EBA Outsourcing Guidelines

Google Cloud Platform Mapping

This document is designed to help financial institutions within the scope of the European Banking Authority's mandate ("**institutions**") to consider the Guidelines on Outsourcing Arrangements (the "**EBA Outsourcing Guidelines**") in the context of Google Cloud Platform ("**GCP**") and the Google Cloud Financial Services Contract.

We focus on Section 13 (Contractual Phase) of the EBA Outsourcing Guidelines. For each paragraph of Section 13, we provide commentary to help you understand how you can address the guidelines using the Google Cloud services and the Google Cloud Financial Services Contract.

The EBA Outsourcing Guidelines replace the Committee of European Banking Supervisors (CEBS) guidelines on outsourcing that were issued in 2006. They also replace the EBA's Recommendations on Outsourcing to Cloud Service Providers published in 2018.

If you have an existing Google Cloud contract and would like to understand how this document applies to your contract, please contact your Google Cloud account representative.

#	EBA Outsourcing Guidelines	Google Cloud Commentary	Google Cloud Financial Services Contract ref.
1.	**13 Contractual phase**		
2.	74. The rights and obligations of the institution, the payment institution and the service provider should be clearly allocated and set out in a written agreement	The rights and obligations of the parties are set out in the Google Cloud Financial Services Contract.	N/A
3.	75. The outsourcing agreement for critical or important functions should set out at least:		
4.	a. a clear description of the outsourced function to be provided;	The GCP services are described here.	Definitions
5.	b. the start date and end date, where applicable, of the agreement and the notice periods for the service provider and the institution or payment institution;	Refer to your Google Cloud Financial Services Contract.	Term and Termination
6.	c. the governing law of the agreement;	Refer to your Google Cloud Financial Services Contract.	Governing Law
7.	d. the parties' financial obligations;	Refer to your Google Cloud Financial Services Contract.	Payment Terms
8.	e. whether the sub-outsourcing of a critical or important function, or material parts thereof, is permitted and, if so, the conditions specified in Section 13.1 that the sub-outsourcing is subject to;	Refer to the comments on Section 13.1 at rows 21 to 35.	Refer to rows 21 to 35.
9.	f. the location(s) (i.e. regions or countries) where the critical or important function will be provided and/or where relevant data will be kept and processed, including the possible storage location, and the conditions to be met, including a requirement to notify the institution or payment institution if the service provider proposes to change the location(s);	Locations To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities. ● Information about the location of Google's facilities and where individual GCP services can be deployed is available here. ● Information about the location of Google's subprocessors' facilities is available here. Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In	Data Transfers (Data Processing and Security Terms) Data Security; Subprocessors (Data Processing

		particular: ● The same robust security measures apply to all Google facilities, regardless of country / region. ● Google makes the same commitments about all its subprocessors, regardless of country / region. Conditions Google provides you with choices about where to store your data - including a choice to store your data in Europe. Once you choose where to store your data, Google will not store it outside your chosen region(s). You can also choose to set up a Resource Locations policy that constrains the location of new GCP resources for your whole organization or individual projects. More information is available here. In addition, Google provides commitments to enable the lawful transfer of personal data to a third country in accordance with European data protection law.	and Security Terms) Data Location (Service Specific Terms) Data Transfers (Data Processing and Security Terms)
10.	g. where relevant, provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data, as specified in Section 13.2;	Refer to the comments on Section 13.2 at rows 36 to 40.	Refer to rows 36 to 40.
11.	h. the right of the institution or payment institution to monitor the service provider's performance on an ongoing basis;	You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: ● The **Status Dashboard** provides status information on the Services. ● **Google Stackdriver** is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP. ● **Access Transparency** is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location).	Ongoing Performance Monitoring

