# Danish FSA - Executive Order 877 on outsourcing for credit institutions

## Google Cloud Platform Mapping

This document is designed to help entities supervised by the Danish Financial Supervisory Authority or 'Finanstilsynet' ("**regulated entity**") to consider Executive Order 877 of 12 June 2020 (the "**framework**") in the context of Google Cloud Platform ("**GCP**") and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: Section 6 - Further outsourcing, Section 14 - Contingency plans, Section 17 - Exit strategies, Section 18 - Outsourcing of authorised processes, services or activities, Section 19 - Risk assessment when using outsourcing, Section 20 - Previous examination, Section 21 - Outsourcing contract, Section 22 - Data protection and IT-related outsourcing, Section 23 and 24 - Monitoring and control, Section 26 - Use of joint audits with other supplier customers, Section 27 - Use of internal audit reports, third-party certifications and third-party audit reports provided by the supplier, Annex 2 - Outsourcing register, paragraph 2 and Annex 3 - Requirements for the outsourcing contract. For each paragraph, we provide commentary to help you understand how you can address the requirements using the Google Cloud services and the Google Cloud Financial Services Contract.

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| **Section 6 - Further outsourcing** | | | |
| 1. | When outsourcing critical or important outsourcing to a subcontractor, the outsourcing company must ensure that there is a written contract between the supplier and the subcontractor that obliges the subcontractor to comply with applicable legislation, regulatory requirements and contractual obligations. | 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. | Google Subcontractors |
| 2. | Subsection 2. The contract, cf. Section 1, shall give the outsourcing company, a third party designated by the outsourcing company and the Danish Financial Supervisory Authority the same rights to access and audit as stated in Section 21, Subsections 4 and 5. | Google recognizes that subcontracting must not reduce the regulated entity's ability to oversee the service or the supervisory authority's ability to supervise the regulated entity. To preserve this, Google will ensure our subcontractors comply with the information, access and audit rights we provide to regulated entities and supervisory authorities.<br><br>Refer to Row 41 and Rows 111 to 115 for information about the audit, access and information rights Google grants to regulated entities and supervisory authorities | Google Subcontractors |
| 3. | Subsection 3. The outsourcing company must terminate the outsourcing contract or parts thereof with the supplier, or exercise its right to oppose further outsourcing, in case such right is agreed, if the proposed further outsourcing or change to existing further outsourcing has significant negative effects on the critical or important outsourcing, or will lead to a significant increase in the risk, or if the contractual requirements laid down in Subsections 1 and 2, are not complied with. | Regulated entities should have a choice about the parties who provide services to them. To ensure this, regulated entities 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 |
| **Section 14 - Contingency plans** | | | |
| 4. | The outsourcing company must prepare, maintain and regularly test contingency plans with regard to critical or important outsourcing. | Information about how regulated entities can use our Services in their own contingency planning is available in our Disaster Recovery Planning Guide.<br><br>In particular, as part of your contingency planning, you can choose to use **Anthos** build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. | N/A |

# Danish FSA - Executive Order 877 on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| 5. | Subsection 2. If the outsourcing company is part of a group, the outsourcing company can instead use centrally determined contingency plans for outsourcing with the necessary adjustments. | This is a customer consideration. | N/A |
| **Section 17 - Exit strategies** | | | |
| 6. | The outsourcing company shall, when outsourcing critical or important outsourcing, have written exit strategies that meet the requirements of Annex 4. | Refer to Rows 130 to 151 on Annex 4. | N/A |
| 7. | *Subsection 2.* If the outsourcing company is part of a group where the exit plan for a critical or important outsourcing has been established at group level, the outsourcing company must receive a summary of the exit plan and ensure that the plan can be carried out effectively. | This is a customer consideration. | N/A |
| **Section 19 - Risk assessment when using outsourcing** | | | |
| 8. | The outsourcing company must prior to a decision on outsourcing or further outsourcing | | |
| 9. | 1) assess the potential consequences for the outsourcing company's operational risks and | Google recognizes that resilience is a key focus for regulated entities and supervisory authorities. Our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper discusses the continuing importance of operational resilience to the financial services sector, and the role that a well-executed migration to Google Cloud can play in strengthening it. | N/A |
| 10. | 2) take necessary measures to limit operational risks associated with outsourcing. | See above. | N/A |
| 11. | *Subsection 2* The assessment according to Subsection 1, no. 1, shall at least contain: | | |
| 12. | 1) An identification and classification of the relevant processes, services or activities and related data and systems based on their sensitivity and required protection measures. | The GCP services are described on our services summary page. You decide which services to use, how to use them and for what purpose. Therefore, you decide the scope of the arrangement. | N/A |
| 13. | 2) A risk-based analysis of the processes, services and activities and related data and systems in connection with outsourcing. | This is a customer consideration. Refer to Row 17 for more information on the security of the services. | N/A |
| 14. | 3) Assessment of the consequences of the supplier's location. | 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. | Data Center Location; Data Transfers (Data Processing and Security Terms) |

# Danish FSA - Executive Order 877
# on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| | | • Information about the location of Google's facilities and where individual GCP services can be deployed is available here.<br>• Information about the location of Google's subprocessors' facilities is available here.<br><br>Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular:<br><br>• The same robust security measures apply to all Google facilities, regardless of country / region.<br>• Google makes the same commitments about all its subprocessors, regardless of country / region.<br><br>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).<br><br>You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper. | Data Security; Subprocessors (Data Processing and Security Terms)<br><br>Data Location (Service Specific Terms) |
| 15. | 4) Assessments of political stability and the security situation in the relevant jurisdictions. | See Row 14 above. | N/A |
| 16. | 5) Definition and establishment of an appropriate level of protection for data confidentiality, the continuity of the outsourced activities and the integrity and traceability of the data and systems in connection with the intended outsourcing. | Confidentiality and integrity of data<br><br>Refer to Row 17 for information on the security of the services.<br><br>Continuity<br><br>Refer to our "Architecting disaster recovery for cloud infrastructure outages" article for information about how Google Cloud is architected to minimize the frequency and scope of outages as well as an architecture planning guide that provides a framework for categorizing and designing applications based on the desired reliability outcomes.<br><br>Traceability | Business Continuity and Disaster Recovery |

