractually require that the third party administrators implement independent administrative domains and accounts per provider.	Google Cloud does not have any access to the provider's physical networks.	N/A

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
M10.31	Providers shall ensure that the elements of the provider network that are accessible by the third party administrator shall be the minimum required to perform its contractual function.	Google Cloud does not have any access to the provider's physical networks.	N/A
M10.32	Providers shall both log and record all third party administrator access into its networks.	Google Cloud does not have any access to the provider's physical networks.	N/A
M10.33	The provider shall contractually require the third party administrator to monitor and audit the activities of the third party administrator's staff when accessing the provider's network.	Google Cloud does not have any access to the provider's physical networks.	N/A
M10.34	The provider shall contractually require from the third party administrator all logs relating to the security of third party administrator's network to the extent that such logs relate to access into the provider's network.	Google Cloud does not have any access to the provider's physical networks.	N/A
M10.35	Providers shall require that the third party administrator networks that could impact the provider undergo the same level of testing as the provider applies to themselves (e.g. TBEST testing as set for the provider by Ofcom from time to time).	Google Cloud does not have any access to the provider's physical networks.	N/A
M10.36	Providers shall contractually require network equipment suppliers to share with them a 'security declaration' on how they produce secure equipment and ensure they maintain the equipment's security throughout its lifetime. It is recommended that any such declaration should cover all aspects described within the Vendor Security Assessment (VSA) (see Annex B), and providers should encourage their suppliers to publish a response to the VSA.	Refer to **M4.02**	N/A
M10.37	As part of the security declaration, any differences in process across product lines shall be recorded.	At the individual product level, compliance with security standards (such as ISO 27001) is recorded on the relevant compliance page.	ISO/IEC 27001
M10.38	Providers shall ensure, by contractual arrangements, that the network equipment supplier's security declaration is signed-off at an appropriate governance level.	Google's Security declarations are signed off at an appropriate senior level of governance. Regarding the commitments that Google requires from its suppliers, refer to **M10.02**.	N/A
M10.39	Where the network equipment supplier claims to have obtained any internationally recognised security assessments or certifications of their equipment (such as Common Criteria or NESAS), providers shall contractually require equipment suppliers to share with them the full findings that evidence this assessment or certificate.	Refer to **M8.03**	N/A
M10.40	Providers shall contractually require network equipment supplier to adhere to a standard no lower than the network equipment supplier's 'security declaration'.	Refer to **M10.02**	N/A
M10.41	Providers shall contractually require network equipment suppliers to supply up-to-date guidance on how the equipment should be securely deployed.	Google Cloud publishes security best practice guides as well as detailed guidance on security, privacy and compliance as part of the Google Cloud Architecture Framework.	Google Cloud security best practices center Google Cloud Architecture Framework: Security, privacy, and compliance

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
		Google Cloud also provides the Security Foundations Blueprint as a reference architecture for secure service deployment.	A blueprint for secure infrastructure on Google Cloud
M10.42	Providers shall contractually require network equipment suppliers to support all equipment and all software and hardware subcomponents for the length of the contract. The period of support of both hardware and software shall be written into the contract.	Google supports its software in accordance with the terms and conditions of the agreement in place between the Customer and Google. That contract details the period of support applicable to each product and timescales applicable to changes or removals of product or service lines.	Google Cloud Platform Terms of Service
M10.43	Providers shall contractually require network equipment suppliers to provide details (product and version) of major third party components and dependencies, including open source components and the period and level of support.	As part of Supply Chain Risk Management, Google conducts such due diligence as it reasonably belives is appropriate on its network equipment suppliers products and software including such relevant due diligence on open source components and dependencies. Google Cloud also publishes details of verified and trusted open source software components via the Assured Open Source Software program (AOSS). This includes SLSA compliance for supply chain assurance and the provision of Software Bill of Materials (SBOM) for open source components.	Assured Open Source Software Securing the software development lifecycle with Cloud Build and SLSA
M10.44	Where relevant to a provider's particular usage of equipment, providers shall contractually require third party suppliers to remediate all security issues that pose a security risk to a provider's network or service discovered within their products within a reasonable time of being notified, providing regular updates on progress in the interim. This shall include all products impacted by the vulnerability, not only the product for which the vulnerability was reported.	Google Cloud implements a **vulnerability management** process that actively scans for security threats across all technology stacks. Security patches are deployed across the Google Cloud estate within an time period that is appropriate to the level of risk. Information is shared with customers via **security bulletins**.	Google security overview
M10.45	Providers shall record where third party suppliers fail to meet these security obligations.	Google Cloud assumes this measure is applicable to providers only (no flow down to suppliers).	N/A
M10.46	Providers shall ensure that their contracts allow details of security issues to be shared as appropriate to support the identification and reduction of the risks of security compromises occurring in relation to the public electronic communications network or public electronic communications service as a result of things done or omitted by third party suppliers.	Google Cloud publicly shares security vulnerability information via **security bulletins**.	Security Bulletins
M10.47	Providers shall contractually require network equipment suppliers to deliver critical security patches separately to feature releases, to maximise the speed at which the patch can be deployed	Refer to **M8.08**	N/A
M10.48	Providers shall ensure their equipment is in a secure-by-default configuration, based on the principle that only required services are made available.	Google Cloud implements security by default, with multiple levels of complementary defenses designed to keep you safe. Our built-in automatic protections include default security services that are part of our secure by design infrastructure such as default encryption for data at rest and in transit, default configurations for services such as compute and storage that limit public access, cloud firewall (with default firewall rules), DDoS protection and always-on audit logs.	Default encryption at rest Encryption in transit Scalable, cloud-first firewall service Google infrastructure security design overview Cloud Audit Logs
M10.49	Providers shall ensure that all deployed equipment either meets the network equipment supplier's recommended secure configuration (as a minimum), or that any variations are recorded and the risk assessed.	Google Cloud assumes this measure is applicable to providers only (no flow down to suppliers).	N/A
M10.50	Providers shall implement necessary mitigations based on identified	Google Cloud assumes this measure is applicable to providers only (no flow down to suppliers).	N/A