12.	i. the agreed service levels, which should include precise quantitative and qualitative performance targets for the outsourced function to allow for timely monitoring so that appropriate corrective action can be taken without undue delay if the agreed service levels are not met;	The SLAs are available here.	Services
13.	j. the reporting obligations of the service provider to the institution or payment institution, including the communication by the service provider of any development that may have a material impact on the service provider's ability to effectively carry out the critical or important function in line with the agreed service levels and in compliance with applicable laws and regulatory requirements and, as appropriate, the obligations to submit reports of the internal audit function of the service provider;	Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available here. In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our whitepaper.	Significant Developments Data Incidents (Data Processing and Security Terms)
14.	k. whether the service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;	Google will maintain insurance cover against a number of identified risks.	Insurance
15.	l. the requirements to implement and test business contingency plans;	Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. In addition, information about how customers can use our Services in their own business contingency planning is available here.	Business Continuity and Disaster Recovery
16.	m. provisions that ensure that the data that are owned by the institution or payment institution can be accessed in the case of the insolvency, resolution or discontinuation of business operations of the service provider;	You retain all intellectual property rights in your data. Google will enable you to access and export your data throughout the duration of our contract. Refer to row 75. Neither of these commitments are disapplied on Google's insolvency. Nor does Google have the right to terminate for Google's own insolvency - although you can elect to terminate. In the unlikely event of Google's insolvency, you can refer to these commitments when dealing with the appointed insolvency practitioner.	Intellectual Property Data Export (Data Processing and Security Terms) Term and Termination
17.	n. the obligation of the service provider to cooperate with the competent authorities and resolution authorities of the institution or payment institution, including other persons appointed by them;	Google will cooperate with competent authorities and resolution authorities exercising their audit, information and access rights.	Enabling Customer Compliance
18.	o. for institutions, a clear reference to the national resolution authority's powers, especially to Articles 68 and 71 of Directive 2014/59/EU (BRRD), and in particular a description of the 'substantive obligations' of the contract in the sense of Article 68 of that Directive;	Google recognizes that institutions and any resolution entity must be able to carry on business during resolution. To provide support through resolution, Google commits to continue providing the Services during resolution as required by the BRRD.	Support through Resolution

19.	p. the unrestricted right of institutions, payment institutions and competent authorities to inspect and audit the service provider with regard to, in particular, the critical or important outsourced function, as specified in Section 13.3;	Refer to the comments at Section 13.3 at rows 41 to 66.	Refer to rows 41 to 66.
20.	q. termination rights, as specified in Section 13.4.	Refer to the comments at Section 13.4 at rows 67 to 77.	Refer to rows 67 to 77.
21.	**13.1 Sub-outsourcing of critical or important functions**		
22.	76. The outsourcing agreement should specify whether or not sub-outsourcing of critical or important functions, or material parts thereof, is permitted.	Google recognizes that institutions need to consider the risks associated with sub-outsourcing. We also want to provide you and all our customers with the most reliable, robust and resilient service that we can. In some cases there may be clear benefits to working with other trusted organizations e.g. to provide 24/7 support. Although Google will provide you with information about the organizations that we work with, we cannot agree that we will never sub-outsource. Given the one-to-many nature of our service, if we agreed with one customer that we would not sub-outsource, we would potentially be denying all our customers the benefit motivating the sub-outsourcing. To ensure institutions retain oversight of any sub-outsourcing, Google will comply with clear conditions designed to provide transparency and choice. Refer to row 26.	Subcontracting
23.	77. If sub-outsourcing of critical or important functions is permitted, institutions and payment institutions should determine whether the part of the function to be sub-outsourced is, as such, critical or important (i.e. a material part of the critical or important function) and, if so, record it in the register.	The institution is best placed to decide if a sub-outsourced function is a material part of a critical or important function. To assist, Google will provide all the information required in the outsourcing register for each of our subcontractors.	Google Subcontractors
24.	78. If sub-outsourcing of critical or important functions is permitted, the written agreement should:		
25.	a. specify any types of activities that are excluded from sub-outsourcing;	Refer to row 22.	Refer to row 22.
26.	b. specify the conditions to be complied with in the case of sub-outsourcing;	To enable institutions to retain oversight of any sub-outsourcing and provide choices about the services institutions use, Google will: ● provide information about our subcontractors; ● provide advance notice of changes to our subcontractors; and ● give institutions the ability to terminate if they have concerns about a new subcontractor.	Google Subcontractors
27.	c. specify that the service provider is obliged to oversee those services that it has subcontracted to ensure that all contractual obligations between the service provider and the institution or payment institution are continuously met;	Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you.	Google Subcontractors

