Digital Operational Resilience Framework for Financial Services: Making the EU Financial Sector More Secure

Submission by Barclays

Barclays is a British universal bank. We are diversified by business, by different types of customers and clients, and by geography. Our businesses include consumer banking and payments operations around the world, as well as a top-tier, full service, global corporate and investment bank, all of which are supported by our service company which provides technology, operations and functional services across the Group.

Executive Summary

Barclays welcomes the opportunity to respond to this consultation from the European Commission. We initially provide an overview of our approach to digital operational resilience and the Commission's proposals, before responding to the Commission's questions.

Barclays Approach to Digital Operational Resilience

Cyber security and resilience are top priorities for Barclays. We are a mature organisation with a comprehensive approach to digital operational resilience and strong capabilities in all stages of the security incident management cycle. Barclays continues to develop its security and resilience capabilities through the Barclays Security Shield strategic framework that drives all security activity to keep our customers, colleagues and clients safe, secure and ensures services are highly available. Barclays Security Shield is sponsored by our Group Board and has full support of our Executive Management team. Indeed, nearly one quarter of Barclays' global workforce of 85,000 is dedicated to technology and security. To ensure 24/7 around-the-clock security and ICT resilience, we operate a network of Joint Operation Centres around the world with state-of-the-art technology and highly trained staff to monitor, track, and handle technology issues and cyber threats.

Barclays approach to Resilience, more broadly, is to deliver within the bank's Enterprise Risk Management Framework (ERMF) and Barclays Control Framework to ensure that Resilience, Cyber and Data risks are assessed, understood and managed appropriately and consistently as set out in Barclays' Operational Risk Frameworks.

Barclays operates Resilience, Cyber and Data as a 'Risk Theme'. A Risk Theme is a material threat to Barclays, requiring a coordinated risk management approach. Risk Themes represent an exposure to risks that are linked either by a common threat, the overall consequence (if they are not managed through an effective, coordinated and prioritised approach) or where a failure to manage change may trigger events⁄ increase risk exposure across a number of risk categories.

Barclays undertakes various types of testing exercises to gain assurance that resilience capabilities are designed and operating effectively. Exercises are undertaken at a frequency set out within Barclays' Resilience Standards, with post exercise learning being a key deliverable; we continue updating our resilience strategy, focusing on further maturing the authenticity and scale of our testing capabilities in line with plausible scenarios.

We believe our focus and approach is proving successful. We regularly successfully defend against both minor and significant cyber threats and, to date, none have had serious repercussions on clients or counterparties. However, to ensure our risk management tools and frameworks remain fit for purpose in an evolving external environment, we undertake regular external assurance exercises to assess and benchmark our resilience levels.

We are striving to develop a technology estate of modern infrastructure, constantly evaluating all of our systems from the perspective of how effectively they are able to serve our customer needs, and their resilience to modern threats.

Barclays Perspective on the Commission's Proposals

Barclays recognises that the increasing digitalisation of the financial services sector raises the importance of ICT and security resilience for firms. We therefore welcome the Commission's intention to introduce a new framework aimed at improving the digital operational resilience of financial services firms across the EU. Barclays supports the Commission's intention to harmonise regulation and introduce minimum standards for digital operational resilience management, to ensure provisions can be implemented proportionally, across firms of various size and complexity across all Member States. We believe these objectives can be best achieved through a principles-based framework providing guidance and base-level standards all financial services firms should aim to meet as a minimum. Policymakers should avoid a prescriptive, rules-based framework that may prove overly rigid and lack proportionality for firms to implement appropriately for their business.

Finally, wherever possible, the Commission should look to align any new framework with, or seek to incorporate within the framework, any existing global standards that relate to ICT and security risk management. For instance, the Commission may wish to build upon existing frameworks used by the European Central Bank for cyber incident management or the Basel Committee on Banking Supervision's Operational Resilience Group's expected publication on definitions and guidance.

We provide below a high level overview of our views on the specific 'building blocks' of the Commission's proposed framework.

Reporting

On reporting, the Commission is considering the introduction of a comprehensive, harmonized system of ICT incident reporting requirements for the financial services sector, in which reporting templates, timeframes and taxonomies would be standardised where possible and the relationship between existing reporting requirements would be clarified. The Commission believes this would enable firms to report more accurate and timely information to regulators.

Barclays welcomes the Commission's intention to reduce the fragmentation of ICT incident reporting requirements by introducing a harmonised EU-wide reporting framework for financial entities. There are currently various different incident reporting requirements under different pieces of EU legislation. Firms may be required to inform multiple regulators about a single incident, often complying with different templates, reporting thresholds, timescales. A single harmonised reporting framework would introduce greater efficiency and reduce the burden of reporting for firms, which currently may draw resource away from actually responding to an incident. For policymakers and regulators, greater standardisation of incident reports would enable higher quality analysis and improve real-team collaboration between firms and regulators during a critical incident.

Barclays would urge policymakers to explore whether a mechanism could be created that would enable firms to report an incident only once through a single channel, but have it go to multiple regulators. For example, a central reporting system in which firms can select which regulators or bodies an incident should be reported to. As well as harmonising reporting templates and timeframes, Barclays would urge the Commission to harmonise the taxonomy and materiality thresholds for reportable incidents: currently, firms may take different interpretations as to when an incident is reportable, potentially leaving regulators with a skewed understanding of the threat landscape. Finally, Barclays believes any new harmonised reporting framework should also involve greater sharing of information from regulators back to firms.

Testing

The Commission states that financial institutions must regularly assess the effectiveness of their preventative, detection and response capabilities to uncover and address vulnerabilities. It is considering introducing a multi-stage approach to raising digital operational resilience across the EU. In the short term, it would focus on setting a common denominator requiring all firms to perform basic assessment of their vulnerabilities. In the medium term, it is considering a cyber-resilience testing framework for all sectors based on common guidance that could lead to mutual acceptance of test results across all EU regulators.

Barclays believes that, as part of a comprehensive approach to ICT security risk, all financial entities should undertake regular testing and assessment of their ICT security. Barclays therefore supports efforts to establish a common denominator requiring basic assessment of systems by firms. However, regarding the more advanced testing proposed for firms deemed 'significant', Barclays would caution against any new EU framework introducing prescriptive rules governing how firms undertake their testing activity. Instead, any framework should take a principles-based approach providing guidance on industry best practice to be assessed as part of the ICT & Security SREP.

Oversight of ICT Third Party Providers

Regarding oversight of ICT third party providers, the Commission states that outsourcing to third party providers could also mean transfer of risks, and may lead to legal or compliance issues with the third party. It also notes the potential for concentration risk in the major ICT third party provider market. It is therefore considering introducing general principles in its new framework to guide firms in their contractual negotiations with third parties, and to provide better oversight of any risk that may stem from third parties.

Barclays uses a number of significant ICT third party service providers, including cloud service providers. To ensure our own digital operational resilience, and to ensure we maintain our regulatory obligations, we negotiate contractual terms with third party service providers, in line with EBA guidelines that aim to manage and address any digital operational risk that outsourcing may create. While we do consider that policymakers and regulators could benefit from greater oversight of major ICT third party providers in the EU, we do not believe provisions to this effect should be included in this future framework for digital operational resilience in financial services.

Instead, the Commission should consider introducing a separate framework to specifically provide oversight of major ICT third party providers operating in the EU. This would provide regulators with direct oversight and visibility of their operations, and any potential for disruption or failure. Regarding the management of concentration risk in the ICT third party provider sector, Barclays would caution against any prescriptive requirements mandating multiple providers or rotation of providers, but would encourage the Commission to explore how they can leverage best practice guidance to encourage appropriate industry management of any concentration risk.