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
	equipment risks (e.g. use of an out-of-support component), such that these equipment risks do not increase the overall risk to their networks.		
M10.51	Providers shall update all supported equipment within such period as is appropriate of any relevant and appropriate version being released.	Google Cloud assumes this measure is applicable to providers only (no flow down to suppliers).	N/A
M10.52	Providers shall deploy all security related patches and patches with a security element in a way that is proportionate to the risk of security compromise that the patch is intended to address (see Table 2). Should this not be possible, patches shall be deployed as soon as practicable and effective alternative mitigations put in place until the relevant patch has been deployed. Where a patch addresses an exposed, actively-exploited vulnerability, providers shall ensure that such patches are deployed as soon as can reasonably be achieved, and at most within 14 days of release	Refer to **M8.08**	N/A
M10.53	Providers shall ensure that network equipment continues to meet the requirements in M8.04, M8.05, M8.06, M10.48 and M10.49 throughout its lifecycle including after an upgrade or patch.	Refer to **M8.06** and **M10.48**	N/A
M10.54	The provider shall verify that the third party supplier has a vulnerability disclosure policy. This shall include, at a minimum, a public point of contact and details around timescales for communication.	Google Cloud publicly shares security vulnerability information via security bulletins. Google adheres to a 90-day vulnerability disclosure deadline. We notify vendors of vulnerabilities immediately, with details shared in public with the defensive community after 90 days, or sooner if the vendor releases a fix. When we observe a previously unknown and unpatched vulnerability in software under active exploitation (a “zero-day”), we believe that more urgent action—within 7 days—is appropriate. After 7 days have elapsed without a patch or advisory, we will support researchers making details available so that users can take steps to protect themselves.	Security Bulletins How Google handles security vulnerabilities
M11.01	Operational changes shall only be made according to a formal change process except under emergency or outage situations.	Google Cloud follows internal change management policies, evidenced by compliance to standards such as **ISO 27001** and **ISO 9001**. Customers should implement their own change management procedures. **IAM** and **Organization Policies** can help customers to set policies and technical constraints on who can make changes and what changes are permitted.	ISO/IEC 27001 ISO 9001:2015 How Google Cloud monitors its Quality Management System Identity and Access Management (IAM) Introduction to the Organization Policy Service
M11.02	Any persistent credentials and secrets (e.g., for break glass access) shall be protected and not available to anyone except for the responsible person(s) in an emergency	Refer to **M6.03**	N/A
M11.03	Central storage for persistent credentials shall be protected by hardware means. For example, on a physical host the drive could be encrypted with the use of a TPM. Where a virtual machine (VM) is used to provide a central storage service, that VM and the data included in it shall also be encrypted, use secure boot and be configured to ensure that it can only be booted within an appropriate environment. This is to ensure that data cannot be removed from the operational environment and accessed.	**Cloud KMS** is used to create, store, manage, rotate and revoke security keys, used for encryption-at-rest of customer data within Google Cloud (plus Kubernetes Secrets within etcd). Cloud KMS keys can be protected in hardware via **Cloud HSM**. Google Cloud's **Shielded VM** capability (enabled by default for all customer VMs) offers a Secure Boot process and also provides a vTPM facilty that can be used to protect secrets generated within the VM. For additional protection, customers can also adopt **Confidential**	Cloud Key Management Cloud HSM Hardened virtual machines on Google Cloud Confidential Computing

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
		Computing to enable encryption-in-use of all customer data within Compute Engine and Kubenetes Engine.	
M11.04	Privileged users are only granted specific privileged accounts and associated permissions which are essential to their business role or function.	For Google Cloud employees, access rights and levels are based on their job function and role, using the concepts of least privilege and need-to-know that match access privileges to defined responsibilities. Our employees are granted only a limited set of default permissions to access company resources. Requests for additional access must follow a formal process that involves a request and an approval from the data or system owner, manager, or other executives, as dictated by our security policies. Customers should implement their own access controls procedures. **IAM** and **Organization Policies** can help customers to set policies and technical constraints on who can make changes and what changes are permitted.	Google security overview Identity and Access Management (IAM) Introduction to the Organization Policy Service
M11.05	Privileged access shall be temporary, timebounded and based on a ticket associated with a specific purpose. Administrators shall not be able to grant themselves privileged access to the network.	Google has security controls in place to limit and control access to customer data within the production network. For more details, refer to the whitepaper on **Privileged Access Management.** Customers can also configure **Access Approval** to enable customer approval for Google Admin access to customer data. This approval is timebound, cryptographically signed and can be associated to a specific ticket.	Privileged Access Management in Google Cloud Platform Access Approval documentation
M11.06	While open, tickets shall be updated daily as a record of why privileged access granted to a user remains required, and shall be closed once privileged access is no longer required	Additional access must follow a formal request and approval process. Records of why privileged access is granted to a user are kept as part of the process. Privileged access by Google Admin can be controlled via **Access Approval** (see **M11.05**). Tickets can be updated either by the customer or by Google support teams.	Access Approval documentation
M11.07	Privileged access shall be automatically revoked once the ticket is closed.	With **Access Approval**, access is revoked at the end of the agreed access time period and is not specifically linked to ticket status.	Access Approval documentation
M11.08	Privileged user accounts are generated from a least privilege role template and modified as required. The permissions associated with this account shall not be copied from existing users.	Refer to **M11.04** and **M11.05**	N/A
M11.09	Given a business need, administrators can have multiple roles, each with its own account, provided the risk of doing so has been considered and accepted as part of the provider's risk management processes.	Refer to **M11.04** and **M11.05**	N/A
M11.10	When an emergency occurs, security requirements may temporarily be suspended. Clean-up steps shall be performed after the emergency is resolved to ensure the suspension of these requirements has not compromised the network. Where an ‘emergency’ event occurs, this shall be recorded and audited, along with the reason and time period for which controls were suspended.	"Emergency Access" occurs when there is an urgent threat to the integrity of Google's services, infrastructure, or to any customer services or content. An access with one of these justifications can override an organization's Access Approval policy. This rare type of access is logged in Access Approval with the auto-approved status.	Access Approval documentation
M11.11	Break-glass privileged user accounts should be present for emergency access	Refer to **M11.10**	Access Transparency

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
	outside of change windows, but alerts shall be raised when these are used, the circumstances investigated, and all activity logs audited post emergency.	Customers can also make use of **Access Transparency** to maintain an audit trail of all Google Cloud admin activity, including Emergency Access	
M11.12	Break-glass privileged user account credentials should be single use and changed after use.	Google Cloud does not make use of single-use credentials. We rely instead on internal security controls and customer access approvals as described above.	N/A
M11.13	All privileged access activity undertaken during a management session shall be fully recorded.	Refer to **M2.02**	N/A
M11.14	A device that is not necessary to perform network management or support management operations shall not be able to logically access the management plane.	Refer to **M13.13**	N/A
M11.15	Privileged access to network equipment shall be via a centralised element manager or equivalent config deployment system. For example, privileged users shall not be provided with direct access to any management terminal, except where network connectivity is not available (e.g. break-glass situations).	Google Cloud admin access to the Google production network is via internal proxies that verify identity and enforce security policies such as ACLs and access approvals. For customer access, management architecture is a customer decision but can leverage centralized element management and/or simplified approach such as a **bastion host.**	Privileged Access Management in Google Cloud Platform Securely connecting to VM instances Connect to Linux VMs using a bastion host
M11.16	It shall not be possible to directly communicate between managed elements over the management plane.	For secure separation of customer workloads into trust domains, refer to **M13.12** and **M13.13.** For secure separation of tenants within Google Cloud managed services, refer to the Infrastructure Security whitepaper.	Google infrastructure security design overview
M11.17	The management plane shall be segregated by third party supplier, and between access networks and core networks (e.g. by VLAN). This would not preclude the use of a single orchestration and management solution, provided it is compliant with measure M11.23	Refer to **M11.16**	N/A
M11.18	The management plane shall be configured to ensure that only necessary connections are allowed. Specifically, element managers and other administrative functions shall only be able to communicate with the network equipment that they administer. Further, network equipment shall only be able to communicate with its administrative functions and its ability to establish a connection with these functions shall be limited.	Refer to **M11.16**	N/A
M11.19	The function authorising privileged user access (e.g. the root authentication service) shall be within a trusted security domain (not the corporate network).	For secure separation of customer workloads into trust domains, refer to **M13.12** and **M13.13** Google's **Identity & Access Management** systems are part of the production network, which is a trusted security domain.	Identity and Access Management (IAM)
M11.20	Multi-factor authentication supporting and authorisation functions shall be treated as a network oversight function and shall be within a separate security	Refer to **M11.19**.	N/A