# Danish FSA - Executive Order 877
# on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| | | Google recognizes that you need visibility into who did what, when, and where for all user activity on our service.<br><br>• Cloud Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud Platform resources.<br>• Cloud Audit Logs help your security teams maintain audit trails in GCP and view detailed information about Admin activity, data access, and system events.<br>• Multi-Factor Authentication provides a wide variety of verification methods to help protect your user accounts and data.<br><br>The "Managing Google's Access to your Data" section of our Trusting your data with GCP whitepaper explains Google's data access processes and policies.<br><br>In addition, you can also monitor and control the limited actions performed by Google personnel on your data using these tools:<br><br>• 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).<br>• Access Approval is a feature that enables you to require your explicit approval before Google support and engineering teams are permitted access to your customer content. Access Approval provides an additional layer of control on top of the transparency provided by Access Transparency. | |
| 17. | 6) Assessments of relevant security measures for data transfer, data processing and data storage. | The security of a cloud service consists of two key elements:<br><br>(1) Google's infrastructure<br><br>Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services.<br><br>Given the one-to-many nature of our service, Google provides the same robust security for all our customers. | Confidentiality; Data Security; Security Measures (Data Processing and Security Terms) |

# Danish FSA - Executive Order 877 on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| | | 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.<br><br>More information is available at:<br><br>● Our infrastructure security page<br>● Our security whitepaper<br>● Our cloud-native security whitepaper<br>● Our infrastructure security design overview page<br>● Our security resources page<br><br>In addition, you can review Google's SOC 2 report.<br><br>(2) Your data and applications in the cloud<br><br>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.<br><br>(a) Security by default<br><br>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:<br><br>● **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.<br><br>● **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.<br><br>(b) Security products | |

# Danish FSA - Executive Order 877 on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| | | 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 on our Cloud Security Products page.<br><br>(c) Security resources<br><br>Google also publishes guidance on:<br><br>• Security best practices<br>• Security use cases | |
| 18. | 7) Assessments of the significance of the supplier possibly being a subsidiary or parent company of the outsourcing company. | This is a customer consideration. | N/A |
| 19. | *Subsection 3.* Where relevant, the assessment must include scenarios of possible risk events. | This is a customer consideration. | N/A |
| 20. | *Subsection 4.* The assessment must take into account the expected consequences of outsourcing, including at least the following: | | |
| 21. | 1) Concentration risks. | Refer to our Engaging in a European dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on how Google's approach to open source can help you address vendor lock-in and concentration risk.<br><br>To manage concentration risk, you can choose to use Anthos to build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments.<br><br>In addition, Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example:<br><br>• Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments.<br>• Migrate for Anthos allows you to move and convert workloads directly into containers in Google Kubernetes Engine. | Data Export (Data Processing and Security Terms) |

# Danish FSA - Executive Order 877
# on outsourcing for credit institutions
## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| | | • You can export/import an entire VM image in the form of a .tar archive. Find more information on images and storage options on our Compute Engine Documentation page. | |
| 22. | 2) The total risks as a result of outsourcing across the outsourcing company or in the entire group. | This is a customer consideration. | N/A |
| 23. | 3) The risk that the outsourcing company may be forced to provide financial support to an distressed supplier or take over its business activities. | This is a customer consideration. You can review information about Google's financial performance and condition on Alphabet's Investor Relations page. | N/A |
| 24. | 4) The measures to be implemented by the outsourcing company and the supplier in order to manage and reduce the risks. | Refer to Row 17 for information about security measures.<br>Refer to Row 28 for information about continuity measures. | N/A |
| 25. | *Subsection 5.* The assessment shall, if suppliers can further outsource critical or important outsourcing to subcontractors, take the following into account: | | |
| 26. | 1) The risks associated with further outsourcing. | Google recognizes that regulated entities 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 we can. In some cases there may be clear benefits to working with other trusted organizations e.g. to provide 24/7 support.<br><br>To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will:<br><br>• provide information about our subcontractors;<br>• provide advance notice of changes to our subcontractors; and<br>• give regulated entities the ability to terminate if they have concerns about a new subcontractor.<br><br>Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you. | Google Subcontractors |
| 27. | 2) The risk that more subcontractors in the event of further outsourcing may reduce the outsourcing company's ability to control critical or important outsourcing and the supervisory authorities' ability to effectively supervise critical or important outsourcing. | We recognize that subcontracting must not reduce the regulated entity's or the supervisory authority's ability to supervise the relevant activity. To preserve this, Google will ensure our subcontractors comply with the information, audit and access rights we provide to regulated entities and supervisory authorities. | Google Subcontractors |