Information sharing

The Commission states that the sharing of information - e.g. threat intelligence, tactics techniques and procedures, and indicators of compromise - between financial services firms can help the prevention of cyber-attacks and stop their spreading across the sector. It is therefore exploring whether the EU should seek to support the sharing of ICT security risk information between firms across the EU.

Barclays believes the EU should play a role in supporting and promoting the voluntary exchange of information between financial institutions. While in the UK various initiatives already exist to facilitate secure and trusted sharing of threat information between firms, other areas of the EU may be less advanced. EU policymakers should therefore explore how the benefits of these initiatives could be achieved at EU level. Ultimately, EU firms would benefit from a high level, cross-sectoral snapshot of live-threat information that can be acted on in their own defence and resilience activity. The EU should consider what role they can play to achieve this outcome.

Cyber Insurance

The Commission believes there is a need for firms and regulators to better understand the role of cyber security insurance within the context of digital operational resilience, and is therefore looking to further analyse the market and what role the EU can play to support for cyber insurance. We note the lack of a common taxonomy on cyber incidents, legal uncertainties around contractual terms and coverage as some of the challenges to the development of the cyber insurance market. We therefore welcome the Commission's intentions as firms increasingly consider obtaining cyber insurance as last resort protection in the event they may be impacted by an ICT incident.

Nomenclature

Consistent nomenclature across jurisdictions is an important feature of the global regulatory system. Barclays would note that the focus of the consultation is predominantly on cyber security risk and cyber resilience. In other jurisdictions, such as the UK, the term 'digital operational resilience' has a broader focus which includes technology change and resilience.

Barclays would recommend that EU policymakers seek to align its nomenclature as much as possible with other jurisdictions to ensure consistent understanding across borders and to avoid confusion with other resilience initiatives. For the purposes of this consultation, Barclays has responded with the understanding that cyber security risk and resilience is the focus.

Consultation Questions

Section 1 – ICT and Security Requirements

1. **Taking into account the deep interconnectedness of the financial sector, its extensive reliance on ICT systems and the level of trust needed among financial actors, do you agree that all financial entities should have in place an ICT and security risk management framework based on key common principles?**
   - Yes
   - No
   - Don't know / no opinion

To the extent you deem it necessary, please explain your reasoning

The financial ecosystem operates increasingly on digital infrastructure. While this provides significant benefits to both firms and consumers, it also provides a new vector through which cyber criminals can threaten financial services firms and their customers. As the consultation notes, due to the interconnected nature of the ecosystem, a cyber-threat at one firm can quickly also impact other firms.

Barclays therefore supports the Commission's proposals that all financial entities should have in place an ICT and security risk management framework based on key common principles. We also welcome the introduction of more harmonised requirements across all EU member states in order to ensure that digital operational resilience standards are sufficiently high for all firms.

However, rather than introduce a rigid, prescriptive, and rules-based system, Barclays believes any new framework should follow a principles-based approach that ensures common minimum standards, but can be implemented proportionally, as appropriate, reflecting firms' size and complexity etc.

2. **Where in the context of the risk management cycle has your organisation until now faced most difficulties, gaps and flaws in relation to its ICT resilience and preparedness? Please rate each proposal from 1 to 5, 1 standing for 'not problematic' and 5 for 'highly problematic').**

Stage in the risk management cycle (or any other relevant related element)	1	2	3	4	5	Don't know /Not applicable
Identification		X				
Detection		X				
Ability to protect		X				
Respond		X				
Recovery		X				
Learning and evolving		X				
Information sharing with other financial actors on threat intelligence	X					
Internal coordination (within the organisation)		X				
Other (please specify)						

To the extent you deem it necessary, please explain your reasoning.

Barclays is a mature organisation with a comprehensive approach to digital operational resilience and ICT and security risk management, providing strong capability in all the areas identified above. Through our Enterprise Risk Management framework, we have established procedures, policies, standards and controls that provide a high level of ICT and security resilience. There are various different standards frameworks (the NIST Cybersecurity Framework, ISO, and the CPMI-IOSCO Guidance) that seek to provide guidance on cybersecurity risk management, and we note that these can overlap and are sometimes functionally equivalent in places.

Barclays is adopting, embedding and where necessary extending the NIST framework to ensure that security and resilience maturity in Barclays can be rigorously assessed and continuously strengthened. Barclays also instructed PwC to complete a comprehensive Operational Resilience review in 2019 and is using recommendations to drive improvements as part of the Barclays Resilience Programme. Barclays would suggest that policymakers seek to align the provisions in any new EU framework with the standards in these international frameworks, to avoid any risk of diverging requirements. Policymakers should also consider how the Financial Services Sector Cyber Security Profile (FSCCP) could be incorporated in, or used as the basis for, any new EU framework. Barclays would suggest that policymakers seek to align the provisions in any new EU framework with the standards in these international frameworks, to avoid any risk of diverging requirements.

Policymakers should also consider how the Financial Services Sector Cyber Security Profile (FSCCP) could be incorporated in, or used as the basis for, any new EU framework. The FSCCP is an important mapping tool, as it allows firms to reconcile various cyber risk management frameworks and demonstrate regulatory compliance. Firms often face more difficulties, not via specific difficulties in the different stages of the risk management cycle, but by reconciling between the different cyber risk management frameworks.

3. **What level of involvement and/or what type of support/ measure has the Board (or more generally the senior management within your organisation) offered or put in place/provided for, in order to allow the relevant ICT teams to effectively manage the ICT and security risk? Please rate each proposal from 1 to 5, 1 standing for 'no support/ no measure' and 5 for 'high support/very comprehensive measures').**

Type of involvement, support or measure	1	2	3	4	5	Don't know /Not applicable
Appropriate allocation of human and financial resources					X	
Appropriate investment policy in relation to the ICT and security risks				X		
Approval by the Board of an ICT strategy (that also deals with ICT security aspects)					X	

Active role of the Board (or the senior management) when your organisation faces major cyber incidents or, as the case may be, role of the Board in the ICT business continuity policy					X	
Top leadership and guidance received in relation to ICT security and ICT risks				X		
Other (please specify)						

To the extent you deem it necessary, please explain your reasoning and emphasize in addition any type of support and measure that you consider that you consider the Board and senior management should provide.

Operational resilience, including digital operational resilience, ICT and security risk, is a top priority for Barclays, with full support from the Board and the Executive Management team. Barclays completed its Board-sponsored Security Program in 2019, which was a multi-year programme successfully placing Barclays in the top quartile of all organisations from a Cyber security perspective - as also benchmarked externally by Leidos/Cap Gemini. We continue to develop our security and resilience capabilities through the Barclays Security Shield strategic framework that drives all security activity to keep our customers, colleagues and clients safe, secure and ensures services are highly available.

Barclays operates a multi-layer/ multi-discipline Incident and Crisis Management Framework. Requirements for Incident Management and Crisis Management are set out in Operational Risk Policies and Standards. Barclays operates a 24 x 7 x 365 incident management capabilities and crisis capabilities regionally, within Business Unites and an overarching Barclays Crisis Leadership Team. Incident and Crisis Management capabilities are regularly tested and assessed for effectiveness through a range of exercises, scenarios and invocations.

4. How is the ICT risk management function implemented in your organisation? To the extent you deem it necessary, please explain your reasoning.

Barclays approach to Resilience is to deliver within the bank's Enterprise Risk Management Framework (ERMF) and Barclays Control Framework to ensure that Resilience risks are assessed, understood and managed appropriately and consistently as set out in Barclays' Operational Risk Frameworks.