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
	domain to the corporate security domain.		
M11.21	Testing procedures shall be established and utilised to verify that management networks enforce these controls.	Google Cloud assumes this measure is applicable to providers only (no flow down to suppliers).	N/A
M11.22	The provider's wider network outside of the management plane shall be continuously scanned to detect and remediate unnecessary open management protocols, ports and services.	Google conducts its own internal security scanning and automated testing. Customers can also make use of **Security Command Center** to automatically discover cloud assets and uncover security vulnerabilities, potential misconfigurations and security threats.	Cloud security and risk management for multi-cloud environments
M11.23	The management plane used for access networks shall be segregated such that disruption of one management plane segment shall only impact a single UK region.	The management architecture for access networks is a customer decision. Customers may choose to segregate a hosted management plane following the principles described in **M13.12** and **M13.13**. Google Cloud also publishes guidance on the best practices for region selection for customer workloads.	Best practices for Compute Engine regions selection
M11.24	A PAW shall only have access to the internet to the extent it is needed to carry out changes to security critical functions, and such access shall be secured (e.g. via VPN).	Google Cloud does not have any access to the provider's physical networks. Regarding Google Cloud's management of its own production network, we do not use dedicated PAWs. Based on our wider security architecture, Google has adopted a different technical solution which we believe provides an equivalent or higher level of security. Google Cloud has implemented a Zero Trust security architecture that continuously verifies all machines, workloads, API calls, users and devices, combined with strong endpoint security, strict access control and a high level of security monitoring and oversight. Google has shared information about its approach with government cybersecurity authorities such as the NCSC in the UK and CISA in the USA. As a result, Zero Trust is now endorsed and recommended by these authorities as their preferred approach to security. Our corporate devices also meet many of the related security requirements for PAWs (see below). For more details about Google Cloud management of privileged access, refer to M11.04 and M11.05 and M11.15.	Google infrastructure security design overview What is zero-trust security? Zero trust architecture design principles (External) Applying the NCSC Zero Trust Principles on Google Cloud Zero Trust Maturity Model (External) Zero Trust Best Practices for Google Workspace
M11.25	The PAW shall only have access to internal only business systems (e.g. not corporate email).	Refer to **M11.24**	N/A
M11.26	A PAW shall support secure boot, boot attestation, data-at-rest encryption backed by a hardware root-of-trust.	Google implements robust endpoint security controls, not all of which are publicly disclosed. As part of Google Cloud's zero trust access controls, device OS updates, security patches, device certificates, installed software, virus scans, and encryption status (among other factors) are evaluated for potential security risks	Privileged Access Management in Google Cloud Platform
M11.27	A PAW shall be kept patched and up-to-date with a supported OS throughout its lifetime.	Corporate devices used by Google employees are patched and updated automatically and always use a supported OS throughout their lifetime.	N/A
M11.28	Security critical patches shall be applied to PAWs within 14 days, or within such period as is appropriate in the circumstances having regard to the severity of the risk of security compromise.	Google installs applicable security-relevant software and firmware updates within an internally defined time period, appropriate to the level of risk.	N/A
M11.29	A PAW shall prevent the execution of unauthorised code such as binaries or macros within documents.	Google monitors the software used on corporate devices and blocks the installation and execution of unapproved software.	N/A

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
M11.30	A PAW shall use data-at-rest encryption.	All corporate devices used by Google employees implement encryption at rest in line with our security policies.	N/A
M11.31	Health attestation of the PAW shall be used wherever possible, and particularly where the PAW is located outside the UK.	Google implements health attestation of all corporate devices as part of our Zero Trust architecture.	N/A
M11.32	All new deployments of equipment shall be administered via secure, encrypted and authenticated protocols. Insecure or proprietary security protocols shall be disabled.	Refer to **M2.03**	N/A
M11.33	Where administrative access is not via secure channels, the risk this poses and the mitigation applied shall be justified, fully documented and reported at board level.	Google Cloud assumes this measure is applicable to providers only (no flow down to suppliers).	N/A
M11.34	Security protocols and algorithms shall not be proprietary whenever technically viable.	Google is commited to open standards and uses a range of open security standards. All data is encrypted at rest, using **AES-256** encryption with a **FIPS 140-2** validated encryption module. Data is also encrypted in transit, using a range of open protocols including **TLS**, **mTLS**, **QUIC** and **IPSec**. Google also believes in innovation. Internally within Google Cloud we use **ALTS**, a proprietary security protocol that is similar to mTLS but which is optimized for Google's requirements. For more details, refer to the Whitepaper on ALTS.	Default encryption at rest Encryption in transit Application Layer Transport Security
M11.35	Each network equipment shall have strong, unique credentials for every account.	Refer to **M6.02**	N/A
M12.01	Incoming and outgoing signalling traffic shall be monitored.	Not applicable to Google Cloud.	N/A
M12.02	Signalling records are sensitive data and shall be protected from misuse or extraction.	Not applicable to Google Cloud.	N/A
M12.03	Security analysis shall be performed on signalling traffic to find and address malicious signalling.	Not applicable to Google Cloud.	N/A
M12.04	Providers shall establish an effective means to alert each other to malicious signalling where there could be a connected security compromise.	Not applicable to Google Cloud.	N/A
M12.05	Detailed negative testing and fuzzing shall be performed for all interfaces that process data provided over an external signalling interface (This applies to all equipment which this measure applies to, including existing equipment).	Not applicable to Google Cloud.	N/A
M12.06	Malformed, inconsistent or unexpected signalling messages shall be blocked.	Not applicable to Google Cloud.	N/A
M13.01	The virtualisation fabric shall be robustly locked-down, shall use the latest patch for the software version and shall be in support.	Google Cloud configures all physical cloud infrastructure (including host machines and network devices) to provide only essential capabilities, enforced via hardware build controls and standard configurations that are deployed and continuously verified by automated configuration management tools All Google Cloud products are regularly updated. Public release notes are available for all changes. Google's data center equipment (including the virtualization fabric) is continuously	Google infrastructure security design overview Google Cloud release notes Compute Engine release notes

