Google Cloud

Questions	Answers
Information about the respondent	
A. Name of respondent institution/firm	Google Cloud
B. Name of representative individual submitting response	Ksenia Duxtield-Karyakina, Government Affairs and Public Policy Manager, EMEA
C. Email address of representative individual submitting response	kseniak@google.com
D. Do you request non-publication of any part(s) of this response? If so, which part(s)? *Unless non-publication (in part or whole) is specifically requested, all consultation responses will be published in full on the FSB's website. An automated e-mail confidentiality claim will not suffice for these purposes.*	No
E. Would you like your response to be confidential (i.e. not posted on the FSB website)?	No
Consultation questions	
General questions	
1. Have you learnt any lessons from the COVID-19 pandemic and related cyber activity that will contribute to your cyber incident response and recovery practices?	The COVID-19 pandemic has accelerated many trends in technology adoption in the financial services sector, and accentuated the benefits of migration to the cloud to improve financial services institutions' operational resilience and security capabilities. A few key finds that we believe are most important in this context are as follows: 1) **Accelerated move to digital and impact on the operations and culture of the industry**: the pace of digital adoption increased in the course of the pandemic in the financial services with consumers shifting to digital banking channels at an unprecedented rate, and capital markets firms having to deal with extraordinary volatility. Many organisations had to move the entire workforce to remote working overnight

	and shift to primarily digital engagement with their customers. These changes have posed new challenges to the firms' resilience and security of their operations including diversified use of devices and online collaboration platforms. 2) **Security is as important as ever**, and we have seen new attacks and COVID-19 related scams since the breakout of the pandemic. Google security teams have worked to analyse the emerging threats, and to guide our customers through additional protection measures we've been implementing. A few examples are below. Google's Threat Analysis Group (TAG), a specialized team of security experts that works to identify, report, and stop government-backed phishing and hacking against Google and the people who use our products, shared their findings and the threats we're seeing in relation to COVID-19: ● Across Google products, we're seeing bad actors use COVID-related themes to create urgency so that people respond to phishing attacks and scams. Our security systems have detected examples ranging from fake solicitations for charities and NGOs, to messages that try to mimic employer communications to employees working from home, to websites posing as official government pages and public health agencies. ● In April, our systems detected 18 million malware and phishing Gmail messages per day related to COVID-19, in addition to more than 240 million COVID-related daily spam messages. ● Our machine learning models have evolved to understand and filter these threats, and we continue to block more than 99.9 percent of spam, phishing and malware from reaching our users. ● TAG has specifically identified over a dozen government-backed attacker groups using COVID-19 themes as lure for phishing and malware attempts—trying to get their targets to click malicious links and download files. ● One notable campaign attempted to target personal accounts of U.S. government

	employees with phishing lures using American fast food franchises and COVID-19 messaging. The vast majority of these messages were sent to spam without any user ever seeing them, and we were able to preemptively block the domains using Safe Browsing. ● Our team also found new, COVID-19-specific targeting of international health organizations, including activity that corroborates reporting in Reuters earlier this month and is consistent with the threat actor group often referred to as Charming Kitten. ● Generally, we're not seeing an overall rise in phishing attacks by government-backed groups; this is just a change in tactics. You can see TAG's findings in more detail here. Some other examples of our recent security efforts are as follows: ● **Protecting Against Covid Scams on G Suite:** bad actors are creating new attacks and scams every day that attempt to take advantage of the uncertainty surrounding the pandemic. Every day, Gmail blocks more than 100 million phishing emails. In the current environment, we are seeing new examples of malware and phishing emails related to COVID-19 - in addition to hundreds of millions COVID-related daily spam messages. Our ML models have evolved to understand and filter these threats, and we continue to block more than 99.9% of spam, phishing, and malware from reaching our users. In this blogpost we are giving some concrete examples of the new types of attacks we are seeing, and how we are improving our security capabilities to proactively address those, as well as sharing broader best practices for our customers and industry peers. In addition, this newly created online resource identifies different ways of how users can protect themselves against the emerging attacks. ● **BeyondCorp Remote Access:** as the number of remote workers increases drastically in a short period of time, organisations need an easier way to provide access to key internal applications which would normally be accessible through a browser on the corporate network in