We undertake various types of testing exercises to gain assurance that resilience capabilities are designed and operating effectively. Exercises are undertaken at a frequency set out within the Resilience Standards with post exercise learning being a key deliverable.

We have also sought to identify and understand our most critical banking services, and the internal processes that exist to support and fulfil any customer requests: Barclays undertakes a Service and Business Impact Assessment to assess the criticality of its most important business services, which Barclays refers to as 'Front-to-Back-Process' (F2BP).

The Service section of the assessment determines their Resilience Category (Res Cat), reviews Service Level Agreements, cut-off times and any defined Minimum Operating Levels. The Business Impact section utilises the Barclays Risks & Issues Classification Matrix (RICM) and a 24-hour outage scenario to evaluate the potential impact on Financial, Customer, Colleague, Reputational and Regulatory impact. Based upon these impacts a Resilience Category is assigned to each F2BP. Barclays uses Resilience Categories to define the criticality of F2BPs. Resilience Categories are defined using a Risk and Issues Classification Matrix (RICM) which defines Risk and Issue materiality on the basis of impacts at Barclays Group level. The scale of Resilience Categories ranges from 0 being the highest to 4 being the lowest.

Barclays considers the F2BPs assessed as Resilience Categories 0 & 1 as the critical processes. Resilience Categories also have correlating Recovery Time Objectives (RTO). The higher the Resilience Category the shorter the RTO. Each F2BP is assigned to Senior Accountable Executive who is responsible for ensuring its resilience and that regular testing is undertaken. A F2BP includes customer journeys, end-to-end processes, product lines, key internal supporting processes and covers delivery channels (physical or virtual, internal and external). They are not bound by legal entity, functional or organisational boundaries and where applicable, they are aligned to Critical Economic Functions (CEFs) defined by the UK Regulatory Authorities.

As part of this approach, Barclays' Business Units are required to ensure the following:

- An inventory of F2BPs is identified and maintained
- The criticality of each F2BP is assessed using the Risk and Issues Classification Matrix (within the Business Impact Assessments).
- Dependencies (such as people, technology, suppliers) are mapped and their resilience requirements set.
- These resilience requirements are mandated in our Standards and Controls and include a requirement for annual review. These outputs from these Controls drive Management Risk Reporting and any necessary remediation activity, and includes RTO, RPO and tolerable downtime.

Barclays also operates a multi-layer/multi-discipline Incident and Crisis Management Framework. Requirements for Incident Management and Crisis Management are set out in Operational Risk Policies and Standards. Barclays operates a 24 x 7 x 365 incident management capabilities and crisis capabilities regionally, within Business Units and an overarching Barclays Crisis Leadership Team. Incident and Crisis Management capabilities are regularly tested and assessed for effectiveness through a range of exercises, scenarios and invocations. Following a significant incident or a crisis, a relevant post-incident/post-crisis report is produced, with relevant 'lessons learnt' exercises also undertaken. All relevant learning points and remediation activity is then prioritised in order to effectively mitigate and remove any identified vulnerabilities. All issues are logged and remediated as per Barclays internal controls framework.

Barclays applies a consistent global approach to operational resilience and associated activities, including a standard process for assessing risk and impact across all jurisdictions. Where jurisdictions across the world take different approaches to operational resilience, Barclays seeks to incorporate

any regional regulations into our global approach to ensure our Group Resilience Policy is suitable across all jurisdictions.

5. **Which main arrangements, policies or measures you have in place to identify and detect ICT risks?**

Type of arrangement, policy, measure	Yes	No	Don't know /Not applicable
Do you establish and maintain updated a mapping of your organisation's business functions, roles and supporting processes?	X		
Do you have an up-to-date registry/inventory of supporting ICT assets (e.g. ICT systems, staff, contractors, third parties and dependencies on other internal and external systems and processes)?	X		
Do you classify the identified business functions, supporting processes and information assets based on their criticality?	X		
Do you map all access rights and credentials and do you use a strict role-based access policy?	X		
Do you conduct a risk assessment before deploying new ICT technologies / models?	X		
Other (please specify)			

To the extent you deem it necessary, please explain your reasoning.

Please refer to our response to Question 4.

6. **Have you experienced cyber-attacks with serious repercussions for your clients or counterparties?**
   - Yes
   - No
   - Don't know/Not applicable

To the extent you deem it necessary, please explain and illustrate in particular the nature of the attack and the impacts on the clients/counterparts.

Barclays regularly successfully defends against both minor and significant cyber-attacks. However, to date, none have had serious repercussions on clients or counterparties.

7. **How many cyber-attacks does your organisation face on average every year? How many of these have/are likely to create disruptions of the critical operations or services of your organisation?**

Please explain your reasoning.

As a major international bank, Barclays regularly faces threats from external actors. Most of these threats are routinely rebuffed automatically by our defence systems.

Occasionally, our specialist cyber security teams are required to resolve more challenging threats, however to date, none of these threats have caused disruption to our critical services.

8. **Do you consider that your ICT systems and tools are appropriate, regularly updated, tested and reviewed to withstand cyber-attacks or ICT disruptions and to assure their operational resilience? Which difference do you observe in this regard between in-house and outsourced ICT systems and tools?**
   - Yes
   - No
   - Don't know/Not applicable

To the extent you deem it necessary, please explain your reasoning.

Financial services firms are subject to various regulatory requirements that set out how they are expected to manage their ICT systems. These requirements subject firms to various controls and tests to ensure their systems can withstand and recover from external threats and operational disruptions. Barclays therefore considers that our ICT systems are appropriate and of a sufficiently high standard to defend against cyber threats and disruptions. However, to ensure our risk management frameworks and tools remain fit for purpose in an evolving external environment, Barclays undertakes regular external assurance exercises to assess and benchmark our resilience.

Barclays Chief Security Office maintains an increasingly active intelligence function that monitors trends in crime, terrorism, cyber threat developments and other threats to the Barclays business in general. Through the Joint Operations Centres (24 x 7 x 365) and a Technology Control Centre we are constantly scanning the environment for threats and taking mitigating action as appropriate. Further the Resilience Risk status is reported and reviewed quarterly at the various Resilience Council fora, which are attended by the Business Units' and the Risk Categories senior management that manage Resilience Risks. Barclays undertakes various types of testing exercises to gain assurance that resilience capabilities are designed and operating effectively. Exercises are undertaken at a frequency set out within Barclays' Resilience Standards with post exercise learning being a key deliverable.

With regard to outsourced ICT systems, Barclays utilises third party ICT suppliers to provide specific or specialist services. While financial services firms are directly subject to regulatory requirements, meaning their ICT systems and tools are required to meet certain standards, providers of outsourced ICT systems and tools may not be regulated in the same way and therefore could have lower levels of ICT resilience.

However, Barclays invest significant time and resource to minimise any impact outsourcing may have on Barclays' digital operational resilience and our ability to serve our customers.

- We have a robust supplier control programme that ensures assurance activities regarding supplier operated controls are carried out in a manner that is commensurate with the level of risk associated with the service being received from the supplier. Such assurance activities may involve supplier self-attestation questionnaires, supplier manager assurance

reviews, on-site reviews by our Global Supplier Assurance team, on-site reviews by Barclays' internal auditing teams, or a combination of these approaches.