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
		monitored and subject to routine preventative and regular maintenance processes. By definition, the Google-maintained virtualization fabric is always "in support". Google has dedicated teams who are responsible for monitoring, maintaining, managing and securing the Google Cloud network. This includes monitoring of all networks and systems for threats to information security and roll-out of security patches when required. Refer to the Whitepaper on Infrastructure Security for more details.	
M13.02	It shall be possible to update the virtualisation fabric without negatively impacting the network functionality.	By default, Google Cloud will Live Migrate any VMs that are affected by maintenance, security updates or hardware failures. Live migration lets Google Cloud perform maintenance without interrupting a workload, rebooting a VM, or modifying any of the VM's properties, such as IP addresses, metadata, block storage data, application state, and network settings. By default, Google Cloud will also Auto Restart any VM that crashes or is stopped by the system.	Live migration process during maintenance events Set VM host maintenance policy
M13.03	All interfaces on physical hostEnhance security with Chrome Enterprise Premiums shall be locked down to restrict access. The only incoming connection to the physical host shall be for management purposes or to support the virtualisation function. There shall be no outgoing connections except to support virtual workloads. Communication between physical hosts shall be inhibited other than as part of data flows between virtual workloads.	Google builds its own host machines and deploys custom operating system images that only permit the necessary ports, protocols, and services. Google enforces least functionality on machines via a baseline configuration that restricts functionality to only essential capabilities. Google maintains configuration management tools to detect and automatically correct deviations from its baseline configuration. Customers are responsible for configuring their Virtual Machines to provide only essential capabilities; and prohibiting or restricting the use of functions, ports, protocols, and/or services that are not required.	Google infrastructure security design overview
M13.04	Controls shall be in place to ensure that only known physical hosts can be added to the virtualisation fabric.	Google Cloud has developed a purpose-built chip (**TITAN**) to establish a hardware root-of-trust and strong machine identity for all Google Cloud servers. TITAN also enables a secure boot process with cryptographic verification of a known-good firmware/software stack before the machine can be used. Google Cloud **Shielded VMs** extend the secure boot process to customer VMs and provide protection against rootkits, bootkits and kernel-level malware via a vTPM (again, leveraging TITAN). Shielded VMs are enabled by default for all customer VMs. Customer are recommended to enable Secure Boot when configuring VMs. Shielded VMs can be mandated as part of an **Organization Policy**.	Titan in depth: Security in plaintext Hardened virtual machines on Google Cloud Introduction to the Organization Policy Service Google infrastructure security design overview
M13.05	Modification of databases and systems that define the operation of the network shall require two authorised-person sign-off.	Change Management policies, including security code reviews and emergency fixes, are in place, and procedures for tracking, testing approving, and validating changes are documented. Changes are developed utilizing the code versioning tool to manage source code, documentation, release labeling and other functions. Google requires all code changes to be reviewed and approved by a separate technical resource, other than the developer, to evaluate the quality and accuracy of changes. Further, all application and configuration changes are tested prior to migration to production environment. Following successful pass of tests, multiple binaries are then grouped into a release and deployed to production.	Google infrastructure security design overview

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
M13.06	As part of the virtualisation fabric, physically separate ports shall be used to segregate internal and external network traffic.	Customer Virtual Machines can be configured with multiple network interfaces. When using multiple interfaces from an instance, each interface must attach to a different VPC network; you can't attach multiple network interfaces to the same VPC network. This is implemented via the Google SDN. Physical separation of the network interfaces is not guaranteed.	Virtual Private Cloud (VPC) Create VMs with multiple network interfaces
M13.07	The virtualisation fabric shall be configured to limit the exposure of virtual workloads (e.g. disable virtual span ports by default).	By default, Compute Engine VMs are assigned with only internal IP addresses. In this scenario, they can only communicate with other resources in the same project and VPC (virtual network). Customers can also choose to implement External IP addresses for their VMs to enable communication with other resources beyond the VPC. In both cases, the Cloud Firewall should be configured to control network access to the VM. Regarding "virtual span ports", this is assumed to refer to port mirroring. Google Cloud does not implement mirroring at the port level. Packet mirroring can be implemented at the VPC level.	Virtual Private Cloud (VPC) Best practices and reference architectures for VPC design VPC firewall rules Packet Mirroring
M13.08	The virtualisation fabric shall be configured to prevent use of hard-coded MAC addresses by default e.g. by individual VNFs.	Google Cloud does not support configurable or hard-coded MAC addresses. Note that it is possible to maintain a MAC address when a VM is restarted, by keeping the same internal IP address for the network interface (because the MAC address is generated deterministically in software based on the internal IP).	VM instance lifecycle
M13.09	Where providers cannot guarantee the security of the physical environment (e.g. within the exposed edge, or within a shared data centre/exchange), the virtualisation fabric shall be configured to encrypt data at rest (no data is written to the host's storage unencrypted and data is encrypted when the host is powered off).	By default, Google Cloud encrypts all data at rest. This cannot be disabled. There are multiple options for key management. Customers can also choose to add a second layer of encryption if required.	Default encryption at rest Cloud Key Management
M13.10	Where there is risk of exposure during transmission, the virtualisation fabric shall be configured to securely encrypt data in transit. Examples and guidance on the use of encryption can be found on the NCSC website	By default, Google Cloud encrypts all data in transit. Customers can also choose to add a second layer of encryption if required.	Encryption in transit Cloud VPN overview Cloud Load Balancing
M13.11	All physical hosts shall be placed into a host security 'pool'. Pools may be defined based on the environment within which that host resides, the type of host, resilience and diversity, purpose etc.	Google Cloud infrastructure is organized into Regions and Zones. Each zone supports a wide range of machine types. The infrastructure does not assume any trust between the services that are running on the infrastructure. This trust model is referred to as a zero-trust security model. A zero-trust security model means that no devices or users are trusted by default, whether they are inside or outside of the network.	Cloud locations Regions and zones Machine families resource and comparison guide Google infrastructure security design overview
M13.12	Virtual workloads shall be authorised, tagged with a specific trust domain, and signed prior to use. The specific trust domain shall be based on the risks associated with the workload.	Google Cloud resources are managed within a resource hierarchy of organizations, folders and projects. Workloads are also deployed into virtual networks called VPCs. By default, there is a single VPC per customer project, which provides isolation from other customers and other projects. Customers can also choose to configure additional projects and additional VPCs (per project) as required, to further segment their resources within Google Cloud. Security configurations can be applied at various levels within the resource hierarchy, at the VPC level, to specific resources, or to specific users. This is all customer configurable.	Resource hierarchy Virtual Private Cloud (VPC)
M13.13	There shall be separation between trust domains. This separation may be enforced by the virtualisation fabric, provided virtualisation cut-throughs are not used.	By default, VPCs are protected at the network level by a Cloud Firewall and all Google Cloud resources are protected at the API level by default IAM configurations. The infrastructure does not assume any trust between the services that are running on the infrastructure. This trust	VPC firewall rules Identity and Access Management (IAM) VPC Service Controls