	an office. To help customers solve this problem and get their workers the access they need, we introduced BeyondCorp Remote Access. This cloud solution—based on the zero-trust approach we've used internally for almost a decade—lets employees and extended workforce access internal web apps from any device, anywhere, without a traditional remote-access VPN. Over time, we plan to offer the same capability, control, and additional protections for any application or resource a user needs to access. ● **Vulnerability Research Grants and Rewards Program (VRP)**: when working to identify and prevent threats, we use a combination of internal investigative tools, information sharing with industry partners and law enforcement, as well as leads and intelligence from third-party researchers. To help support this broader security researcher community, Google is providing more than $200,000 in grants as part of a new Vulnerability Research Grant COVID-19 fund for Google VRP researchers who help identify various vulnerabilities. As part of this program, we are also awarding our most active VRP Bug Hunters additional 1000+ USD leet grants. We are doing so in recognition of the individual challenges COVID-19 has on the research community, and we hope these grants will support our Bug Hunters during these uncertain times. The grants themselves may be used to support security and anti-abuse research related to COVID-19. 3) **Cloud providers have continued to demonstrate resilience and enhanced cybersecurity capabilities** in the course of the pandemic with no shortfalls in our network, compute or customer support capacity. All our technical and personnel readiness steps implemented in response to the pandemic are from our standard playbooks, which were written and have been tested for exactly this type of scenario, well ahead of the crisis. This is strong evidence of how transition to the public cloud can help improve financial services operational resilience - not increase financial

	stability risks. The geographic scale, redundancy and distribution of our architecture - as well as the principles of openness, portability, and interoperability - are critical to support our customers' resilience and address regulator concerns on the single point of failure. Modern, digital, cloud-based infrastructure is going to be key to driving ongoing safe and secure innovation and productivity within the financial services sector, for the benefit of consumers and the economy at large. We believe that in the long term the greater risk will come from not moving to cloud and not embracing digital. This is something that the IIF have indicated in their Cloud Computing Paper series[1] first in 2018, and now the COVID-19 industry experience is proving this statement.
2. To whom do you think this document should be addressed within your organisation?	N/A
3. How does your organisation link cyber incident response and recovery with the organisation's business? Does your organisation follow international standards or common frameworks? If so, which international standards or common frameworks?	We understand that this question is addressed to financial services institutions. As an infrastructure provider, we are submitting a response describing these practices within our organisation which are important to the financial services customers that we support. As a public cloud service provider, Google Cloud has a rigorous cyber-risk management system across our organisation which is ultimately designed to deliver better security and protection for our customers across all verticals (including financial services customers) - compared to many traditional on-premises solutions. The risk management and security processes and capabilities that third party providers can offer to their financial services customers are critical in understanding the nature of outsourcing to public cloud in the first place. We believe, and this is confirmed by independent research, that security protections of public cloud are better than those available on premise. From this perspective, transition to cloud helps increase security - not increase the risk for financial services institutions. These considerations substantiated by technical evidence below are critically important for the regulators and policymakers to take into account when they formulate their assessment of outsourcing to third party providers in the context of public cloud.

[1] https://www.iif.com/Publications/ID/780/PageID/780/IIF-Cloud-Computing-paper-Part-1

	Security drives our organizational structure, training priorities and hiring processes, and we implement risk management processes throughout our culture, operational controls, technical security controls, and transparency. Google has a dedicated security team who are part of our software engineering and operations division. The Google privacy team participates in every Google product launch by reviewing design documentation and performing code reviews to ensure that privacy requirements are followed. Vulnerability Management, Malware protection, Monitoring, and Incident response are fundamental issues of Google's operational security. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in-house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. Incident response is a key aspect of Google's overall security and privacy program. We have a rigorous process for managing data incidents. This process specifies actions, escalations, mitigation, resolution, and notification of any potential incidents impacting the confidentiality, integrity, or availability of customer data. Google's processes are tested on a regular basis as part of our ISO-27017, ISO-27018, ISO-27001, PCI-DSS, SOC 2 and FedRAMP programs to provide our customers and regulators with independent verification of our security, privacy, and compliance controls. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and