28.	d. require the service provider to obtain prior specific or general written authorisation from the institution or payment institution before sub-outsourcing data;	Google will comply with our obligations under the GDPR regarding authorization for subprocessing.	Processing of Data; Subprocessors (Data Processing and Security Terms)
29.	e. include an obligation of the service provider to inform the institution or payment institution of any planned sub-outsourcing, or material changes thereof, in particular where that might affect the ability of the service provider to meet its responsibilities under the outsourcing agreement. This includes planned significant changes of subcontractors and to the notification period; in particular, the notification period to be set should allow the outsourcing institution or payment institution at least to carry out a risk assessment of the proposed changes and to object to changes before the planned sub-outsourcing, or material changes thereof, come into effect;	You need enough time from being informed of a subcontractor change to perform a meaningful risk assessment before the change comes into effect. To ensure you have the time you need, Google provides advance notice before we engage a new subcontractor or change the function of an existing subcontractor.	Google Subcontractors
30.	f. ensure, where appropriate, that the institution or payment institution has the right to object to intended sub-outsourcing, or material changes thereof, or that explicit approval is required;	Institutions have the choice to terminate our contract if they think that a subcontractor change materially increases their risk. Refer to row 31. However, given the one-to-many nature of our service, if we agreed that one customer could veto a sub-outsourcing, we would potentially allow a single customer to deny all our customers the benefit motivating the sub-outsourcing. The European Banking Authority recognizes that consent is "overly burdensome" in the cloud outsourcing context. See the comment at page 24 of the Final Report of the European Banking Authority's Recommendations on Outsourcing to Cloud Service Providers.	Google Subcontractors
31.	g. ensure that the institution or payment institution has the contractual right to terminate the agreement in the case of undue sub-outsourcing, e.g. where the sub-outsourcing materially increases the risks for the institution or payment institution or where the service provider sub-outsources without notifying the institution or payment institution.	Institutions should have a choice about the parties who provide services to them. To ensure this, institutions have the choice to terminate our contract if they think that a subcontractor change materially increases their risk or if they do not receive the agreed notice.	Google Subcontractors
32.	79. Institutions and payment institutions should agree to sub-outsourcing only if the subcontractor undertakes to:		
33.	a. comply with all applicable laws, regulatory requirements and contractual obligations; and	Google requires our subcontractors to meet the same high standards that we do. In particular, Google requires our subcontractors to comply with our contract with you and applicable law and regulation.	Google Subcontractors
34.	b. grant the institution, payment institution and competent authority the same contractual rights of access and audit as those granted by the service provider.	Sub-outsourcing must not reduce the institution's ability to oversee the service or the competent authority's ability to supervise the institution. To preserve this, Google will ensure our subcontractors comply with the information, access and audit rights we provide to institutions and competent authorities.	Google Subcontractors

35.	80. Institutions and payment institutions should ensure that the service provider appropriately oversees the sub-service providers, in line with the policy defined by the institution or payment institution. If the sub-outsourcing proposed could have material adverse effects on the outsourcing arrangement of a critical or important function or would lead to a material increase of risk, including where the conditions in paragraph 79 would not be met, the institution or payment institution should exercise its right to object to the sub-outsourcing, if such a right was agreed, and/or terminate the contract.	Refer to row 27, row 30 and row 31.	Refer to row 27, row 30 and row 31.
36.	**13.2 Security of data and systems**		
37.	81. Institutions and payment institutions should ensure that service providers, where relevant, comply with appropriate IT security standards.	Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: ● ISO/IEC 27001:2013 (Information Security Management Systems) ● ISO/IEC 27017:2015 (Cloud Security) ● ISO/IEC 27018:2014 (Cloud Privacy) ● PCI DSS ● SOC 1 report ● SOC 2 report ● SOC 3 report	Certifications and Audit Reports
38.	82. Where relevant (e.g. in the context of cloud or other ICT outsourcing), institutions and payment institutions should define data and system security requirements within the outsourcing agreement and monitor compliance with these requirements on an ongoing basis.	The security of a cloud service consists of two key elements: Security of Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers. Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis. More information is available at: ● Our infrastructure security page ● Our security whitepaper ● Our infrastructure security design overview page	Data Security; Security Measures (Data Processing and Security Terms)

		• Our security resources page In addition, you can review Google's SOC 2 report. Refer to row 37. Security of your data and applications in the cloud You define the security of your data and applications in the cloud. This refers to the security measures that you choose to implement and operate when you use the Services. (a) Security by default Although we want to offer you as much choice as possible when it comes to your data, the security of your data is of paramount importance to Google and we take the following proactive steps to assist you: • **Encryption at rest.** Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available at: https://cloud.google.com/security/encryption-at-rest/default-encryption. • **Encryption in transit.** Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available at https://cloud.google.com/security/encryption-in-transit. (b) Security products In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available here. Here are some examples: • **Cloud Identity and Access Management** helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud Platform resources. • **Cloud Security Scanner** automatically scans App Engine, Compute Engine, and Google Kubernetes Engine apps for common vulnerabilities.	