- To manage the operational resilience of suppliers themselves, Barclays uses a consistent framework for resilience across our supplier network. Prior to contracting, Barclays carries out an assessment of the inherent risk associated with the service being received from the supplier. Depending on the nature of the service being delivered, suppliers are contractually obligated to manage risk in the supplier chain, e.g. ensure timely availability of IT applications and infrastructure, facilities, and people to ensure that service continuity plans are appropriately tested. Each supplier is also assigned a resilience rating, which would take into account their criticality to the provision of our banking services.

9. Has your organisation developed and established a cloud strategy?

- Yes
- No
- Don't know/no opinion

10. If the answer to the previous question (no. 9) is yes, please explain which of the following aspects are covered and how.

	Yes	No	Don't know /Not applicable
Do you use on-premise cloud technology?	X		
Do you use off-premise cloud technology?	X		
Does this strategy contribute to managing and mitigating ICT risks?	X		
Do you use multiple cloud service infrastructure providers? How many?		X	
Did your Board and senior management establish a competence center for cloud in your organisation?	X		

To the extent you deem it necessary, please explain your reasoning.

Technology plays an integral role in supporting our strategy to accelerate growth, deliver Group-wide efficiencies and create the capacity to invest in growth initiatives that will generate sustainable returns for Barclays.

Our Group Cloud Programme plays a fundamental part in creating this capacity, as well as providing a modern and flexible infrastructure for our customers and colleagues. Barclays has a multi-cloud strategy made up of three offerings: public cloud IAAS and SAAS; internal private cloud; and Barclays' on-premises physical and virtual hosting (how we host the majority of our applications today).

Cloud technology is laying the foundations for the next generation of banking, powering the technology behind our future products and services. It provides a fantastic opportunity for us to innovate.

11. Do you have legacy ICT systems that you would need to reconsider for enhanced ICT security requirements? What would be the level of investments needed (in relative or absolute terms)?

- Yes
- No
- Don't know / Not applicable

To the extent you deem it necessary, please explain your reasoning.

Barclays is a large complex organisation with many systems that have been developed organically over a long period of time. Barclays strives to develop a technology estate of modern systems with high levels of resilience and service provision for our customers. We are constantly evaluating all of our systems from the perspective of how effectively they are able to serve our customer needs and their resilience to modern threats. This is an organic and continuous process involving significant, and increasing investment, in both upgrading our existing technology estate, and in decommissioning elements that are no longer strategic to our banking services. These actions continue to create a more resilient, simplified, strategic technology estate, ensuring Barclays is well positioned to serve our customers and clients.

Barclays operates, manages, and maintains a number of core strategic technology platforms that underpin the banking services to our customers and clients. These platforms use a variety of technologies and are appropriately secured using strong controls to protect our customer and client information and transactions. While some systems may be less modern than others, our older systems are regularly tested to ensure they continue to provide high levels of security and resilience.

Barclays take an intelligence-led approach to vulnerability and patch management to identify, categorise, prioritise and orchestrate the remediation or mitigation of vulnerabilities. These include unsecured system configurations or missing patches, as well as other security-related updates in the systems connected to the enterprise network directly.

12. What in your view are possible causes of difficulties you experienced in a cyber-attack/ ICT operational resilience incident? Please rate each answer from 1 to 5, 1 standing for 'not problematic' and 5 for 'highly problematic').

Causes of difficulties	1	2	3	4	5	Don't know /Not applicable
ICT environmental complexity			X			
Issues with legacy systems		X				
Lack of analysis tools	X					
Lack of skilled staff	X					
Other (please specify)						

To the extent you deem it necessary, please explain your reasoning.

Please refer to our response in Question 11.

13. Do you consider that your organisation has implemented high standards of encryption?

- Yes
- No
- Don't know/Not Applicable

To the extent you deem it necessary, please explain your reasoning.

Barclays operates a defined set of standards to ensure high levels of encryption, based on risk assessment, and meets industry encryption standards as required. Where encryption is impossible, impractical or otherwise not used, Barclays refers to equivalent compensating controls.

14. Do you have a structured policy for ICT change management and regular patching and a detailed backup policy?

- Yes
- No
- Don't know/not Applicable

To the extent you deem it necessary, please explain your reasoning.

Barclays processes approximately 25,000 technology changes every month to ensure our systems stay ahead of a range of threats, trends, and customer demands. These changes are rigorously managed, and achieve a 99.8 per cent success rate. When incidents do occur, we seek to resolve them as efficiently as possible to minimise any impact on the customer. Even in the case of the 0.2 per cent of changes that are not executed in the way that we would wish, an even smaller fraction result in any noticeable impact on our customers.

We operate, manage, and maintain a number of core strategic technology platforms that underpin the banking services to our customers and clients. These platforms use a variety of technologies and are appropriately secured using strong controls to protect our customer and client information and transactions. As part of our regular control processes, Barclays ensures that the software we operate is maintained to the latest level of security, via a regime of regular updates.

Barclays believes that a principles and risk-based approach for how firms manage ICT change management and data backups would provide the flexibility needed while being commensurate to the risks, as the technology and threats evolves.

15. Do you consider that your organisation has established and implemented security measures to manage and mitigate ICT and security risks (e.g. organisation and governance, logical security, physical security, ICT operations security, security monitoring, information security reviews, assessment and testing, and/or information security training and awareness measures)?

- Yes
- No
- Don't know/Not applicable

To the extent you deem it necessary, please explain your reasoning and for which measures legal clarity and simplification would be needed.

As part of Barclays Enterprise Risk Management Framework, Barclays has implemented strong measures and frameworks to manage and mitigate ICT and security risks. In addition, firms are expected to meet the requirements set out by the EBA in the ICT guidelines.

16. On average, how quickly do you restore systems after ICT incidents, in particular after a serious/major cyber-attack? Are there any differences in that respect based on where the impact was (impact on the availability, confidentiality or rather the integrity of data)?

To the extent you deem it necessary, please specify and explain.

The vast majority of disruptions, regardless of cause, are resolved quickly and within the Recovery Time Objective (RTO) defined within Barclays' Technology and Resilience Standard, which also covers infrastructure failure / disaster recovery. However, in line with the approach defined by the UK regulators, Barclays is increasingly focusing on recovery from more extreme scenarios, such as wide-spread destructive and intrusive cyber-attacks. This work is still at an early stage, but will include planning for and testing against a wide range of severe but plausible scenarios in order to identify:

- gaps in recovery capability;
- opportunities to improve plans, processes and procedures;
- cross-business and cross-sector collaboration options for service substitution;
- alternate technical mechanisms for service delivery and recovery and;
- investment priorities.

The extent of testing will cover various types of impacts in relation to availability, confidentiality and integrity of data and systems as well as different scales of impact to validate which scenarios Barclays can recover from within the defined Impact Tolerance for the Service being tested (maximum tolerable period of disruption). Test outputs will be shared at Board level and will help shape future investment particularly in relation to recovery capability and service continuity.

However, it should be noted that recovery capability is not the only factor that would be considered with regard to incident management and RTOs: assessing firms' overall resilience position for incidents, it is important that the focus is not limited to recovery capability, but also considers the entire capability (prevention, detection, response, recovery).

We therefore would encourage EU policymakers to avoid inadvertently creating a culture whereby firms seek to restore systems as soon as possible in order that they can meet a regulatory RTO deadline. Firms should instead focus on restoring systems only with they are sufficiently safe, secure and stable. Policymakers should therefore consider how they can use an RTO in a principles based framework of minimum common standards and best practice guidelines, rather than as part of a prescriptive, rules based framework.

The Commission should, additionally, take into the consideration the planned Financial Stability Board public consultation on a toolkit of effective practices for cyber incident response and recovery this year. It is important that the Commission aligns to these global guidelines for any legislative proposals made.