# Danish FSA - Executive Order 877
# on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| 28. | *Subsection 6.* The assessment must take into account risks associated with the possible cessation of outsourcing, including risks from transferring the outsourced process, service or activity to another supplier or by reintegrating the process, service or activity of the outsourcing company. | Cessation of outsourcing<br><br>Google recognizes that regulated entities must plan for situations where their providers are unable, for any reason, to provide the services contracted.<br><br>Google is committed to addressing customers' needs for portability and interoperability. We will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example:<br><br>• Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments.<br>• Migrate for Anthos allows you to move and convert workloads directly into containers in Google Kubernetes Engine.<br>• You can export/import an entire VM image in the form of a .tar archive. Find more information on images and storage options on our Compute Engine Documentation page.<br><br>In addition, Google believes in an open cloud that supports multi-cloud and hybrid cloud approaches. If implemented through the use of open-source based technologies, these approaches can provide customers with the levels of portability, substitutability and survivability, required for robust exit planning. Refer to our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper for more information.<br><br>Transferring the outsourced process<br><br>Google recognizes that regulated entities need sufficient time to exit our services (including to transfer services to another service provider). To help regulated entities achieve this, upon request, Google will continue to provide the Services for 12 months beyond the expiry or termination of the contract. | N/A<br><br>Transition Term<br><br>Data Export (Data Processing and Security Terms)<br><br>Transition Term |
| **Section 20 - Previous examination** | | | |
| 29. | An outsourcing company must, before making a decision on the choice of supplier for outsourcing, conduct an investigation of the supplier. | | |

# Danish FSA - Executive Order 877
# on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| 30. | *Subsection 2* At a minimum, the study must include an assessment of: | Google recognizes that you need to conduct due diligence and perform a risk assessment before deciding to use our services. To assist you, we've provided information for each of the areas you need to consider in the rows that follow. | N/A |
| 31. | 1) Supplier's business model, business type, size, complexity, financial situation, ownership and group structure. | You can review Google's corporate and financial information on Alphabet's Investor Relations page. This provides information about our mission, business model, and strategy. It also provides information about our organizational policies e.g. our Code of Conduct. | N/A |
| 32. | 2) The long-term relationships with suppliers that have already been assessed, and who perform services for the outsourcing company. | This is a customer consideration. | N/A |
| 33. | 3) Whether the supplier is affiliated with the outsourcing company. | This is a customer consideration. | N/A |
| 34. | 4) Whether the supplier is subject to supervision by the Danish Financial Supervisory Authority or other relevant authority. | Google is not directly subject to supervision by the Danish Financial Supervisory Authority for the GCP services. However, Google will provide supervisory authorities with the assistance they need to review our Services. | Enabling Customer Compliance; Regulator Information, Audit and Access |
| 35. | 5) Whether the supplier can take appropriate technical and organisational measures to protect the outsourcing company's data, including personal data. | Refer to Row 17 for information on Google's security measures. | N/A |
| 36. | 6) Regarding the supplier and any subcontractors, act in accordance with the outsourcing company's values and code of conduct. | You can review information about our mission, philosophies and culture on Alphabet's Investor Relations page. It also provides information about our organisational policies e.g. our Code of Conduct. | N/A |
| **Section 21 - Outsourcing contract** | | | |
| 37. | The outsourcing company must enter into a written outsourcing contract with the supplier, clearly stating the rights and obligations of the parties. | The rights and obligations of the parties are set out in the Google Cloud Financial Services Contract. | N/A |
| 38. | *Subsection 2.* The outsourcing contract shall for critical or important outsourcing meet the requirements in Annex 3. | Refer to Rows 73 to 129. | N/A |
| 39. | *Subsection 3.* The outsourcing company must, in the outsourcing contract for outsourcing that is not critical or important, meet the requirements of Annex 3, No. 3. | Refer to Row 109. | N/A |
| 40. | *Subsection 4.* In the outsourcing contract for outsourcing that is not critical or important, the outsourcing company must, based on a risk-based approach, ensure the right of access and audit as stated in subsection 5 and Annex 3, No. 4. | See Row 41 below and refer to Rows 111 to 115. | N/A |
| 41. | *Subsection 5.* In the case of critical or important outsourcing, the outsourcing company must ensure that the outsourcing contract or other contractual arrangements do not | Nothing in our contract is intended to limit or impede a regulated entity's or the supervisory authority's ability to audit our services effectively. | Enabling Customer Compliance |

# Danish FSA - Executive Order 877 on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| | hinder or limit the actual exercise of the right of access and audit for the outsourcing company, the Danish Financial Supervisory Authority, Finansiel Stabilitet or a third party designated by the outsourcing company to exercise these rights. | | |
| 42. | *Subsection 6.* In the outsourcing contract for outsourcing that is not critical or important, the outsourcing company must take into account that outsourced processes, services and activities may become critical or important. | Google recognizes that use of the Services could scale up over time. Regardless of how regulated entities choose to use the Services at the start of our relationship, Google will provide regulated entities and supervisory authorities with audit, access and information rights. | Enabling Customer Compliance |
| **Section 22 - Data protection and IT-related outsourcing** | | | |
| 43. | The outsourcing company shall, subject to the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC and subsequent amendments, take into account differences in national data protection rules when outsourcing or further outsourcing of data. | Google will comply with all data protection regulations applicable to it in the provision of the Services, including the GDPR.<br><br>In addition, Google makes commitments to protect your data in the Data Processing and Security Terms, including regarding security, access and transfer.<br><br>In addition, Google provides commitments to enable the lawful transfer of personal data to a third country in accordance with European data protection law. | Representations and Warranties<br><br>Data Transfers (Data Processing and Security Terms) |
| 44. | *Subsection 2* The outsourcing company must take a risk-based approach to data storage and data processing premises and information security considerations if the outsourcing involves the processing or disclosure of personal data or confidential data. | 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.<br><br>• Information about the location of Google's facilities and where individual GCP services can be deployed is available here.<br>• Information about the location of Google's subprocessors' facilities is available here.<br><br>Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular:<br><br>• The same robust security measures apply to all Google facilities, regardless of country / region.<br>• Google makes the same commitments about all its subprocessors, regardless of country / region. | Data Center Location; Data Transfers (Data Processing and Security Terms)<br><br>Data Security; Subprocessors (Data Processing and Security Terms) |