		● **Event Threat Detection** automatically scans various types of logs for suspicious activity in your Google Cloud Platform environment. ● **Cloud Security Command Center** and **Security Health Analytics** provide visibility and monitoring of Google Cloud Platform resources and changes to resources including VM instances, images, and operating systems. ● **Forseti** is an open source toolkit designed to help give your security teams the confidence and peace of mind that they have the appropriate security controls in place across our services. Forseti includes the following security tools: ○ Inventory: provides visibility into existing GCP resources ○ Scanner: validates access control policies across GCP resources ○ Enforcer: removes unwanted access to GCP resources ○ Explain: analyzes who has what access to GCP resources. For more information, see here. ● **Shielded VMs** enable live measurement, monitoring, and alerting for any changes of the full stack. (c) Security resources Google also publishes guidance on: ● Security best practices ● Security use cases	
39.	83. In the case of outsourcing to cloud service providers and other outsourcing arrangements that involve the handling or transfer of personal or confidential data, institutions and payment institutions should adopt a risk-based approach to data storage and data processing location(s) (i.e. country or region) and information security considerations.	This is a customer consideration. Refer to row 9 for more information on data location.	N/A
40.	84. Without prejudice to the requirements under the Regulation (EU) 2016/679, institutions and payment institutions, when outsourcing (in particular to third countries), should take into account differences in national provisions regarding the protection of data. Institutions and payment institutions should ensure that the outsourcing agreement includes the obligation that the service provider protects confidential, personal or otherwise sensitive information and complies with all legal	The security of the Services is fundamental to protecting your data. This is described in the Data Processing and Security Terms. Refer to row 37 and 38 for more information on security. See our GDPR resource center for more information.	Confidentiality; Data Security (Data Processing and Security Terms)

	requirements regarding the protection of data that apply to the institution or payment institution (e.g. the protection of personal data and that banking secrecy or similar legal confidentiality duties with respect to clients' information, where applicable, are observed).		
41.	**13.3 Access, information and audit rights**		
42.	85. Institutions and payment institutions should ensure within the written outsourcing arrangement that the internal audit function is able to review the outsourced function using a risk-based approach.	Google recognizes that using our Services should not impair an institution's (or their competent authority's) ability to oversee and supervise compliance with applicable laws and regulations as well as an institution's internal policies. We will provide institutions with the assistance they need to review our Services.	Enabling Customer Compliance
43.	86. Regardless of the criticality or importance of the outsourced function, the written outsourcing arrangements between institutions and service providers should refer to the information gathering and investigatory powers of competent authorities and resolution authorities under Article 63(1)(a) of Directive 2014/59/EU and Article 65(3) of Directive 2013/36/EU with regard to service providers located in a Member State and should also ensure those rights with regard to service providers located in third countries.	Google acknowledges the information gathering and investigatory powers under the relevant EU Directives.	Enabling Customer Compliance
44.	87. With regard to the outsourcing of critical or important functions, institutions and payment institutions should ensure within the written outsourcing agreement that the service provider grants them and their competent authorities, including resolution authorities, and any other person appointed by them or the competent authorities, the following:	Google grants audit, access and information rights to institutions, competent authorities (including resolution authorities) and both their appointees.	Regulator Information, Audit and Access; Customer Information, Audit and Access
45.	a. full access to all relevant business premises (e.g. head offices and operation centres), including the full range of relevant devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the service provider's external auditors ('access and information rights'); and	Refer to row 44.	Refer to row 44.
46.	b. unrestricted rights of inspection and auditing related to the outsourcing arrangement ('audit rights'), to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements.	Refer to row 44.	Refer to row 44.
47.	88. For the outsourcing of functions that are not critical or important, institutions and payment institutions should ensure the access and audit rights as set out in paragraph 87 (a) and (b) and Section 13.3, on a risk-based approach, considering the nature of the outsourced function and the related operational and reputational risks,	Google recognizes that use of the Services could scale up over time. Regardless of how institutions choose to use the Services at the start of our relationship, Google will provide institutions and competent authorities with audit, access and information rights.	Enabling Customer Compliance