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
		model is referred to as a zero-trust security model. A zero-trust security model means that no devices or users are trusted by default, whether they are inside or outside of the network. Google Cloud has many features to refine and enforce the separation and protection of trust domains. The Cloud Firewall and IAM features are highly configurable according to customer needs. The VPC Service Control feature provides a service perimeter for API access (with granular control over who can access resource APIs based on location, IP address and device). This is incremental to IAM protection. Google Cloud also supports a Zero-Trust security architecture via BeyondCorp (to further secure remote access to Google Cloud resources).	Beyondcorp enterprise
M13.14	Host pools shall be tagged with trust domains they can execute. This will be based on risk and ensure that sensitive functions are not executed alongside vulnerable functions, or in physically exposed locations. The virtualisation fabric shall verify that the virtual workload is signed and complies with policy prior to use, including that the virtual workload's trust domain is permitted to execute within the host's pool.	Many Google Cloud products can be configured to operate in specific Regions or Zones. Other products are designed as Multi-Regional or Global, based on the product requirements and architecture. Organization Policies can be used to limit the locations in which resources within an Org, Folder or Project can be deployed (and can also mandate use of Shielded VMs) For more granular control over workload placement (VMs and Containers), customers can also select Sole-Tenancy to get exclusive access to one or more physical compute servers. These can be managed in groups, with control over affinity and anti-affinity for particular workloads. Regarding "signing" of virtual workloads, Binary Authorization can be used to ensure only containers signed by a trusted authority can be deployed within Google Kubernetes Engine or Cloud Run. For Virtual Machines, Google Compute Engine supports both Secure Boot and Measured Boot via Shielded VMs. Attestation of specific applications within a VM environment is a customer responsibility.	Geography and regions Introduction to the Organization Policy Service Sole-tenancy overview Binary Authorization What is Shielded VM?
M13.15	A physical host shall not be able to impact hosts in other host pools. This includes, but is not limited to, spoofing VLAN/VXLANs of virtual networks.	For separation between trust domains, refer to **M13.13.** Regarding VLAN spoofing, each customer VM is allocated to one or more unique VPCs which are fully isolated from each other at the SDN level, preventing any possibility of VLAN spoofing between customers or VPCs.	Virtual Private Cloud (VPC) overview
M13.16	Containers shall not be used to implement separation between trust domains. To implement separation between trust domains, providers shall use Type-1 hypervisors (without cut-throughs) or discrete physical hardware.	Compute Engine VMs run on a physical host, managed via Google's security-hardened, KVM-based hypervisor. This is a Type-1 architecture. In Google Kubernetes Engine (GKE), the worker nodes are Compute Engine VMs that are instantiated by GKE. Customers also have the option to configure Sole-Tenant Nodes if dedicated physical hosts are preferred. Sole-tenant nodes can be used for individual VMs or groups of VMs within a common trust domain. GKE can also be configured to use sole-tenant VMs as the worker nodes.	Compute Engine overview GKE cluster architecture Sole-tenancy overview Isolate your GKE workloads using sole-tenant nodes
M13.17	Containerised hosts shall only support a single trust domain.	This is a customer design choice. Customers can implement tenant isolation at the Container, Pod, Node, Cluster or Project level according to their security requirements, described in a **Google Cloud blog**. Google has also developed **gVisor** as an open-source solution to strengthen container isolation within a specific node. This technology is available within GKE as the **GKE Sandbox**.	Exploring container security: Isolation at different layers of the Kubernetes stack gVisor: Protecting GKE and serverless users in the real world GKE Sandbox
M13.18	The control and orchestration functions for virtualisation are network oversight functions and shall reside in a trusted physical and logical location.	The extensive physical and logical security measures in place within Google Cloud data centers and at all layers of the Google Cloud network stack means that Google Cloud data centers can be considered trusted physical and logical locations (arguably more secure than	Google security overview Google infrastructure security design overview

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
		many on-prem data centers). This principle is well documented by the NCSC in their whitepaper on Security Benefits of Cloud.	Security benefits of a good cloud service (External)
M13.19	The administration network of the virtualisation fabric is a management plane and shall be protected as such.	Refer to **M13.20-M13.26**	N/A
M13.20	Privileged access to the virtualisation fabric shall only be available over authenticated and encrypted channels.	Google has security controls in place to ensure that administrative access to Google Cloud only takes place via authenticated and encrypted channels.	Google infrastructure security design overview
M13.21	Functions that support the administration and security of the virtualisation fabric shall not be run on the fabric it is administering.	Google uses a number of technologies to ensure the isolation of all independent software functions, including security and non-security functions. Isolation and sandboxing techniques are used to protect a service from other services running on the same machine. These techniques include Linux user separation, language and kernel-based sandboxes, and hardware virtualization. In general, Google uses more layers of isolation for high risk workloads. For extra security, sensitive services, such as the cluster orchestration service and some key management services, run exclusively on dedicated machines.	Google infrastructure security design overview
M13.22	Functions that support the administration and security of the virtualisation fabric are network oversight functions and shall reside in a trusted physical and logical location.	Google implements a wide range of physical and logical security measures to ensure that all of its data center locations are considered as trusted physical and logical locations. - Access to our data centers is tightly controlled. We use multiple physical security layers to protect our data center floors. We use biometric identification, metal detection, cameras, vehicle barriers, and laser-based intrusion detection systems. - We design the server boards and the networking equipment. We vet the component vendors that we work with and choose components with care. We work with vendors to audit and validate the security properties that are provided by the components. - We also design custom chips, including a hardware security chip (TITAN), that we deploy on servers, devices, and peripherals. - We implement a zero-trust model where all machines, services and users must prove their identity before any actions are permitted and all actions are controlled on a least-privilege basis. - We encrypt all data in transit and in rest (and optionally in-use). - We implement DDOS protection and intrusion detection for all of our networks and data centers. - We implement a secure software development process via source code governance, version control and binary authorization. - We have dedicated security teams that constantly monitor all of our networks as well as tracking emerging threats and responding to security incidents.	Google security overview Google infrastructure security design overview
M13.23	The number of privileged accounts for the virtualisation fabric shall be constrained to the minimum necessary to meet the provider's needs.	Google has security controls in place to limit and control access to the production network, following the principles of zero trust and least privilege.	Privileged Access Management in Google Cloud Platform
M13.24	Virtualisation fabric administrator accounts shall not have any privileged rights to other services within the provider, or vice-versa.	Google Cloud administrators do not have any privileged rights to other services within the providers network. Any such access would need to be explicitly created by the customer.	N/A
M13.25	Virtualisation fabric administrator accounts shall only be provided with the	Refer to **M13.23** and **M13.24**	N/A

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
	privileges and accesses required to carry out their role.		
M13.26	Virtualisation fabric administrator accounts shall not have access to the provider's workloads running within the virtualised environment.	Google does not have access to customer workloads at the application level. However, Google does have access to the underlying virtualization fabric (compute, storage and networking), as this is required to maintain, secure and troubleshoot Google Cloud services. This is a position of responsibility which Google takes very seriously and which Google approaches via clear operational principles of **security transparency and trust**. For further details, refer to **M10.05**	Creating trust through transparency
M13.27	Network oversight functions shall not share trust domains or host pools with workloads that are not network oversight functions	This is a customer design choice. As noted above, Google enables physical segregation of hosts at the Region, Zone and Node level as well as logical segregation via Projects and VPCs, with a range of related controls such as IAM, Cloud Firewalls and VPC Service Controls.	Enterprise foundations blueprint
M13.28	Containers shall not be used to enforce separation between different network oversight functions and between network oversight functions and other functions.	This is a customer design choice. As noted above, containers within GKE run on worker nodes implemented as Compute Engine VMs.	Security overview
M14.01	Once equipment reaches the vendor's endof-life date, providers shall only continue to use the equipment if the following conditions are met: a) the equipment's configuration is rarely modified, and modifications are reviewed; b) either the addressable interfaces of the unsupported equipment are monitored and use of those interfaces can be explained, or there is no realistic possibility that exploitation of all unsupported equipment would have an impact on the network; and c) the network exposure (attack surface) of the unsupported equipment is minimal (e.g. some transport equipment).	Services that are provided by Google Cloud are supported in line with our terms of service. Customers will be notified well in advance of any Google Cloud services that will be discontinued, as per our standard service terms.	Google Cloud Platform Terms of Service
M14.02	The provider shall block and record any SIM OTA messages sent to their own SIMs, except where these are sent from allowed sources.	Not applicable to Google Cloud.	N/A
M15.01	Network oversight functions shall be robustly locked-down, in support and patched within such period as is proportionate to the risk of security compromise that the patch is intended to address (see Table 2). Should this not be possible, patches shall be deployed on network oversight functions as soon as practicable and robust alternative mitigations put in place until the relevant patch has been deployed.	Refer to **M13.01** & **M8.08**	N/A
M15.02	Any service that supports or contains a network oversight functions shall be rebuilt from an up-to-date known-good software state every 24 months. This includes the operating system and application software. This can be performed in line with a system upgrade.	Google Cloud provides a software-defined and API controlled environment, where services are abstracted from the underlying hardware. It is therefore well suited to the rebuild of customer workloads on demand. **Terraform** and **Cloud Build** can be used to further automate the infrastructure deploy / re-deploy process, using an Infrastructure-as-Code (IaC) approach.	Terraform on Google Cloud documentation Cloud Build Managing infrastructure as code with Terraform, Cloud Build, and GitOps
M15.03	Any workstations or functions (e.g. jump boxes) through which it is possible to make administrative changes to network oversight functions shall be rebuilt from an up-to-date known-good software state on a yearly basis. This applies to the workstation or function's operating systems and above.	The management architecture for 3rd Party Network Oversight Functions is not in Google's control. The 3rd Party can implement PAWs to access NOFs running in Google Cloud.	N/A