# Danish FSA - Executive Order 877
# on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| | | 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).<br><br>You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper. | Data Location (Service Specific Terms) |
| 45. | *Subsection 3* The outsourcing company shall, where appropriate, ensure that it is able to perform IT security testing to assess the effectiveness of cyber- and information-risk mitigation measures as well as communication technology risks. | You can perform penetration testing of the Services at any time without Google's prior approval.<br><br>In addition, Google engages a qualified and independent third party to conduct penetration testing of the Services. More information is available here. | Customer Penetration Testing |
| **Section 23 - Monitoring and control** | | | |
| 46. | Based on a risk-based approach, the outsourcing company must continuously monitor, examine and control the supplier's work and carry out audits of the supplier. | Monitoring<br>You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services.<br><br>For example:<br>• The Status Dashboard provides status information on the Services.<br>• Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP.<br>• 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 |

# Danish FSA - Executive Order 877
# on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| | | Control<br><br>Regulated entities can use the following functionality to control the Services:<br><br>• **Cloud Console:** A web-based graphical user interface that customers can use to manage their GCP resources.<br>• **gcloud Command Tool:** A tool that provides the primary command-line interface to GCP. A command-line interface is a user interface to a computer's operating system.<br>• **Google APIs:** Application programming interfaces which provide access to GCP<br><br>Audits<br><br>Google recognizes that regulated entities must be able to audit our services effectively. Google grants audit, access and information rights to regulated entities and their appointees.<br><br>For more information on the independent third-party audit reports that Google provides, refer to Row 59. | Instructions<br><br>Customer Information, Audit and Access |
| 47. | *Subsection 2.* Prior to a scheduled visit to a supplier, the outsourcing company must ensure that the outsourcing company, auditors or third parties acting on behalf of the outsourcing company give the supplier reasonable notice. | 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. | Arrangements |
| 48. | *Subsection 3.* The supplier shall not receive reasonable notice if this is not possible due to an emergency or crisis situation or if the purpose of the visit will be invalidated. | 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 |
| 49. | *Subsection 4.* When conducting a visit, cf. Section 2, the outsourcing company must take due account of the supplier's operation and safety if the supplier serves other customers. The representatives of the outsourcing company must have relevant qualifications and knowledge to complete the visit. | 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.<br><br>When a regulated entity 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 regulated entity. In particular, we will be careful to comply with our security commitments at all times. | Arrangements |
| 50. | *Subsection 5.* The outsourcing company must continually update its assessments in accordance with Sections 5 and 19. | This is a customer consideration. | N/A |

# Danish FSA - Executive Order 877 on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| 51. | *Subsection 6.* The outsourcing company shall monitor its internal concentration risks as a result of outsourcing taking into account Section 19, Subsection 4. | This is a customer consideration. Refer to Row 28 for information on the substitutability of our services. | N/A |
| 52. | *Subsection 7.* The outsourcing company must continuously ensure that outsourcing meets appropriate performance and quality standards in accordance with the outsourcing company's policies by | | |
| 53. | 1) ensuring that the outsourcing company receives appropriate reporting from the supplier, | 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 on our Incidents & the Google Cloud dashboard page.<br><br>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<br><br>Data Incidents (Data Processing and Security Terms) |
| 54. | 2) evaluating the deliverables received from the supplier by using tools, including key performance and control indicators, reports on the performance of the services, self-certification and independent investigations, and | The SLAs provide measurable performance standards and remedies for the services and are available on our Google Cloud Platform Service Level Agreements page.<br><br>Refer to Row 46 for information on how you can monitor Google's performance of the Services, including the SLAs. | Services |
| 55. | 3) reviewing all other relevant information received from the supplier, including reports on contingency plans and tests of these. | Audit reports<br><br>For more information on the third-party audit reports Google provides refer to Row 59.<br><br>Contingency plans<br><br>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. Regulated entities can review our plan and testing results.<br><br>In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide. | Business Continuity and Disaster Recovery |
| 56. | *Subsection 8.* The outsourcing company shall monitor whether the supplier complies with the agreed data and system security requirements, if outsourcing concerns IT services. | Refer to Row 28 for information on how you can use Google's Security Products to monitor the security of your data. | N/A |
| **Section 24 - Monitoring and control** | | | |

# Danish FSA - Executive Order 877 on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| 57. | The outsourcing company must take appropriate measures, and if necessary, terminate the outsourcing contract with immediate effect if it finds deficiencies in the outsourced process, service or activity. | If Google's performance of the Services does not meet the Google Cloud Platform Service Level Agreements regulated entities may claim service credits.<br><br>In addition, regulated entities may terminate our contract for Google's material breach. | Services<br><br>Term and Termination |
| **Section 26 - Use of Joint Audits with Other Supplier Customers** | | | |
| 58. | The outsourcing company may use joint audits, which are organised and carried out jointly with other of the supplier's customers, or a third party, appointed by the outsourcing company and other of the supplier's customers jointly. | Google recognizes the benefits of pooled audits. We would be happy to discuss this with regulated entities. For more information about Google's approach to pooled audits, refer to our 'Earning customer trust through a pandemic: delivering our 2020 CCAG pooled audit' blog post. | N/A |
| **Section 27 - Use of internal audit reports, third-party certifications and third-party audit reports provided by the supplier** | | | |
| 59. | The outsourcing company may use third party certifications, third party audit reports and internal audit reports provided by the supplier if the conditions in nos. 1-7 are met: | 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:<br><br>• ISO/IEC 27001:2013 (Information Security Management Systems)<br>• ISO/IEC 27017:2015 (Cloud Security)<br>• ISO/IEC 27018:2014 (Cloud Privacy)<br>• PCI DSS<br>• SOC 1<br>• SOC 2<br>• SOC 3<br><br>You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources. | Certifications and Audit Reports |
| 60. | 1) The outsourcing company considers that the audit plan for the outsourced process, service or activity is adequate. | 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 |