	its scalability, the potential impact on the continuous performance of its activities and the contractual period. Institutions and payment institutions should take into account that functions may become critical or important over time.		
48.	89. Institutions and payment institutions should ensure that the outsourcing agreement or any other contractual arrangement does not impede or limit the effective exercise of the access and audit rights by them, competent authorities or third parties appointed by them to exercise these rights.	Nothing in our contract is intended to limit or impede an institution's or the competent authority's ability to audit our services effectively. In particular, although we will make a lot of information and tools available to help institutions review our Services, our contract does not contain pre-defined steps before institutions or competent authorities can approach Google to exercise their audit, access and information rights. In other words, there is no hierarchy amongst the options for assessing our Services.	Enabling Customer Compliance
49.	90. Institutions and payment institutions should exercise their access and audit rights, determine the audit frequency and areas to be audited on a risk-based approach and adhere to relevant, commonly accepted, national and international audit standards.	The institution is best placed to decide what audit frequency and scope is right for their organization. Our contract does not limit institutions to a fixed number of audits or a pre-defined scope.	Customer Information, Audit and Access
50.	91. Without prejudice to their final responsibility regarding outsourcing arrangements, institutions and payment institutions may use:		
51.	a. pooled audits organised jointly with other clients of the same service provider, and performed by them and these clients or by a third party appointed by them, to use audit resources more efficiently and to decrease the organisational burden on both the clients and the service provider;	Google recognizes the benefits of pooled audits. We would be happy to discuss this with institutions.	N/A
52.	b. third-party certifications and third-party or internal audit reports, made available by the service provider.	Refer to row 37.	Refer to row 37.
53.	92. For the outsourcing of critical or important functions, institutions and payment institutions should assess whether third-party certifications and reports as referred to in paragraph 91(b) are adequate and sufficient to comply with their regulatory obligations and should not rely solely on these reports over time.	This is a customer consideration.	N/A
54.	93. Institutions and payment institutions should make use of the method referred to in paragraph 91(b) only if they:		
55.	a. are satisfied with the audit plan for the outsourced function;	Refer to row 37. Google is audited at least once a year for each audited framework. Google performs planning, scoping and readiness activities prior to each audit.	Certifications and Audit Reports
56.	b. ensure that the scope of the certification or audit report covers the systems (i.e. processes, applications, infrastructure, data centres, etc.) and key controls identified by the institution or payment institution and the compliance with relevant regulatory requirements;	Refer to row 37. Google's audit scope covers in scope Services, infrastructure systems, policies and procedures, common processes and personnel. Google is audited on our security and	Certifications and Audit Reports

		privacy controls covering the relevant certifications and audit reports for the audit scope.	
57.	c. thoroughly assess the content of the certifications or audit reports on an ongoing basis and verify that the reports or certifications are not obsolete;	Refer to row 37. You can review Google's current certifications and audit reports at any time. ● Google's **ISO certifications** are available here. ● Google's **SOC reports** and **PCI Attestation of Compliance (AOC)** are available via your Google Cloud account representative.	Certifications and Audit Reports
58.	d. ensure that key systems and controls are covered in future versions of the certification or audit report;	Refer to row 37. As part of Google's routine planning, scoping, and readiness activities, recurring key systems and controls, as well as new systems and controls, are reviewed prior to the audit work commencing.	Certifications and Audit Reports
59.	e. are satisfied with the aptitude of the certifying or auditing party (e.g. with regard to rotation of the certifying or auditing company, qualifications, expertise, reperformance/verification of the evidence in the underlying audit file);	Refer to row 37. Google engages certified and independent third party auditors for each audited framework. Refer to the relevant certification or audit report for information on the certifying or auditing party.	Certifications and Audit Reports
60.	f. are satisfied that the certifications are issued and the audits are performed against widely recognised relevant professional standards and include a test of the operational effectiveness of the key controls in place;	Refer to row 37. Audits include testing of operational effectiveness of key controls in place.	Certifications and Audit Reports
61.	g. have the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls; the number and frequency of such requests for scope modification should be reasonable and legitimate from a risk management perspective; and	To ensure that they remain an effective tool, if a key system or control for a Service is not covered by Google's certifications or audit reports for that service, institutions can request an expansion of the scope.	Certifications and Audit Reports
62.	h. retain the contractual right to perform individual audits at their discretion with regard to the outsourcing of critical or important functions.	Institutions always retain the right to conduct an audit. The contract does not contain pre-defined steps before institutions can approach Google to exercise their audit, access and information rights. In other words, there is no hierarchy amongst the options for assessing our Services.	Customer Information, Audit and Access
63.	94. In line with the EBA Guidelines on ICT risk assessment under the SREP, institutions should, where relevant, ensure that they are able to carry out security penetration testing to assess the effectiveness of implemented cyber and internal ICT security	You can perform penetration testing of the Services at any time without Google's prior approval.	Customer Penetration Testing