	software vulnerabilities. Our incident response whitepaper details Google's end-to-end process. Google Cloud runs on a technology platform that is conceived, designed and built to operate securely. We custom-designed our servers, proprietary operating system, and geographically distributed data centers. Using the principles of "defense in depth," we've created an IT infrastructure that is more secure and easier to manage than more traditional technologies. The security of Google infrastructure is designed in progressive layers starting from the physical security of data centers, continuing on to the security of the hardware and software that underlie the infrastructure, and finally, the technical constraints and processes in place to support operational security. Google undergoes regular and independent, third-party audits and certifications to verify that our data protection practices match our commitments. In addition to certifications, Google adheres to globally recognized regulations such as GDPR and frameworks such as ISO 27018 or NIST SP 800-53. Google provides Cloud Compliance & Regulations Resources for all certifications, regulations, and frameworks. Google has established Data Processing and Security Terms that state a minimum set of certifications for a published list of Audited Services in order to evaluate the continued effectiveness of the Security Measures. Google's Third Party Auditor and updated annually based on an audit performed at least once every 12 months.

4. Does your organisation structure its cyber incident response and recovery activities along the seven components set out in the FSB toolkit? Please describe any additional components your organisation considers.	Although not directly structured along the FSB toolkit, our incident response and recovery activities contain many of the same concepts. Our incidents response and recovery activities contain the following:
	
	● **Identification**
	  ○ **Detection**
	  ○ **Reporting**
	● **Coordination**
	  ○ **Triage**
	  ○ **Response team engagement**
	● **Resolution**
	  ○ **Investigation**
	  ○ **Containment and recovery**
	  ○ **Communication**

	● **Closure** ○ **Lessons learned** ● **Continuous improvement** ○ **Program development** ○ **Prevention**
5. Based on your organisation's experience, please provide any additional effective practice(s) for any of the tools. Please list the number of the tool (e.g. Tools 1 – 46) and describe the effective practice(s).	N/A
6. Based on your organisation's experience, please provide additional examples of effective practices listed in the boxes (e.g. Boxes 1-6).	N/A
7. What role, if any, should authorities play in supporting an organisation's cyber incident response and recovery activities?	Regulators and supervisory authorities need to work together and with the industry to ensure harmonisation of incident reporting requirements based on joint taxonomy and internationally recognised standards and best practices. Duplication and fragmentation of the reporting requirements (including parallel reporting) on the national and global levels is ultimately damaging for the efficiency of incident response and recovery as it takes away the resources that the organisations need to allocate to dealing with the said incidents in the immediate terms. This challenge is particularly acute in the European context, and is currently being addressed as part of ongoing discussion on the Digital Operational Resilience legislative proposal. Coordination and effective information sharing between the competent supervisory authorities is therefore critical for operational international collaboration and to reduce the burden of multiple incident reporting by the financial services institutions.
● **Governance**	
●.1 To what extent does your organisation designate roles and responsibilities as described in Tool 3? Does your organisation identify these roles by business line, technology application or department?	Google's incident response program is managed by teams of expert incident responders across many specialized functions to ensure each response is well-tailored to the challenges presented by each incident. Depending on the nature of the incident, the professional response team may include: ● Cloud incident management ● Product engineering ● Site reliability engineering ● Cloud security and privacy

	● Digital forensics ● Global investigations ● Signals detection ● Security, privacy, and product counsel ● Trust and safety ● Counter abuse technology ● Customer support. Subject matter experts from these teams are engaged in a variety of ways. For example, incident commanders coordinate incident response and, when needed, the digital forensics team detects ongoing attacks and performs forensic investigations. Product engineers work to limit the impact on customers and provide solutions to fix the affected product(s). The legal team works with members of the appropriate security and privacy team to implement Google's strategy on evidence collection, engage with law enforcement and government regulators in line with the applicable regulation, and advise on legal issues and requirements. Support personnel respond to customer inquiries and requests for additional information and assistance.
●.2 How does your organisation promote a non-punitive culture to avoid "too little too late" failures and accelerate information sharing and CIRR activities?	Google has created a vibrant and inclusive security culture for all employees. The influence of this culture is apparent during the hiring process, employee onboarding, as part of ongoing training and in company-wide events to raise awareness and information sharing within in teams. Security drives our organizational structure, training priorities and hiring processes. Google has a strong and structured learning culture. All teams that participate in the disaster recovery exercise develop testing plans and post mortems which document the results and lessons learned from the tests. All incidents are the object of post mortems where the incident impact and response are documented in detail, root causes are analyzed and action items are identified, and, later, verified contributing to a healthy continuous improvement cycle. In addition, Google conducts regular (weekly to monthly) operational practice tests, where incidents (real or anticipated) are simulated and need to be responded appropriately with minimal service disruption. The operational team is thus trained