# Danish FSA - Executive Order 877 on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| 61. | 2) The outsourcing company ensures that the scope of the certification or audit report covers the key systems and key controls designated by the outsourcing company and that the certification or audit report complies with relevant regulatory requirements. | Google's audit scope covers in-scope Services, infrastructure systems, policies and procedures, common processes and personnel. Google is audited on our security and privacy controls covering the relevant certifications and audit reports for the audit scope. | Certifications and Audit Reports |
| 62. | 3) The outsourcing company continuously assesses the content of the certifications or audit reports and verifies that they are not obsolete. | Google is audited at least once a year for each audited framework. You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources. | Certifications and Audit Reports |
| 63. | 4) The outsourcing company is satisfied with the suitability of the party or parties performing the certification or audit. | 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 |
| 64. | 5) The outsourcing company ensures that the certifications and audits are carried out in accordance with recognised relevant industry standards and includes tests of the operational effectiveness of the key controls. | Google's independent third party audits include testing of operational effectiveness of key controls in place. | Certifications and Audit Reports |
| 65. | 6) The outsourcing company has a contractual right to demand that the scope of the certifications or audit reports be extended to other relevant systems and controls. | 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, regulated entities can request an expansion of the scope. | Certifications and Audit Reports |
| 66. | 7) The outsourcing company retains the contractual right to decide whether to carry out its own audit procedures with regard to critical or important outsourcing. | Regulated entities always retain the right to conduct an audit.Google offers regulated entities certifications and audit reports in addition to (and not instead of) audit, access and information rights. | Customer Information, Audit and Access |
| 67. | *Subsection 2.* If the outsourcing company uses third-party certifications, third-party audit reports or internal audit reports provided by the supplier, it must ensure that the outsourcing company can meet its regulatory obligations. | This is a customer consideration. | N/A |
| 68. | *Subsection 3.* For critical or important outsourcing, the outsourcing company may not over time rely solely on third party certifications, third party audit reports or internal audit reports provided by the supplier. | Refer to Row 66. | N/A |
| **Annex 2 - Outsourcing register** | | | |
| 69. | 2) In the event that an outsourcing agreement contains the use of cloud services, the outsourcing register must contain the following: | | |
| 70. | a) Information about the cloud provider in question. | Refer to your Google Cloud Financial Services. | Order Form; Recitals |

# Danish FSA - Executive Order 877 on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| 71. | b) Cloud service implementation models. | GCP is a public cloud service. Customers can choose to deploy it as part of a hybrid or multi-cloud deployment. | N/A |
| 72. | c) The specific nature and locations of the data to be stored. | You decide which services to use, how to use them and for what purpose. Therefore, you decide the nature of the data that is stored on the services.<br><br>Information about the location of Google's facilities and where individual GCP services can be deployed is available on our Global Locations page. | N/A |
| **Annex 3 - Requirements for the outsourcing contract** | | | |
| 73. | 1) The outsourcing contract for critical or important outsourcing must contain at least: | | |
| 74. | a) A description of the outsourced process, service or activity to be delivered, including quantitative and qualitative targets for the deliveries and the results contained in the outsourcing agreements. | The GCP services are described on our services summary page.<br><br>The SLAs are available on our Google Cloud Platform Service Level Agreements page. | Definitions<br><br>Services |
| 75. | b) A start date and any end date for the outsourcing contract. | Refer to your Google Cloud Financial Services Contract. | Term and Termination |
| 76. | c) Deadlines for termination for the outsourcing company. | Refer to your Google Cloud Financial Services Contract. | Term and Termination |
| 77. | d) The applicable law to which the outsourcing contract is subject. | Refer to your Google Cloud Financial Services Contract. | Governing Law |
| 78. | e) The parties to the agreement's financial obligations to each other. | Refer to your Google Cloud Financial Services Contract. | Payment Terms |
| 79. | f) Indication of whether the supplier can outsource a critical or important process, service or activity or essential parts thereof. | Refer to Row 99 on subcontracting. | N/A |

# Danish FSA - Executive Order 877 on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| 80. | g) The location or locations where the outsourcing will be provided or where relevant data will be stored and processed, including the possible location for storage. | 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.<br><br>• Information about the location of Google's facilities and where individual GCP services can be deployed is available on our Global Locations page.<br>• Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page.<br><br>Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular:<br><br>• The same robust security measures apply to all Google facilities, regardless of country / region.<br>• Google makes the same commitments about all its subprocessors, regardless of country / region. | Data Transfers (Data Processing and Security Terms)<br><br>Data Security; Subprocessors (Data Processing and Security Terms) |
| 81. | h) The conditions to be met, including contractual requirements to notify the outsourcing company if the supplier wishes to change the location of the storage. | 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).<br><br>You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for European customers on Google Cloud Whitepaper. | Data Location (Service Specific Terms) |
| 82. | i) Access, availability, integrity, data protection and security of data, if applicable to the outsourcing agreement. | Access<br><br>Regulated entities may access their data on the services at any time.<br><br>Availability<br><br>The SLAs contain Google's commitments regarding availability of the Services. They are available on the Google Cloud Platform Service Level Agreements page.<br><br>Data protection and security of data | Customer Information, Audit and Access<br><br>Services |