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
M15.04	Network oversight functions shall run on trusted platforms.	Refer to **M13.18.**	N/A
M15.05	Where providers cannot guarantee the security of the physical environment (e.g. within the exposed edge, or within a shared data centre/exchange) network oversight functions shall not be deployed.	Google Cloud does not operate services within the Exposed Edge, or within physically shared data center environments or exchange buildings. Google Cloud data centers are dedicated environments with extremely limited access and multiple layers of security protection as described in **M13.18**.	About Google Data Centers
M15.06	Network oversight functions shall only be managed by a minimal set of trusted privileged users.	Refer to **M11.04.**	N/A
M15.07	The management functions (e.g. jump-box) used to manage network oversight functions shall only be accessible from designated PAWs.	Refer to **M15.03.**	N/A
M15.08	Dedicated management functions shall be used to manage network oversight functions.	Refer to **M15.03.**	N/A
M15.09	The management plane used to manage network oversight functions shall be isolated from other internal and external networks, including the management plane used by other equipment.	Refer to **M15.03.**	N/A
M15.10	All management accesses to network oversight functions shall be pre-authorised by a limited set of people who have been assigned with an appropriate role.	Refer to **M11.04.**	N/A
M15.11	Changes to network oversight functions shall be monitored in real-time (e.g. Syslog).	Refer to **M2.02**	N/A
M15.12	The designated PAWs, dedicated management functions and the network oversight functions themselves shall be monitored for signs of exploitation.	Refer to **M11.22**	N/A
M15.13	Network oversight functions shall only access services (e.g. AAA, network time, software updates) over internally-facing interfaces.	3rd Party NOFs running within Google Cloud can reach public Google APIs via internal interfaces using **Private Google Access, Private Google Access for On-Prem Hosts or Private Service Connect**	Private Google Access Private Google Access for on-premises hosts About accessing Google APIs through endpoints
M16.01	Providers shall use appropriately-skilled and dedicated resources to understand and analyse security-related network activity. These resources may be provided by a third party supplier.	Google Cloud can provide customers with skilled and dedicated security resources via **Mandiant Cyber Security Consulting**. Internally, Google also has a highly capable security engineering team that monitors Google Cloud's network.	Mandiant Cybersecurity Consulting Google infrastructure security design overview
M16.02	Providers shall ensure that threat hunting is periodically performed using available logging and monitoring data.	Google Cloud customers can implement cloud-scale threat threat detection and threat hunting (supported by Generative AI and Machine Learning) via **Security Command Center** and **Google Security Operations.** Internally, Google has a highly capable security engineering team that perform Threat Hunting in Google Cloud's network.	Cloud security and risk management for multi-cloud environments Say goodbye to legacy security operations Google infrastructure security design overview
M16.03	Providers may outsource threat hunting to an independent third party, but, if possible, should not outsource audit or threat hunting to any party involved in operating the network.	Google Cloud customers can leverage Mandiant's deep security expertise to carry out threat hunting within Google Security Operations, via **Mandiant Hunt**.	Uncover hidden attacks with elite threat hunters by your side with Mandiant Hunt

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
M16.04	Asset management and network monitoring systems shall be kept up to date to enable security staff to identify and track down anomalies within networks. This shall include comprehensive details of normal system and traffic behaviour (e.g. source and destination, frequency of communication, protocols and ports used, and expected bandwidth consumed).	For Google Cloud's own asset management, refer to **M1.01**. For customer asset management, **Security Command Center** supports **Cloud Asset Inventory** and **Anomaly Detection** (as well as many other security features)	Cloud security and risk management for multi-cloud environments Introduction to Cloud Asset Inventory Detection services
M16.05	Network changes that could impact network security shall be notified to those monitoring the network. Monitoring processes shall be maintained and modified if necessary.	Refer to **M11.01**	N/A
M16.06	Physical and logical interfaces between networks that operate at different trust levels shall be monitored, and between groups of network functions (e.g. core networks and access networks).	Customers can enable **VPC Flow Logs** and/or **Firewall Rule Logs** for additional monitoring of sensitive network interfaces within Google Cloud.	Configure VPC Flow Logs Firewall Rules Logging
M16.07	Systems that collect and process logging and monitoring data shall be treated as network oversight functions.	Refer to the section on **Network Oversight Functions (M15.xx)**	N/A
M16.08	The integrity of logging data shall be protected, and any modification alerted and attributed.	All Google Cloud logs are handled by **Cloud Logging**, which encrypts all logging data at rest (and in transit). Customers can aslo choose to use **Customer Managed Encryption Keys (CMEK)** for Cloud Logging if required. For alerting and attribution, refer to **M16.09**	Configure CMEK for Cloud Logging
M16.09	All actions involving stored logging or monitoring data (e.g. copying, deleting, modification, or viewing) shall be traceable back to an individual user.	Both **Cloud Logging** and **Cloud Monitoring** support **Audit Logs**, which are enabled by default and can't be disabled.	Cloud Logging audit logging Monitoring audit logging
M16.10	Logging datasets shall be synchronised, using common time sources, so separate datasets can be correlated in different ways.	All Google Cloud systems are synchronized by default to **Google Public NTP**. This can also be used by external resources to ensure common time across a Hybrid environment.	Google Public NTP
M16.11	An alarm shall be raised if logs stop being received from any network equipment.	Customers can **configure alerts** based on specific logs being received. Its not possible to create an alert due to logs NOT being received, because its not known in advance when logs should be expected. **Cloud Monitoring** supports a range of **uptime checks** to verify the status of VMs or other customer applications (via heartbeats) and to generate alerts	Configure log-based alerting policies Synthetic monitoring overview
M16.12	Logs for network equipment in security critical functions shall be fully recorded and made available for audit for 13 months.	Google Cloud **Audit Logs** are stored for **400 days** (not configurable). Other logs types are stored for 30 days by default, but this is configurable up to 3650 days.	Quotas and limits
M16.13	Network-based and host-based sensors shall be deployed and run throughout networks to obtain traffic to support security analysis.	Google Cloud supports **Packet Mirroring** at the VPC level. This could be used to send network flows of interest to virtual probes.	Packet Mirroring
M16.14	Access events to network equipment shall be collected. Unauthorised access attempts shall be considered a security event.	Access attempts are captured via **Audit Logs,** which are enabled by default in Google Cloud (and can't be turned off).	Cloud Audit Logs
M16.15	Logging data shall be enriched with other network knowledge and data. In order to successfully analyse logging data it must be used in conjunction with knowledge of the providers' network as well as other pertinent data needed for	All Google Cloud logs are handled by **Cloud Logging**. For native enrichment refer to **M16.17**. Logs can also be exported to other platforms for additional analysis.	Route logs to supported destinations