	through practice and procedures are kept up to date to maintain a high level of operational readiness. Beyond team-level activities, Google also exercises disaster recovery (DiRT) company-wide to ensure coordination across products and to measure the response effectiveness.
● **Preparation**	
●.1 What tools and processes does your organisation have to deploy during the first days of a cyber incident?	Google's incident detection team employs advanced detection tools, signals, and alert mechanisms that provide early indication of potential incidents. Google's sources of incident detection include: ● Automated network and system logs analysis — Automated analysis of network traffic and system access helps identify suspicious, abusive, or unauthorized activity and escalates to Google's security staff; ● Testing — Google's security team actively scans for security threats using penetration tests, quality assurance (QA) measures, intrusion detection, and software security reviews; ● Internal code reviews — Source code review discovers hidden vulnerabilities, design flaws, and verifies if key security controls are implemented; ● Product-specific tooling and processes — Automated tooling specific to the team function is employed wherever possible to enhance Google's ability to detect incidents at product level; ● Usage anomaly detection — Google employs many layers of machine learning systems to differentiate between safe and anomalous user activity across browsers, devices, application logins, and other usage events; ● Data center and / or workplace services security alerts — Security alerts in data centers scan for incidents that might affect the company's infrastructure; ● Google employees — A Google employee detects an anomaly and reports it; ● Google's vulnerability reward program — Potential technical vulnerabilities in Google-owned browser extensions, mobile, and web applications that affect the confidentiality

	or integrity of user data are sometimes reported by external security researchers. When we declare an incident, we designate an incident commander who coordinates incident response and resolution. The incident commander selects specialists from different teams and forms a response team. A typical view of our response organization appears in our whitepaper on incident response https://cloud.google.com/security/incident-response. As described above, scenario planning and stress testing is a critical part of the preparation measures at Google. We understand that the FSB recommends that firms may need to conduct their testing exercises in cooperation with their third-party providers. Whilst we agree that cooperation is important, it needs to take into account the nature and technological reality of cloud services, in particular that they are a one-to-many multi-tenant environment and they provide tools to customers to perform independent testing. For example, a public cloud provider cannot simulate a disruption of its service to support a single customer's testing because this could impact the integrity and security of the operations of other customers of the same provider. At the same time, cloud services do allow customers to simulate disruptions of their own cloud resources in a way that would allow customers to perform testing independently. If collaborative testing is required it is critically important that such exercises remain voluntary, risk-based and bilaterally agreed upon between the customers and their providers.
●.2 Please provide an example of how your organisation has enhanced its cyber incident response plan over the last 12 months.	At Google, we strive to learn from every incident and implement preventative measures to avoid future incidents. The actionable insights from incident analysis enable us to enhance our tools, trainings and processes, Google's overall security and privacy data protection program, security policies, and / or response efforts. The key learnings also facilitate prioritization of engineering efforts and building of better products. Due to the sensitive nature we do not provide specific details.

●.3	How does your organisation monitor, manage and mitigate risks stemming from third-party service providers (supply chain)?	N/A
●	**Analysis**	
●.1	Could you share your organisation's cyber incident analysis taxonomy and severity framework?	Many aspects of Google's response depend on the assessment of severity, which is based on the key facts that are gathered and analyzed by the incident response team. These may include: ● Potential for harm to customers, third parties, and Google; ● Nature of the incident (e.g., whether data was potentially destroyed, accessed, or unavailable); ● Type of data that may be affected; ● Impact of the incident on customers' use of the service; ● Status of the incident (e.g., whether the incident is isolated, continuing, or contained) It is important that organisations, both firms, and their providers, use internationally recognised taxonomy.
●.1	What are the inputs that would be required to facilitate the analysis of a cyber incident?	Please see above
●.2	What additional tools could be useful to analyse the effectiveness of cyber incident response and recovery activities and the severity, impact and root cause of cyber incidents?	N/A
●.3	What sector associations does your organisation participate in and what benefit does your organisations accrue from that participation?	Google Cloud is a member of UK Finance, AFME, IIF, ASIFMA, and the Center for Financial Industry Information Systems (FISC) in Japan, an active participant of the European Banking Federation Cloud Forum; from security perspective we are members of the Cloud Security Alliance, ISMS Forum, Spanish Association for Cybersecurity, DEUTSCHLAND SICHER IM NETZ and the BSI's ALLIANZ FÜR CYBERSICHERHEIT in Germany, and Cybermalveillance France. We are also contributing to ENISA's efforts around a security certification scheme for cloud services in the context of the EU Cybersecurity Act. We believe industry collaboration, including through the associations bringing together financial services firms and their providers, is critical to ensure effective exchange of