# Danish FSA - Executive Order 877
# on outsourcing for credit institutions
## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| | | Refer to Row 17 for information about the security of the services. Google makes commitments to protect your data in the Data Processing and Security Terms. | Data Security; Security Measures (Data Processing and Security Terms) |
| 83. | j) The outsourcing company's right continuously to monitor the supplier's deliveries and performance. | You can monitor Google's performance of the Services (including the SLAs) on a regular basis using the functionality of the Services.<br><br>For example:<br><br>• The **Status Dashboard** provides status information on the Services.<br><br>• Google Cloud **Operations** is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP.<br><br>• **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 |
| 84. | k) The outsourcing company's requirements for the ongoing reporting that the supplier must provide to the outsourcing company, including internal audit reports prepared by the supplier's internal auditor, where applicable. | 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 on our Incidents & the Google Cloud dashboard page.<br><br>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.<br><br>You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources. | Significant Developments<br><br>Data Incidents (Data Processing and Security Terms)<br><br>Certifications and Audit Reports |
| 85. | l) The supplier's obligations to inform the outsourcing company of any development of the supplier that may have a material impact on the supplier's ability to effectively perform the outsourced critical or important process, service or activity in accordance with | See above. | N/A |

# Danish FSA - Executive Order 877
# on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| | | | |
| 86. | i) the agreed service levels; or | See above. | N/A |
| 87. | ii) applicable legislation and regulatory requirements. | See above. | N/A |
| 88. | m) Any obligation of the supplier to take out insurance against certain risks and any extent of the insurance coverage. | Google will maintain insurance cover against a number of identified risks. | Insurance |
| 89. | n) The requirements for the Supplier's execution and testing of 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. Regulated entities can review our plan and testing results.<br><br>In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide. | Business Continuity and Disaster Recovery |
| 90. | o) Requirements that ensure that the data belonging to the outsourcing company and associated relevant systems can be accessed in the event of insolvency, liquidation or termination of the supplier's business activities. | You retain all intellectual property rights in your data.<br><br>Google will enable you to access and export your data throughout the duration of our contract. Refer to Row 124.<br><br>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<br><br>Data Export (Data Processing and Security Terms)<br><br>Term and Termination |
| 91. | p) Requirements that ensure that the supplier is obliged to cooperate with the Danish Financial Supervisory Authority, Finansiel Stabilitet and other persons appointed by these authorities. | Google will cooperate with supervisory authorities, and their appointees, exercising their audit, information and access rights. | Enabling Customer Compliance |
| 92. | q) The outsourcing company's or a third party designated by the outsourcing company and the Danish Financial Supervisory Authority' s unlimited right to investigate and audit the supplier. | Google recognizes that regulated entities must be able to audit our services effectively. Google grants audit, access and information rights to regulated entities and supervisory authorities, and both their appointees. | Regulator Information, Audit and Access<br>Customer Information, Audit and Access |

# Danish FSA - Executive Order 877
# on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| 93. | r) Termination rights. | You can elect to terminate our contract for convenience with advance notice, including if necessary to comply with law or if directed by a supervisory authority.<br><br>In addition, regulated entities may terminate our contract with advance notice for Google's material breach after a cure period. | Term and Termination |
| 94. | Special Requirements for Further Outsourcing | | |
| 95. | 2. If the outsourcing contract allows the use of further outsourcing of critical or important processes, services or activities or essential parts thereof, cf. Annex 3, no. 1, letter f, the outsourcing contract must meet the following requirements: | | |
| 96. | a) It shall specify any types of processes, services or activities which may not be outsourced. | Google recognizes that regulated entities need to consider the risks associated with subcontracting. 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.<br><br>Although Google will provide you with information about the organizations that we work with, we cannot agree that we will never subcontract. Given the one-to-many nature of our service, if we agreed with one customer that we would not subcontract, we would potentially be denying all our customers the benefit motivating the subcontracting arrangement.<br><br>To ensure regulated entities retain oversight of any subcontracting, Google will comply with clear conditions designed to provide transparency and choice. | Subcontracting; Google Subcontractors |
| 97. | b) It shall specify the conditions to be met in the event of outsourcing. | To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will:<br><br>• provide information about our subcontractors;<br>• provide advance notice of changes to our subcontractors; and<br>• give regulated entities the ability to terminate if they have concerns about a new subcontractor. | Google Subcontractors |

# Danish FSA - Executive Order 877
# on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| 98. | c) It must state that the supplier is obliged to monitor and control the processes, services or activities that the supplier has outsourced, in order to ensure that all contractual obligations between the supplier and the outsourcing company are fulfilled on an ongoing basis. | Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you. | Google Subcontractors |
| 99. | d) It must require the supplier to obtain prior specific or general written permission from the outsourcing company before further outsourcing of data covered by Article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on protection of natural persons in connection with the processing of personal data and on the free movement of such data and on the repeal of Directive 95/46/EC. | Google will comply with our obligations under the GDPR regarding authorization for subprocessing. | Processing of Data; Subprocessors (Data Processing and Security Terms) |
| 100. | e) It must include an obligation for the supplier to protect confidential, personal or otherwise sensitive information and comply with all legal requirements regarding the protection of data applicable to the outsourcing company. | Refer to Row 17 for information on the security of the services.<br>Google will comply with all data protection regulations applicable to it in the provision of the Services, including the GDPR. | Representations and Warranties |
| 101. | f) It must include an obligation for the supplier to notify the outsourcing company with an agreed notice of planned further outsourcing or significant changes in existing further outsourcing. The notification period must be sufficiently long for the outsourcing company to at least make a risk assessment, cf. Section 19, of the proposed changes and object to changes before the planned further outsourcing or significant changes thereof enter into force. | Regulated entities 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 |
| 102. | g) It shall, where appropriate, include a right for the outsourcing company to oppose the planned further outsourcing or significant changes to existing further outsourcing agreements or a right for the outsourcing company to explicitly approve the planned further outsourcing or significant changes to existing further outsourcing agreements. | See above. | N/A |
| 103. | h) It must ensure that the outsourcing company has the right to terminate the contract in the event of unjustified further outsourcing, including in cases where the unjustified further outsourcing | Regulated entities should have a choice about the parties who provide services to them. To ensure this, regulated entities 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 |
| 104. | h i) significantly increases the risk to the outsourcing business, or | See above. | N/A |
| 105. | h ii) where the supplier continues to outsource without notifying the outsourcing company in advance, cf. Annex 3, no. 2, letter f. | See above. | N/A |