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
	understanding log entries		
M16.16	Network equipment configurations shall be regularly and automatically collected and audited to detect unexpected changes.	**Audit Logs** can be used to track any unexpected configuration changes.	Cloud Audit Logs
M16.17	Logs shall be linked back to specific network equipment or services.	All Google Cloud logs automatically report the resource that generated the log, including resource type, identity and metadata.	Cloud Logging - LogEntry Cloud Logging - Monitored Resource
M16.18	Logs shall be processed and analysed in near real-time (in any case within 5 minutes) and generate security relevant events.	Google Cloud logs are typically processed and analysed in near real-time (typically within a few seconds)	N/A
M16.19	The provider shall ensure that tools and techniques are utilised to support analysts in understanding the data collected.	Google Cloud provides **Logs Explorer** and **Log Analytics** to help customers understand, query and analyse Cloud Logs.	View logs by using the Logs Explorer Query and view logs in Log Analytics
M16.20	Providers shall regularly review access logs and correlate this data with other access records and ticketed activity.	Refer to **M16.14**	
M16.21	Indications of potential anomalous activity shall be promptly assessed, investigated and addressed.	Google has security controls in place to detect network intrusion, unauthorized network access or unauthorized configuration changes and will respond promptly to any identified security threats. Google Cloud customers can implement cloud-scale threat threat detection and threat hunting (supported by Generative AI and Machine Learning) via **Security Command Cente**r and **Google Security Operations**.	Google infrastructure security design overview
M16.22	Logging data shall be correlated with data within asset management systems to detect anomalies. Models shall be developed to characterise ‘normal’ traffic within networks, including type and volume.	**Google Cloud Monitoring** enables customers to set baselines and create alerts for anomolous conditions. **Security Command Center** supports Cloud Asset Inventory and Anomaly Detection (as well as many other security features) **Cloud Armor Adaptive Protection** uses machine learning to baseline normal traffic patterns and alert on anomolous network activity.	Cloud Monitoring Detection services Google Cloud Armor Adaptive Protection overview
M17.01	Administrators should not need privileged access to network equipment to make administrative changes. Administrators should instead have privileged access to administrative systems (e.g. OSS) which make the necessary changes on the administrator’s behalf. Administrative systems should group administrative changes to automate administrative processes and minimise administrator input and risk. When an administrator uses a privileged access into a security critical function, which is not an administrative system, this shall create a security alert.	Google automates the majority of network deployment, configuration and maintenance activities. Human intervention by Google Cloud admin is a last resort. As noted elsewhere, all customer admin access is logged and customers can also choose to log any Google Cloud admin access. Google Cloud provides tooling and best practice guidelines to help customers automate the deployment and maintenance of customer workloads. Refer to the **Architecture Framework guides on automation**.	Automate your deployments Create a culture of automation
M18.01	The provider shall ensure that their critical, core and signalling security systems are highly resilient to signalling attacks. Signalling messages shall be validated at the logical edge of the network prior to being forwarded to critical or core nodes. Messages that are not encoded in a normal manner, or that are unrelated to a normal operation or call flow in the network, shall be blocked. All exceptions to this shall be understood, justified, and documented.	Not applicable to Google Cloud.	N/A

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
M18.02	A signalling failure for an externally-facing service shall not impact core nodes or security critical functions.	Not applicable to Google Cloud.	N/A
M18.03	With the exception of SS7 and GTP-C, only ‘hub’ signalling addresses shall be exposed externally. This shall be done in such a way that internal signalling addresses of critical core nodes are not shared or exposed externally.	Not applicable to Google Cloud.	N/A
M18.04	Outgoing signalling shall be authenticated where this is supported by international standards.	Not applicable to Google Cloud.	N/A
M18.05	Customer data and customer identifiers shall be obfuscated before being released over an external signalling network, except where it is functionally essential to provide this information.	Not applicable to Google Cloud.	N/A
M19.01	All non-ephemeral secrets, passwords and keys shall be stored in hardware-backed secure storage.Where providers are not able to apply this measure to existing networks and services they must set out what mitigating steps they are taking.	**Cloud KMS** is used to create, store, manage, rotate and revoke security keys, used for encryption-at-rest of customer data within Google Cloud (plus Kubernetes Secrets within etcd). Cloud KMS keys can be protected in hardware via Cloud HSM. Google Cloud also supports **Secret Manager** for secure storage of customer API Keys, Passwords, Certificates and other sensitive data.	Cloud Key Management Cloud HSM Store API keys, passwords, certificates, and sensitive data
M19.02	Only physical hosts that have cryptographically attested to be in a knowngood state can be provisioned into the virtualisation fabric.	Refer to **M13.04**	N/A
M19.03	Where the virtualisation fabric provides a security boundary, it shall not be able to directly access the physical hardware (no cut-throughs).	Compute Engine VMs run on a physical host, managed via Google's **security-hardened, KVM-based hypervisor**. This approach implements full virtualization (not para-virtualization) and supports **standard Guest OS implementations**. Underlying hardware features such as CPU, GPU, Memory & Local Storage are exposed via the hypervisor, but there is no direct access to physical hardware. VM Networking is implemented via Google's **Andromeda SDN**. This uses Intel's DMA Engine for performance reasons but, unlike SR-IOV, this does not tie a VM to a physical machine.	Compute Engine overview Operating system details Google Cloud networking in depth: How Andromeda 2.2 enables high-throughput VMs
M19.04	Where possible, the virtualisation fabric shall be built and updated through an automated and verifiable process.	Regarding the management of Google Cloud by Google: - Google has embraced the principle of automated operations since 2004 via its **SRE practice**, which is widely recognized across the industry. - Google operates a very large global network with a high degree of automation, including a fully software-defined network (**Andromeda**), running over an automated optical data center fabric (**Jupiter**), with automated cluster management and software orchestration system (**Borg**), a global-scale software-defined storage service (**Colossus**), a workload autoscaling system (**Autopilot**) and automated monitoring and remediation of hardware and software faults (various internal tools that are not public). - Google automatically configure all new machines and network devices. - Configurations for machine and network devices are verified by automated configuration management tools to ensure configurations are applied consistently with the identified baselines. Regarding the management of services deployed on Google Cloud (by the customer): - Google makes multiple tools available to customers to assist with automated deployment.	What is Site Reliability Engineering (SRE)? Google Cloud networking in depth: How Andromeda 2.2 enables high-throughput VMs Jupiter evolving: Reflecting on Google’s data center network transformation Large-scale cluster management at Google with Borg Colossus under the hood: a peek into Google’s scalable storage system Google Cloud Deployment Manager documentation Terraform on Google Cloud documentation Basic scenarios for creating managed instance groups (MIGs) Autopilot overview Cloud Composer