17. Which issues you struggle most with, when trying to ensure a quick restoration of systems and the need to maintain continuity in the delivery of your (critical) business functions?

Issues	Yes	No	Don't know /Not applicable
Lack of comprehensive business continuity policy and/or recovery plans		X	
Difficulties to keep critical/ core business operations running and avoid shutting down completely		X	
Internal coordination issues (i.e. within your organisation) in the effective deployment of business continuity and recovery measures		X	
Lack of common contingency, response, resumption/recovery plans for cyber security scenarios - when more financial actors in your particular ecosystem are impacted		X	
No ex-ante determination of the precise required capacities allowing the continuous availability of the system		X	
Difficulties of the response teams to effectively engage with all relevant (i.e. business lines) teams in your organization to perform any needed mitigation and recovery actions		X	
Difficulty to isolate and disable affected information systems		X	
Other (please specify)			

To the extent you deem it necessary, please explain your reasoning.

Please refer to our response to Question Q16.

18. What are your views on having in the legislation a specific duration for the Recovery Time Objective (RTO) and having references to a Recovery Point Objective (RPO)?

To the extent you deem it necessary, please explain your reasoning.

Please refer to our response to Question Q16.

We urge regulators and policymakers to avoid creating perverse incentives for firms and FMIs when it comes to recovery from a real event. Impact Tolerances (maximum tolerable period of disruption) should be used for planning purposes rather than treated as an expected recovery target or service level.

An Impact Tolerance may be used to refine priorities, inform recovery plans and Incident Management processes, a baseline for testing and a mechanism for reporting recovery capability gaps. It is important that in real disruption events, firms focus on making recovery decisions carefully such that additional risk is not introduced within the financial system.

EU policymakers should therefore consider how they can encourage firms to incorporate an RTO as part of their ICT resilience, through a principles based framework of minimum common standards and best practice guidelines, rather than a prescriptive, rules based framework. It is important that any future framework maintains sufficient flexibility for firms to implement it proportionately, depending on the size and criticality of their services.

Policymakers should also look to align measures in any framework with other international standards in this space, for example, FSB work on incident response times.

19. Through which activities or measures do you incorporate lessons post-incidents and how do you enhance the cyber security awareness within your organisation?

	Yes	No	Don't know /Not applicable
Do you promote staff education on ICT and security risk through regular information sessions and/or trainings for employees?	X		
Do you regularly organize dedicated trainings for the Board members and senior management?	X		
Do you receive from the Board all the support you need for implementing effective cyber incident response and recovery improvement programs?	X		
Do you make sure that the root causes are identified and eliminated to prevent the occurrence of repeated incidents?	X		
Do you conduct ex post root cause analysis of cybersecurity incidents?	X		
Other (please specify)			

To the extent you deem it necessary, please explain your reasoning.

Following a significant incident or a crisis, a relevant post-incident/post-crisis report is produced, with relevant 'lessons learnt' exercises also undertaken. All relevant learning points and remediation activity is then prioritised in order to effectively mitigate and remove any identified vulnerabilities. All issues are then logged and remediated as per Barclays' internal controls framework.

Section 2: ICT and Security Incident Reporting Requirements

20. Is your organisation currently subject to ICT and security incident reporting requirements?

- Yes
- No
- Don't know/Not applicable

To the extent you deem it necessary, please explain your reasoning.

As a firm operating in the EU, Barclays is subject to the following EU regulatory cyber incident reporting requirements:

- NIS Directive: major incident reporting for operators of essential services
- GDPR: data breach notification
- eIDAS: incident reporting for trusted services providers
- PSD2: incident reporting for payment service providers
- ECB SSM: incident reporting for significant institutions
- Target 2: incident reporting for critical participants

In addition to the above EU regulatory requirements, we are also required to update national regulators in other jurisdictions in which we operate. For example, we are required to inform UK, Asian and US regulators of cyber incidents that cause material disruption to our services.

As a result, a firm could be required to inform multiple regulators about an incident, often under different pieces of regulation, and therefore complying with different templates, thresholds, and timescales.

***21.* Do you agree that a comprehensive and harmonised EU-wide system of ICT and security incident reporting should be designed for all financial entities?**

- Yes
- No
- Don't know

To the extent you deem it necessary, please explain your reasoning.

Barclays agrees that EU policymakers should look to introduce a harmonised EU-wide system of ICT and security incident reporting for financial entities. Such a framework would introduce greater efficiency and reduce the burden of reporting for firms during an incident, when resources may be needed most to respond and deal with an incident.

For policymakers and regulators, there would be benefit in terms of greater standardisation of incident reports from firms across the EU, thereby enabling higher quality analysis. A harmonised, more coordinated system of incident reporting could also improve real-team collaboration between firms and regulators during a critical incident, enabling firms to prepare for potential incidents yet to hit them.

Barclays would note that industry would benefit from greater information sharing from regulators back to the firms. Currently, firms report incidents to regulators, but there is no mechanism to

receive any aggregated information back to firms from the regulators. In any new incident reporting framework, policymakers should seek to create a more bilateral, two-way sharing of information. This sharing of information back to firms could form part of any information sharing framework, explored in section 5.

22. **If the answer to the previous question (no. 21) is yes, please explain which of the following elements should be harmonised?**

Elements to be harmonised in the EU-wide system of ICT incident reporting	Yes	No	Don't know /Not applicable
Taxonomy of reportable incidents	X		
Reporting templates	X		
Reporting timeframe	X		
Materiality thresholds	X		
Other (please specify)			

To the extent you deem it necessary, please explain your reasoning.

Please refer to responses provided in Question 20 and 21.

Furthermore, we encourage policymakers to look at harmonising the taxonomy and materiality of reportable incidents across the EU. Currently, firms may take different interpretations as to whether an incident is reportable to regulators. This can serve to skew regulators perceptions of the incident landscape, if some firms report many incidents regardless of size of impact, while others report only few. Harmonising the taxonomy and materiality would resolve this problem.

We would note that the Commission should look to align any incident reporting element of the new framework with international standards, to avoid creating an EU framework with diverging requirements.

23. **What level of detail would be required for the ICT and security incident reporting? Please elaborate on the information you find useful to report on, and what may be considered as unnecessary.**

To the extent you deem it necessary, please explain your reasoning.

Barclays has not answered this question.

24. **Should all incidents be within the scope of reporting, or should materiality thresholds be considered, whereby minor incidents would have to be logged and addressed by the entity but still remain unreported to the competent authority?**

- Yes
- No
- Don't know

To the extent you deem it necessary, please explain your reasoning.

Barclays considers that any new EU incident reporting framework should only require significant security incidents to be reported. Significant incidents could be determined using common materiality thresholds based on impacts to a firms' operations, systems, sensitive information and reputation. Firms should not be required to report all incidents, i.e. insignificant incidents below a materiality threshold. This would reduce the reporting burden on firms, and enable regulators to receive information only on significant incidents that require greater focus.

25. Which governance elements around ICT and security incident reporting would be needed? To which national competent authorities should ICT and security incidents be reported or should there be one single authority acting as an EU central hub/database?

To the extent you deem it necessary, please explain your reasoning.

Please refer to responses provided under Question 21 and 22.

26. **Should a standing mechanism to exchange incident reports among national competent authorities be set up?**

- Yes
- No
- Don't know

To the extent you deem it necessary, please explain your reasoning.

Please refer to our responses provided in Question 22 and 25.

27. What factors or requirements may currently hinder cross-border cooperation and information exchange on ICT and security incidents?