# Danish FSA - Executive Order 877
# on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| 106. | i) It must ensure that the subcontractor undertakes to comply with applicable legislation, regulatory requirements and contractual obligations corresponding to the obligations that the supplier has assumed to the outsourcing company, and provide the outsourcing company, including a third party designated by the outsourcing company, and the Danish Financial Supervisory Authority with the same contractual rights to access and audit, as mentioned in Section 21, Subsections 4 and 5. | Google requires our subcontractors to meet the same high standards that we do. Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you and applicable law and regulation. . Google recognizes that subcontracting must not reduce the regulated entity's ability to oversee the service or the supervisory authority's ability to supervise the regulated entity. To preserve this, Google will ensure our subcontractors comply with the information, access and audit rights we provide to regulated entities and supervisory authorities. | Google Subcontractors |
| 107. | j) It must ensure that the supplier monitors and controls subcontractors in accordance with the outsourcing company's policies. | See above. | N/A |
| 108. | Special Requirements for Outsourcing Involving IT Services | | |
| 109. | 3. When outsourcing IT services, the outsourcing contract must define data and system security requirements and ensure that suppliers meet relevant IT security standards that enable the outsourcing company to comply with its IT security policy. | Refer to Row 17 for information about the security of the services.<br><br>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:<br><br>• ISO/IEC 27001:2013 (Information Security Management Systems)<br>• ISO/IEC 27017:2015 (Cloud Security)<br>• ISO/IEC 27018:2014 (Cloud Privacy)<br>• PCI DSS<br>• SOC 1<br>• SOC 2<br>• SOC 3<br><br>You can review Google's current certifications and audit reports at any time. | Certifications and Audit Reports |
| 110. | Special requirements for rights to access and audit | | |
| 111. | 4. The outsourcing contract must contain requirements for the supplier, which ensure the following: | | |

# Danish FSA - Executive Order 877
# on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| 112. | a) That the internal audit department in the outsourcing company can perform an audit of the outsourced process, service or activity. | Google grants information, audit and access rights to regulated entities. This includes the regulated entity's internal audit department or a third party auditor appointed by the regulated entity. | Customer Information, Audit and Access |
| 113. | b) That the Danish Financial Supervisory Authority has the right to obtain information and exercise investigative powers, cf. Sections 346 and 347 of the Financial Business Act. | Google grants information, audit and access rights to supervisory authorities and their appointees. | Regulator Information, Audit and Access |
| 114. | c) That the Danish Financial Supervisory Authority and Finansiel Stabilitet have the right to obtain information and exercise investigative powers in connection with liquidation planning | Google will cooperate with supervisory authorities and resolution authorities exercising their audit, information and access rights.<br><br>In addition, Google recognizes that regulated entities 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. | Enabling Customer Compliance<br><br>Support through Resolution |
| 115. | d) That the outsourcing company, the Danish Financial Supervisory Authority, Finansiel Stabilitet and any other person appointed by the outsourcing company, the Danish Financial Supervisory Authority or Finansiel Stabilitet, have<br>i) full access to all relevant business premises, including all relevant units, systems, networks, information and data used to provide the outsourced process, service or activity, including relevant financial information, staff and the supplier's external auditors, and<br>ii) unlimited right to inspect and audit outsourcing in order to monitor the outsourcing agreement and ensure compliance with all applicable regulatory and contractual requirements. | Google recognizes that regulated entities must be able to audit our services effectively. Google grants audit, access and information rights to regulated entities and supervisory authorities, and both their appointees. This includes access to Google's premises used to provide the Services to conduct an on-site audit. | Regulator Information, Audit and Access<br>Customer Information, Audit and Access |
| 116. | Special requirements for termination rights | | |
| 117. | 5. For critical or important outsourcing, the outsourcing contract must include agreements on termination rights, including the outsourcing company's express option to terminate the outsourcing contract in accordance with applicable law, and in the following situations: | Regulated entities can elect to terminate our contract for convenience with advance notice, including if necessary to comply with law or if directed by a supervisory authority.<br><br>In addition, regulated entities may terminate our contract with advance notice for Google's material breach after a cure period. | Termination for Convenience<br><br>Term and Termination |
| 118. | a) Where the supplier of the outsourced processes, services or activities violates applicable law, other regulations or contractual provisions. | See above. | N/A |

# Danish FSA - Executive Order 877 on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| 119. | b) Where there are obstacles that may change the outcome of the outsourced process, service or activity. | See above. | N/A |
| 120. | c) Where there are significant changes that affect the deliveries or the supplier, including significant changes as a result of further outsourcing or by change of subcontractors | See above. Refer to Row 97 for information on the regulated entity's rights in respect of new subcontractors. | N/A |
| 121. | d) Where weaknesses are found in the handling and security of confidential, personal or otherwise sensitive data and information. | See above. | N/A |
| 122. | e) Where the Danish Financial Supervisory Authority issues the outsourcing company one or more orders that relate to the outsourced processes, services or activities. | See above. | N/A |
| 123. | 6. For critical or important outsourcing, the outsourcing contract must contain requirements for the supplier, which in the event of termination: | | |
| 124. | a) Describe the obligations of the existing supplier if the outsourced process, service or activity is transferred to another supplier or to the outsourcing company. | 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:<br>• **Google Kubernetes Engine** is a managed, production-ready environment that allows portability across different clouds as well as on premises environments.<br>• **Migrate for Anthos** allows you to move and convert workloads directly into containers in Google Kubernetes Engine.<br>• 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) |
| 125. | b) Establish an appropriate transition period during which the supplier, after termination of the outsourcing contract, undertakes to continue its deliveries. | Google recognizes that regulated entities 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 regulated entities achieve this, upon request, Google will continue to provide the Services for 12 months beyond the expiry or termination of the contract. | Transition Term |
| 126. | c) Contain an obligation on the part of the supplier to assist the outsourcing company in ensuring a sound transfer of the process, service or activity. | Our Services enable you to transfer your data independently. You do not need Google's permission to do this. Refer to Row 124. However, if a regulated entity would like | Transition Assistance |