	information and sharing of best practices, and broader sectorial alignment.
• **Mitigation**	
●.1 Besides reducing impact to business and system security, what are other considerations that need to be taken into account during mitigation?	A key aspect of remediation is notifying customers when incidents impact their data. Key facts are evaluated throughout the incident to determine whether the incident affected customers' data. If notifying customers is appropriate, the incident commander initiates the notification process.
●.2 What tools or effective practices does your organisation have related to mitigating the impact from: (i) data breaches (ii) loss of data integrity and (iii) ransomware events?	

●.3 What tools or practices are effective for integrating the mitigation efforts of third-party service providers with the mitigation efforts of the organisation?	We note that as part of the **Business continuity measures,** the FSB toolkit recommends that organisations consider 'activating an alternative service provider if the primary service provider will not be able to recover from an incident within a certain period of time, as agreed in the respective SLA'. We agree that open and multi-cloud approach is critically important for financial services institutions and needs to formulate part of their long-term cloud strategy. At Google we have always been building for the open ecosystem and interoperability (eg Kubernetes - an industry wide cloud containerisation and application portability standard was originally developed by Google and is now completely open-sourced and independently managed by a nonprofit organisation). To further address this challenge, we introduced Anthos - a managed, cloud-native platform that helps organisations modernize their hybrid cloud environments and allows them to run their applications on any public cloud (not just Google Cloud). However choosing a multi-cloud strategy needs to remain a business decision based on an individualised risk assessment of each workload by financial institutions. Given that many financial services institutions are at a very early stage of their cloud adoption, a multiple cloud approach should be encouraged as a best risk-based practice at the FSB level but not mandated as a one-fits-all standard. Cloud providers should also be encouraged to support their customer choices, and make strong tangible commitments to open source, portability and transparency. Additionally testing exercises can also be conducted by the firms in a multi-cloud environment for additional resilience assurances.

●.4 What additional tools could be useful for including in the component Mitigation?	
●.5 Are there situations in which effective practices for mitigation and restoration activities of the organisation are the same or overlap substantially? If yes, please provide examples.	
• **Restoration**	
●.1 What tools and processes does your organisation have available for restoration?	
●.2 Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?	
●.3 How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?	
• **Improvement**	
●.1 What are the most effective types of exercises, drills and tests? Why are they considered effective?	Testing of incident response processes and procedures is essential and needs to be performed regularly for key areas. At Google such tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities and help us better prepare for security and privacy incidents.
●.2 What are the major impediments to establishing cross-sectoral and cross-border exercises?	N/A
●.3 Which technological aids and tools does your organisation consider most useful to improve cyber incident response and recovery?	Google's security and privacy professionals enhance the security program by reviewing the company's security plans for all networks, systems, and services and provide project-specific consulting services to product and engineering teams. They deploy machine learning, data analysis, and other novel techniques to monitor for suspicious activity on Google's networks, address information security threats, perform routine security evaluations and audits, and engage outside experts to conduct regular security assessments. Additionally, our full-time team, known as Project Zero, aims to prevent targeted attacks by reporting bugs to software vendors and filing them in an external database.
• **Coordination and Communication**	

●.1	Does your organisation distinguish “coordination activities” from broader “communication” in general? If yes, please describe the distinct nature of each component.	
●.2	How does your organisation address the possibility that email or traditional communication channels will be unavailable during a cyber incident?	
●.3	Apart from regulatory/compliance reporting, what other information does your organisation consider useful to share with authorities?	