To the extent you deem it necessary, please explain your reasoning and provide concrete examples.

We note that firms may operate in multiple jurisdictions - both within, and outside the EU - and therefore engage with multiple regulators in those jurisdictions. As per our earlier responses, the reporting process in terms of templates, timeframes and channels may differ across different jurisdictions, as well as the style and content of reports. A new EU wide framework requiring a harmonised incident reports to be provided though one central channel would ease this issue, at least within the EU.

Beyond the EU, policymakers should look to ensure strong cooperation arrangements and relationships exist with regulators in other major jurisdictions

Section 3 - Digital Operational Resilience Testing Framework

28. Is your organisation currently subject to any ICT and security testing requirements?

- Yes
- No
- Don't know/not applicable

If the answer is yes:

	Yes	**No**	**Don't know / not applicable**
Do you face any issues with overlapping or diverging obligations?			
Do you practice ICT and security testing on a voluntary basis?			

To the extent you deem it necessary, please explain your reasoning.

Barclays undertakes ICT and security testing as part of various regulatory initiatives in the jurisdictions in which we operate. In the EU, the EBA's ICT guidelines include provisions on testing. The ECB also requires firms to test their systems and inform them of any risks. In the UK, Barclays also participates in the Bank of England's CBEST initiative which seeks to provide a controlled approach to security testing within the financial sector.

In the US, Barclays undertakes security testing in alignment with defined Barclays' controls, industry best-practices and relevant regulatory expectations. To ensure global consistency, Barclays would suggest that any new EU framework covering testing of ICT security should be aligned with recommendations provided by the FSB and the BIS.

***29.* Should all financial entities be required to perform a baseline testing/assessment of their ICT systems and tools? What could its different elements be?**

Different elements of a baseline testing/assessment framework	Yes	No	Don't know /Not applicable
Gap analyses?	X		
Compliance reviews?	X		
Vulnerability scans?	X		
Physical security reviews?	X		
Source code reviews?	X		
Other (please specify)			

To the extent you deem it necessary, please explain your reasoning.

Barclays believes that, as part of a comprehensive approach to ICT security risk, all financial entities should undertake regular testing and assessment of their ICT security. Barclays therefore supports efforts to establish a common denominator requiring basic assessment of systems by firms. The EBA ICT guidelines could be appropriate for baseline testing requirements.

30. **For the purpose of being subject to more advanced testing (e.g. threat led penetration testing, TLPT), should financial entities be identified at EU level (or should they be designated by competent authorities) as "significant" on the basis of a combination of criteria such as:**

Criteria	Yes	No	Don't know /Not applicable
Proportionality–related factors (i.e. size, type, profile, business model)?			X
Impact – related factor (criticality of services provided)?			X
Financial stability concerns (Systemic importance for the EU)?			X
Other appropriate qualitative or quantitative criteria and thresholds (please specify)?			

To the extent you deem it necessary, please explain your reasoning.

CBEST-style testing, or threat led penetration testing, can put a significant strain on resources and is therefore disruptive. Any testing performed by the regulator should be limited in frequency and should not conflict with other regulators performing similar testing.

We would like to note that should the Commission intend to subject certain financial firms deemed 'significant' to more advanced framework testing, we would suggest that firms deemed to be 'in scope' for more advanced requirements should be identified based on existing frameworks that already outline 'significant' institutions, e.g. ECB supervised firms, BCBS GSIBs, or firms deemed significant by member state authorities.

31. In case of more advanced testing (e.g. TLPT), should the following apply?

	Yes	No	Don't know /Not applicable
Should it be run on all functions?			X
Should it be focused on live production systems?			X
To deal with the issue of concentration of expertise in case of testing experts, should financial entities employ their own (internal) experts that are operationally independent in respect of the tested functions?			X
Should testers be certified, based on recognised international standards?			X
Should tests run outside the Union be recognised as equivalent if using the same parameters (and thus be 18 held valid for EU regulatory purposes)?	X		
Should there be one testing framework applicable across the Union? Would TIBER-EU be a good model?			X
Should the ESAs be directly involved in developing a harmonised testing framework (e.g. by issuing			X

guidelines, ensuring coordination)? Do you see a role for other EU bodies such as the ECB/SSM, ENISA or ESRB?			
Should more advanced testing (e.g. threat led penetration testing) be compulsory?			x

To the extent you deem it necessary, please explain your reasoning.

Whilst we agree that it is important for financial entities in the EU to perform some form of testing or assessment of their ICT systems, we do not believe any new EU framework should introduce prescriptive rules governing how firms undertake testing and assessment of their ICT security. Instead, any framework should take a principles-based approach providing guidance on industry best practice for testing. It is also important that any framework is able to adapt to the changing external threat environment.

As per our response provided under Q28, we urge EU policymakers to ensure that any new EU testing framework is aligned other international testing frameworks, such as the FSB and the BIS. Consistent frameworks across jurisdictions would allow policymakers and regulators to recognise tests and assessments undertaken outside the EU as 'equivalent' to those undertaken within EU. This would reduce the burden on firms having to undertake multiple assessments under different frameworks in different regimes.

32. **What would be the most efficient frequency of running such more advanced testing given their time and resource implications?**

- Every six months
- Every year
- Once every three years
- Other

To the extent you deem it necessary, please explain your reasoning.

Barclays believes the Commission should not seek to mandate a strict schedule for advanced testing, but should recommend that firms continuously monitor the sector and undertake regular testing exercises as appropriate. It is important that any testing framework allow firms sufficient time to plan, undertake and respond to testing appropriately. Testing should be limited in frequency and seek to ensure it does not conflict with other regulators performing similar tests.

33. **The updates that financial entities make based on the results of the digital operational testing can act as a catalyst for more cyber resilience and thus contribute to overall financial stability. Which of the following elements could have a prudential impact?**

	Yes	No	Don't know /Not applicable
The baseline testing/assessment tools (see question 29)?			X
More advanced testing (e.g. TLPT)?			X
Other (please specify)			X

Barclays has not responded to this question.

Section 4 - Addressing third party risk: Oversight of third party providers (including outsourcing)

34. What are the most prominent categories of ICT third party providers which your organisation uses?

To the extent you deem it necessary, please explain your reasoning.

The following are our top categories in order of spend:

1. IT Professional Services
2. IT Infrastructure
3. Networks and Telecoms
4. Enterprise Wide Software
5. Customer Facing Software

35. **Have you experienced difficulties during contractual negotiations between your organisation and any ICT third party providers, specifically with regard to establishing arrangements reflecting the outsourcing requirements of supervisory/regulatory authorities?**

- Yes
- No
- Don't know/not applicable

To the extent you deem it necessary, please explain your reasoning, elaborating on which specific outsourcing requirements were difficult to get reflected in the contract(s).

Barclays has strong governance frameworks in place to ensure that all regulatory requirements are satisfied when outsourcing to third party service providers. Barclays requires third parties to agree to these provisions before any outsourcing can be agreed.

Barclays has experienced certain challenges when seeking to establish outsourcing arrangements that satisfy regulatory requirements:

- Third-party providers may lack clarity and understanding of the regulatory requirements governing outsourcing of services (i.e. disagreements as to whether a third-party complies with certain provisions)
- Whilst the EBA's outsourcing guidelines are global in application, however, third-party providers in third countries (e.g. USA) may be unaware of such requirements and therefore reluctant to comply.
- While direct third-party suppliers may be willing to comply with relevant requirements, a supplier may have limited leverage to require their subcontractors to comply with the same requirements.