# Danish FSA - Executive Order 877
# on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| | | support, upon request, Google will provide advisory and implementation services to assist in migrating workloads or otherwise transitioning use of the Services. | |
| 127. | 7. For banks, mortgage banks and stockbroking companies, the outsourcing contract for critical or important outsourcing must contain information on the powers granted to Finansiel Stabilitet in accordance with Chapter 5 of the Act on Restructuring and Liquidation of Certain Financial Undertakings, including | | |
| 128. | a) references to the obligations arising from sections 31 and 34 of the Restructuring and Liquidation of Certain Financial Undertakings Act, and | Google recognizes that regulated entities 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 |
| 129. | b) a description of the essential obligations in the contract in accordance with Section 243 d, Subsection 2, of the Financial Business Act and Section 31, Subsection 2 of the Act on Restructuring and Liquidation of Certain Financial Undertakings. | See above. | N/A |
| **Annex 4 - Exit strategy** | | | |
| 130. | The outsourcing company's written exit strategies must be in accordance with the outsourcing company's outsourcing policy and contingency plans, and must at least take into account: | Google recognizes that regulated entities must plan for situations where their providers are unable, for any reason, to provide the services contracted.<br><br>Google is committed to addressing customers' needs for portability and interoperability. We will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. Refer to Row 124 for more information.<br><br>In addition, Google believes in an open cloud that supports multi-cloud and hybrid cloud approaches. If implemented through the use of open-source based technologies, these approaches can provide customers with the levels of portability, substitutability and survivability, required for robust exit planning. Refer to our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper for more information. | N/A |
| 131. | Termination of outsourcing agreements. | See above. | N/A |
| 132. | Breach of contract by the supplier. | See above. | N/A |

# Danish FSA - Executive Order 877
# on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| 133. | Deterioration of the quality of the process, service or activity provided due to improper or inadequate management of the outsourced process, service or activity. | See above. | N/A |
| 134. | Actual or potential business interruptions caused by inappropriate or non-performance of the outsourced process, service or activity. | See above. | N/A |
| 135. | Significant risks that may arise in relation to the continued use of the outsourced process, service or activity. | See above. | N/A |
| 136. | The outsourcing company's exit strategies must adequately ensure that it is able to complete an outsourcing without: | Google recognizes that resilience is a key focus for regulated entities and supervisory authorities. Our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper discusses the continuing importance of operational resilience to the financial services sector, and the role that a well-executed migration to Google Cloud can play in strengthening it. | N/A |
| 137. | unnecessary interruption of the outsourcing business' activities, | See above. | N/A |
| 138. | to limit the outsourcing company's compliance with regulatory requirements and | See above. | N/A |
| 139. | that it is detrimental to the continuity and quality of the outsourcing company's provision of services to customers. | See above. | N/A |
| 140. | The outsourcing company's exit strategies must include the following: | This is a customer consideration. | N/A |
| 141. | A delimitation of the purposes of the exit strategy. | This is a customer consideration. | N/A |
| 142. | Adequate exit plans that are adequately tested. | This is a customer consideration. | N/A |
| 143. | A description of how roles, responsibilities and adequate resources are allocated to ensure management of exit plans and transition activities. | This is a customer consideration. | N/A |
| 144. | A delimitation of which indicators in relation to the supplier's delivery are to be included in monitoring the outsourcing, including which indicators in relation to services are to trigger a situation where exit must be initiated. | This is a customer consideration. Refer to Row 83 for information about how you can monitor Google's performance of the Services (including the SLAs) | N/A |
| 145. | An impact assessment with the aim of finding out what human and financial resources will be required to implement the exit plan and how long it will take. | This is a customer consideration. | N/A |

# Danish FSA - Executive Order 877 on outsourcing for credit institutions

## Google Cloud Platform Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| 146. | Transition plans for how the outsourcing company implements transitions of outsourced processes, services, activities or data from the supplier and: | We recognize the importance of continuity for regulated entities and for this reason we are committed to data portability and open-source. Refer to our Engaging in a European dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on how Google's approach to open source can help you address vendor lock-in and concentration risk.<br><br>As part of your contingency planning, you can choose to use Anthos to build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. For more information, refer to the IDC Whitepaper on How A Multicloud Strategy Can Help Regulated Organizations Mitigate Risks In Cloud.<br><br>Refer to Row 124 to 126 for information about the transition support that Google provides. | N/A |
| 147. | transfer them to alternative suppliers, | See above. | N/A |
| 148. | transfers them to the outsourcing company or | See above. | N/A |
| 149. | take other measures to ensure the continuous delivery of the process, service or activity in a controlled and adequately tested manner. | See above. | N/A |
| 150. | The transition plans, cf. Annex 4, no. 3, letter f, must contain the necessary measures to ensure business continuity in the transition phase, including taking into account any challenges due to the data site. | See above. | N/A |
| 151. | The transition plans, cf. Annex 4, No. 3, letter f, must contain success criteria for the transfer of outsourced processes, services, activities and data. | See above. | N/A |