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
		- **Terraform** is a recommended method to automate Google Cloud deployments (supported and documented by Google) - Compute Engine **Managed Instance Groups** enables automated fleet management of VMs at scale. - **GKE Autopilot** automates the deployment and management of GKE Clusters. - **Cloud Composer** provides automated workflow orchestration for data pipelines, based on Apache Airflow. - Many Google Cloud services (Cloud Run, Cloud Functions, Pub/Sub, Dataflow, BigQuery etc) are serverless, meaning that all infrastructure is managed transparently without any operational burden on the customer.	
M19.05	Where possible, only automated and verifiable methods of configuration shall be used for administration of the virtualisation fabric (authorised API calls etc).	Regarding the management of Google Cloud infrastructure by Google: - In line with Google's **SRE principles**, the majority of administration tasks required to deploy, maintain, manage and secure Google Cloud are already automated and implemented via secure, internal APIs. - Manual access and configuration is considered to be more error prone and is used only as a last resort. Regarding the management of services deployed on Google Cloud (by the customer): - All Google Cloud services are exposed via **APIs** (they can also be configured via the Cloud Console or via CLI). - Access to these APIs is controlled via **IAM**, backed by **Cloud Identity** - **VPC Service Controls** can also be used to implement a service perimeter for API access. - **BeyondCorp** can be deployed to implement zero-trust remote access via **Identity-Aware Proxy**.	What is Site Reliability Engineering (SRE)? Google Cloud APIs Identity and Access Management (IAM) Cloud Identity VPC Service Controls BeyondCorp Identity-Aware Proxy
M19.06	Where possible, administration of the virtualisation fabric shall be automated during normal operation.	Regarding the management of Google Cloud infrastructure, Google has developed automated systems for many administrative tasks. Regarding the management of services deployed on Google Cloud (by the customer): - Google makes multiple tools available to customers to help them automate in-life operations. - **Cloud Operations** provides a full suite of logging, monitoring, auditing, tracing, debugging and application profiling tools. - **Cloud Operations** can be integrated with a wide range of 3rd-party tooling (Prometheus, Grafana, ELK, Splunk, Datadog etc) - Google provides documentation, tutorials, tooling and (if required) professional services to help customers implement SRE principles within their own operational model.	Google Cloud's Observability Site Reliability Engineering (SRE)
M19.07	Manual administration of the virtualisation fabric (e.g. access to a command line on host infrastructure) shall produce an immediate alert	As noted above, the majority of Google administration of Google Cloud is already automated and manual access is an exception. Additionally, Google has security controls in place to detect network intrusion, unauthorized network access or unauthorized configuration changes. Customers have the option to enable the following features for additional visibility and control over Google admin access to their services. - **Access Transparency** (logging of all Google Admin access) - **Access Approval** (customer approval for all Google Admin access)	Google infrastructure security design overview Access Transparency Access Approval documentation

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
M20.01	Automated tools shall be used to find and prioritise events that require manual analysis.	Native features within Cloud Logging include **Logs Explorer** (to help you troubleshoot and analyze the performance of your services and applications) and **Log Analytics** (to run queries that analyze your log data). Logs can also be exported to other tools such as **BigQuery** for more complex analytics. Google Cloud customers can implement cloud-scale threat threat detection and threat hunting (supported by Generative AI and Machine Learning) via **Security Command Center** and **Google Security Operations**.	Query and view logs overview View logs routed to BigQuery Cloud security and risk management for multi-cloud environments Modern SecOps
M21.01	Procedures should ensure contingencies are in place in the event that further locations are added to the Schedule of the Electronic Communications (Security Measures) Regulations.	Google Cloud limits access from embargoed and restricted locations. Additionally, Google Cloud customers can use **Context Aware Access** to implement configurable geo-location access restrictions, that are policed via **BeyondCorp** and **VPC Service Controls**.	Access Context Manager Overview
M21.02	The measures to be taken by the provider under Regulation 3(3)(f) should normally include ensuring, so far as is reasonably practicable, that the equipment performing provider's network oversight functions is located within the UK, and operated using UK-based staff.	The majority of Google Cloud services can be configured as **Regional** services within the UK, with support for **Data Residency**. Some Google Cloud services are **Multi-Regional** or **Global.** Google maintains an **SRE** (operational support) team in the UK but operates a global support model to ensure 24/7 cover for all Google Cloud services.	Products available by location (Europe) Products available by location (multi-region) Google Cloud Platform Services with Data Residency SecOps Services Locations Page What is Site Reliability Engineering (SRE)?
M21.03	The provider shall retain a UK-based technical capability to provide subject matter expertise on the operation of the provider's UK networks and the risks to the provider's UK networks.	Google Cloud provides extensive customer training options to enable our customers to build up Google Cloud expertise as required. Google maintains an **SRE** (operational support) team in the UK but operates a global support model to ensure 24/7 cover for all Google Cloud services.	Google Cloud Training and Certification What is Site Reliability Engineering (SRE)?
M21.04	Where data is stored offshore, the provider shall maintain a list of locations where the data is held. The risk due to holding the data in these locations, including any risk associated with local data protection law, shall be managed as part of the provider's risk management processes.	The majority of Google Cloud services can be deployed and operated within the UK (as UK **Regional** services), with support for **Data Residency**. Google Cloud has also announced a major investment in a **new UK data center**. Google Cloud documents other potential data storage locations and related terms in the **Cloud Data Processing Addendum**.	Products available by location (Europe) Google Cloud Platform Services with Data Residency Our $1 billion investment in a new UK data centre Cloud Data Processing Addendum
M21.05	Decisions about holding outside of the UK data relating to more than 100,000 UK subscribers, the operation of the large parts of the network, or the operation of network oversight functions, shall be taken at an appropriate governance level and recorded in writing. The sign-off for these decisions should normally be given by a person or committee at board level (or equivalent).	Google Cloud assumes this measure is applicable to providers only (no flow down to suppliers).	N/A
M21.06	If it should become necessary to do so, the provider shall have the ability to maintain (as relevant, where it provides such a form of connectivity prior to the event) the following UK network connectivity for a period of one month in the event of loss of international connections: fixed and mobile data connectivity to UK peering points; mobile voice; and text-based mobile messaging	Google Cloud embeds redundancy as part of its architecture and provides multiple levels of resilience and failover, to help protect customers from data loss. For example, Google Cloud services are abstracted from the underlying hardware using virtualization technologies and may therefore exceed traditional component reliability. Google also has access to multiple redundant fixed networks as well as satellite connectivity. Google Cloud provides strong support for business continuity across Google Cloud's operations, with our data centers being certified against ISO 22301.	ISO 22301:2019 & BS EN ISO 22301:2019 Google Cloud Architecture Framework: Reliability Google Cloud infrastructure reliability guide bookmark_border Architecting disaster recovery for cloud infrastructure outages.

UK Telecommunications Security Code Of Practice

Google Cloud Compliance Guide (IaaS/PaaS)

Measure	Description	Google Cloud Commentary	Google Cloud Reference
		Under the shared responsibility model, customers are also responsible for architectural decisions that can impact availability. Google Cloud provides customers with a Reliability Architecture Framework plus guidance on how to architect for Disaster Recovery considering potential cloud infrastructure outages, including both zonal and regional outages. Google Cloud provides operational SLAs for its platform services. However, these SLAs exclude "factors outside of Google's reasonable control".	Google Cloud Platform Service Level Agreements
M21.07	If it should become necessary to do so, the provider shall be able to transfer into the UK functions required by UK networks to maintain an operational service, should international bearers fail.	Refer to **M21.06**	N/A