36. **As part of the Commission's work on Standard Contractual Clauses for cloud arrangements with financial sector entities, which outsourcing requirements best lend themselves for standardisation in voluntary contract clauses between financial entities and ICT third party service providers (e.g. cloud)?**

To the extent you deem it necessary, please explain your reasoning

Barclays' position regarding the Commission's work on Standard Contractual Clauses for cloud arrangements with financial sector entities is that the existing clauses related to cloud providers are considered when assessing compliance.

Any possible development of Standard Contractual Clauses (SCCs) between financial firms and ITC Third Party Providers should be voluntary, principles-based, and seek to harmonise existing mandatory outsourcing requirements that are required by the broadest range of firms. We recognise that there is currently a lack of contractual and technical standardisation between ICT Third Party Providers, which provide similar service offerings. Therefore, this can often make contractual negotiation burdensome with a provider, and complex where a firm wishes to use multiple providers (such as in a hybrid service model).

However, introducing SCCs between firms and ICT Third Party Providers should not create additional regulatory and operational complexity for firms (such as the need for extensive renegotiation of current contracts, changes to existing outsourcing services, or increases in the costs of services). SCCs should also ensure that the level playfield field for ICT Third Party Providers is not restricted (reduced competition in the market), or restrictions are placed on firms to manage their outsourcing arrangements in a risk and principles-based approach.

There has been a significant increase in the regulatory focus on ICT Third Party Outsourcing over the last three years (such as the 2019 EBA Guidelines on Outsourcing) and we also note that there are further regulatory developments expected (such as further guidance from ESMA on outsourcing). These recent regulatory requirements (on contractual aspects such as access and audit rights, transition, sub-outsourcing, resilience, registers, and exit strategies) have been successful in providing clarity between firms and ICT Third Party Providers. We recommend that the Commission continues to support harmonising the EBA Guidelines on Outsourcing across Member States to support both firms and providers in their contracting obligations.

37. **What is your view on the possibility to introduce an oversight framework for ICT third party providers?**

	Yes	No	Don't know /Not applicable
Should an oversight framework be established?	X		
Should it focus on critical ICT third party providers?	X		
Should "criticality" be based on a set of both qualitative and quantitative thresholds (e.g. concentration, number of customers, size, 20			X

interconnectedness, substitutability, complexity, etc.)?			
Should proportionality play a role in the identification of critical ICT third party providers?			X
Should other related aspects (e.g. data portability, exit strategies and related market practices, fair contractual practices, environmental performance, etc.) be included in the oversight framework?			X
Should EU and national competent authorities responsible for the prudential or organisational supervision of financial entities carry out the oversight?			X
Should a collaboration mechanism be established (e.g. within colleges of supervisors where one national competent authority assumes the lead in overseeing a relevant ICT service provider to an entity under its supervision - see e.g. CRD model)?	X		
Should the oversight tools be limited to nonbinding tools (e.g. recommendations, crossborder cooperation via joint inspections and exchanges of information, onsite reviews, etc.)?		X	
Should it also include binding tools (such as sanctions or other enforcement actions)?			X

To the extent you deem it necessary, please explain your reasoning.

Barclays does see benefit in policymakers having greater oversight of major ICT third party providers in the EU, for example cloud providers, however we do not consider provisions to this effect should be included in any future digital operational resilience framework for financial services. Instead the Commission should consider introducing a separate and distinct oversight framework specifically for major ICT third party providers operating in the EU. This would provide regulators with direct oversight and visibility of their operations, and any potential for disruption or failure.

Furthermore, Barclays does not believe the Commission should introduce prescriptive requirements in its new framework governing how firms manage third party risk.

The mitigation of third party risk is an issue faced by multiple jurisdictions. Indeed, Barclays would note there are many existing frameworks that seek to provide oversight of third party providers, for example, the EBA guidelines, ISO 27001, and FedRAMP in the US. EU policymakers should therefore look to ensure any new framework for oversight of major ICT third party providers is aligned with broader international frameworks, or risk the EU have diverging rules from the rest of the world.

38. **What solutions do you consider most appropriate and effective to address concentration risk among ICT third party service providers?**

	Yes	No	Don't know /Not applicable
Diversification strategies, including a potential mandatory or voluntary rotation mechanism with associated rules to ensure portability (e.g. auditing model)		X	
Mandatory multi-provider approach		X	
Should limits be set by the legislator or supervisors to tackle the excessive exposure of a financial institution to one or more ICT third party providers?		X	
Other (please specify)			

To the extent you deem it necessary, please explain your reasoning.

As per our response to Q37, Barclays does not believe the Commission should include in any new framework prescriptive requirements governing how firms manage their third party risk. We would caution the Commission against introducing prescriptive rules mandating firms to operate a multi-provider approach to cloud services, or requiring firms to rotate their service providers. Mandating such solutions could increase complexity for firms looking to manage their third party risk, and reduce their flexibility to adapt their strategies.

Instead, policymakers should explore how they can leverage best practice guidance to encourage appropriate industry management of any concentration risk.

As set out in our response to Q37, a new separate framework providing direct oversight of major ICT third party providers would give regulators direct visibility of their service provision across the sector and enable easier assessment of sector concentration risk.

Section 5 - Other Areas Where EU Action May Be Needed

39. Do you agree that the EU should have a role in supporting and promoting the voluntary exchanges of such information between financial institutions?

- Yes
- No
- Don't know/no opinion

To the extent you deem it necessary, please explain your reasoning.

Barclays believes the EU should play a role in supporting and promoting the voluntary exchange of information between financial institutions. Given the interconnected nature of the financial services sector, cyber threats on one firm can quickly extend to other firms. Greater cooperation, coordination and exchange of threat information between firms can therefore provide firms with advanced notice of an impending threat, and provide crucial time to prepare.

In the UK, information sharing between financial services firms is relatively advanced with various initiatives in place to facilitate secure and trusted voluntary sharing of threat information – see question 40. Other areas of the EU may be less advanced. While we do not believe the Commission should introduce a mandatory framework requiring firms to share threat information, policymakers should explore how the benefits of these existing information sharing initiatives could be achieved more broadly at EU level. The Commission could encourage firms across the EU to participate in these existing data sharing initiatives.

Ultimately, firms would benefit from a high level, cross-sectoral snapshot of live threat information that can be acted on in their own defence and resilience activity. The EU should consider what role they can play to achieve this outcome.

40. **Is your organisation currently part of such information-sharing arrangements?**

- Yes
- No
- Don't know/no opinion

To the extent you deem it necessary, please explain your reasoning. If you have answered yes to the question, please explain how these arrangements are organised and with which financial counterparts you exchange this information. Please specify the type of information exchanged and the frequency of exchange.

Barclays is a member of a number of industry level, threat information-sharing initiatives, including:

- The Cyber Defence Alliance (CDA) – The CDA is a group of British-based banks and law enforcement agencies which seek to combat cyber threats by exchanging expertise, threat information, best practice, statistical data, technical information or trends related to cybercrime.
- The Financial Services Information Exchange (FSIE) – exists to share confidential mutually beneficial information regarding security threats, vulnerabilities, incidents and solutions in the UK financial sector. The FSIE includes UK-based financial organisations including banking, insurance, securities, service providers, exchanges and CPNI.
- The Financial Services Cyber Collaboration Centre (FSCCC) - the FSCCC's mission is to proactively identify, analyse, assess and coordinate activities to mitigate systemic risk and strengthen the resilience of the UK financial sector. It does this through enhanced collaborative activities and focused operations across financial services organisation industry partners and UK and international authorities.
- The Financial Services Information Sharing and Analysis Center (FS-ISAC) is an industry consortium dedicated to reducing cyber-risk in the global financial system. Serving financial institutions around the globe and in turn their customers, the organisation leverages its intelligence platform, resiliency resources and a trusted peer-to-peer network of experts to anticipate, mitigate and respond to cyber threats.