	measures and processes. Taking into account Title I, payment institutions should also have internal ICT control mechanisms, including ICT security control and mitigation measures.		
64.	95. Before a planned on-site visit, institutions, payment institutions, competent authorities and auditors or third parties acting on behalf of the institution, payment institution or competent authorities should provide reasonable notice to the service provider, unless this is not possible due to an emergency or crisis situation or would lead to a situation where the audit would no longer be effective.	Reasonable notice enables Google to deliver an effective audit. For example, we can ensure the relevant Google experts are available and prepared to make the most of your time. Notice also enables Google to plan the audit so that it does not create undue risk to your environment or that of any other Google customer. Google recognizes that in some cases extended notice is not possible. In these cases we will work with the auditing party to address their needs.	Arrangements
65.	96. When performing audits in multi-client environments, care should be taken to ensure that risks to another client's environment (e.g. impact on service levels, availability of data, confidentiality aspects) are avoided or mitigated.	It is extremely important to Google that what we do with one customer should not put any other customers at risk. This applies when you perform an audit. It also applies when any other customer performs an audit. When an institution performs an audit we will work with them to minimize the disruption to our other customers. Just as we will work with another auditing customer to minimize the disruption to the institution. In particular, we will be careful to comply with our security commitments at all times.	Arrangements
66.	97. Where the outsourcing arrangement carries a high level of technical complexity, for instance in the case of cloud outsourcing, the institution or payment institution should verify that whoever is performing the audit – whether it is its internal auditors, the pool of auditors or external auditors acting on its behalf – has appropriate and relevant skills and knowledge to perform relevant audits and/or assessments effectively. The same applies to any staff of the institution or payment institution reviewing third-party certifications or audits carried out by service providers.	This is a customer consideration.	N/A
67.	**13.4 Termination rights**		
68.	98. The outsourcing arrangement should expressly allow the possibility for the institution or payment institution to terminate the arrangement, in accordance with applicable law, including in the following situations:	Institutions can elect to terminate our contract for convenience, including if necessary to comply with law, if directed by the competent authority or in any of the scenarios listed in Section 13.4.	Termination for Convenience
69.	a. where the provider of the outsourced functions is in a breach of applicable law, regulations or contractual provisions;	Refer to row 68.	Refer to row 68.
70.	b. where impediments capable of altering the performance of the outsourced function are identified;	Refer to row 68.	Refer to row 68.

71.	c. where there are material changes affecting the outsourcing arrangement or the service provider (e.g. sub-outsourcing or changes of sub-contractors);	Refer to row 68.	Refer to row 68.
72.	d. where there are weaknesses regarding the management and security of confidential, personal or otherwise sensitive data or information; and	Refer to row 68.	Refer to row 68.
73.	e. where instructions are given by the institution's or payment institution's competent authority, e.g. in the case that the competent authority is, caused by the outsourcing arrangement, no longer in a position to effectively supervise the institution or payment institution.	Refer to row 68.	Refer to row 68.
74.	99. The outsourcing arrangement should facilitate the transfer of the outsourced function to another service provider or its re-incorporation into the institution or payment institution. To this end, the written outsourcing arrangement should:		
75.	a. clearly set out the obligations of the existing service provider, in the case of a transfer of the outsourced function to another service provider or back to the institution or payment institution, including the treatment of data;	Google will enable you to access and export your data throughout the duration of our contract. You can export your data from the Services in a number of industry standard formats. For example: • **Google Kubernetes Engine** is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. • **Migrate for Anthos** allows you to move and convert workloads directly into containers in Google Kubernetes Engine. • You can export/import an entire VM image in the form of a .tar archive. Find more information on images here and on storage options here.	Data Export (Data Processing and Security Terms)
76.	b. set an appropriate transition period, during which the service provider, after the termination of the outsourcing arrangement, would continue to provide the outsourced function to reduce the risk of disruptions; and	Google recognizes that institutions need to be able to exit our Services without undue disruption to their business, without limiting their compliance with regulatory requirements and without any detriment to the continuity and quality of their service to their own clients. To help institutions achieve this, upon request, Google will continue to provide the Services for 12 months beyond the expiry or termination of the contract.	Transition Term
77.	c. include an obligation of the service provider to support the institution or payment institution in the orderly transfer of the function in the event of the termination of the outsourcing agreement.	Our Services enable you to transfer your data independently. You do not need Google's permission to do this. Refer to row 75. However, if an institution would like support, upon request, Google will provide advisory and implementation services to assist in migrating workloads or otherwise transitioning use of the Services.	Transition Assistance