41. **Do you see any particular challenges associated with the sharing of information on cyber threats and incidents with your peer financial institutions?**

- Yes
- No
- Don't know/no opinion

To the extent you deem it necessary, please explain your reasoning. If you answered yes, please explain which are the challenges and why, by giving concrete examples.

While improving the sharing of information between firms at EU level may be a positive opportunity, we also note certain challenges that EU policymakers may want to consider:

- Whilst firms generally do not look to compete in the area of ICT security, there may be a certain reluctance to share threat information with peer firms, especially if doing so could risk their market position.
- Firms may only share information with peers once the threat has been handled, which in certain instances may be too late to be useful for other firms.

42. **Do you consider you need more information sharing across different jurisdictions within the EU?**

- Yes
- No
- Don't know/no opinion

To the extent you deem it necessary, please explain your reasoning and clarify which type of information is needed and why its sharing is beneficial.

As set out in our answer to Q39 – Barclays considers that firms would benefit from a high level, cross-sectoral snapshot of live threat information that can be acted on in their own defence and resilience activity. The EU should consider what role they can play to achieve this outcome.

Promotion of Cyber Insurance and Other Risk Transfer Schemes

43. Does your organisation currently have a form of cyber insurance or risk transfer policy?

- Yes
- No
- Don't know/no opinion

If you answered yes, please specify which form of cyber insurance and whether it comes as a stand-alone cyber risk insurance policy or is offered bundled with other more traditional insurance products.

As part of our comprehensive approach to ICT security, Barclays has a number of insurance policies in place intended to provide additional protection against cyber threats and related aspects.

44. What types of cyber insurance or risk transfer products would your organisation buy or see a need for?

To the extent you deem it necessary, please specify and explain whether they should cover rather first or third-party liability or a combination of both?

Barclays purchases both first-party insurance, which covers potential damages incurred directly to Barclays as a result of a cyber incident, and third-party liability insurance, which covers potential costs related to damages to third parties.

***45.* Where do you see challenges in the development of an EU cyber insurance/risk transfer market, if any?**

Issues	Yes	No	Don't know /Not applicable
Lack of a common taxonomy on cyber incidents	X		
Lack of available data on cyber incidents		X	
Lack of awareness on the importance of cyber/ICT security		X	
Difficulties in estimating pricing or risk exposures		X	
Legal uncertainties around the contractual terms and coverage	X		
Other (please specify)			

To the extent you deem it necessary, please explain your reasoning, by also specifying to the extent possible how such issues or lacks could be addressed.

Barclays do not see any significant challenges regarding lack of available data on cyber incidents, lack of awareness on the importance of cyber security, or difficulties in estimating pricing or risk exposures. Barclays believes that cyber security is now broadly recognised as a significant risk to firms, and there is an increasing volume of information available across the market regarding insurance pricing, exposures and claims.

Barclays recognises the market for cyber insurance is relatively new and is developing organically. However, we do see challenges to its development in the lack of a common taxonomy on cyber incidents, and legal uncertainties around contractual terms and coverage. As there is no harmonised definition as to what constitutes a cyber incident, it can be challenging to arrange appropriate cyber insurance and make claims against the policy when an incident occurs. Similarly, legal uncertainties and lack of transparency regarding cyber insurance of third parties can create challenges. For example, firms may request third parties to provide evidence they have cyber insurance, but it may not be transparent as to what is actually covered by their policy.

***46.* Should the EU provide any kind of support to develop EU or national initiatives to promote developments in this area?** If so, please provide examples.

- Yes
- No
- Don't know/no opinion

To the extent you deem it necessary, please explain your reasoning.

Yes, Barclays considers that EU policymakers should look to support the development of cyber insurance / risk transfer markets in the EU.

While we consider that insurance is an important element in firms' protection against security and ICT threats, we do not believe the Commission should introduce prescriptive rules mandating the extent to which firms should have insurance in place. Policymakers should instead consider how they can encourage firms to incorporate insurance into their security programs through a principles-based framework providing guidance and base-level standards all firms should aim to meet as a minimum. It is important that any framework or guidance encourages firms to best protect themselves, but should retain flexibility for firms to do so in a proportionate manner that is most appropriate for them.

Interaction with the NIS Directive

47. Does your organisation fall under the scope of application of the NIS Directive as transposed in your Member State?

- Yes
- No
- Don't know/no opinion

To the extent you deem it necessary, please explain your situation in this respect. If you answered yes to the question, please specify the requirements you are subject to, indicating the financial sector you are operating in.

Barclays operates in a number of EU Member States, however for the majority of these, Barclays is not in scope of the NIS Directive as an Operator of Essential Services or a Digital Services Provider. Through our Barclaycard business, Barclays is in scope of the regulation transposing the NIS Directive in Germany.

48. **How would you asses the effects of the NIS Directive for your specific financial organisation? How would you assess the impact of the NIS Directive on your financial sector - taking into account the 3 specific financial sectors in its scope (credit institutions, trading venues and central clearing parties), the designation of operators of essential services and the lex specialis clause?**

To the extent you deem it necessary, please explain your reasoning.

In the UK, financial services organisations were exempted by Government from many aspects of the NIS directive as provisions deemed equivalent were already in force by the Bank of England and the Financial Conduct Authority.

49. **Are you covered by more specific requirements as compared to the NIS Directive requirements and if so, do they originate from EU level financial services legislation or do they come from national law?**

To the extent you deem it necessary, please explain your reasoning and provide details.

In the UK, financial services organisations were exempted by Government from many aspects of the NIS directive as provisions deemed equivalent were already in force by the Bank of England and the Financial Conduct Authority.

50. Did you encounter difficulties based on the fact that in the Member State where you are established the NIS competent authority is not the same as your own financial supervisory authority?

Please provide details on your experience.
As mentioned in our response to Q47, Barclays is subject to the NIS directive in Germany, and for the purposes of the Directive, we engage with the German Federal Office for Information Security (BSI). We have not encountered any issues due to the BSI not being our financial supervisor in Germany.

51. How do you cooperate with the NIS competent authority in the Member State where you are established? Do you have agreements for cooperation/MoUs?

Please provide details on your experience.
Barclays does not have any cooperation agreements, or MOUs with the national competent authorities in Member States in which we are subject to the NIS Directive. However, we have relationships in place with clear awareness of points of contact, should there be a need to engage with each other.

Section 6 – Potential Impacts

57. To the extent possible and based on the information provided for in the different building blocks above, which possible impacts and effects (i.e. economic, social, corporate, business development perspective etc.) could you foresee, both in the short and the long term?

Please provide details.
Barclays has not provided an answer to this question.

58. Which of the specific measures set out in the building blocks (as detailed above) would bring most benefit and value for your specific organisation and your financial sector? Do you also have an estimation of benefits and the one-off and/or recurring costs of these specific measures?

Please provide details.

Barclays considers that the proposed harmonization of incident reporting requirements and frameworks across EU legislation would be particularly beneficial to the sector.

59. Which of these specific measures would be completely new for your organisation and potentially require more steps/gradual approach in their implementation?

Please provide details.

Barclays does not believe any of the 'building blocks' set out in the consultation would be completely new. As mentioned in this response, Barclays is a mature organisation with a well-developed risk management framework and approach to ICT security. However, we would reiterate our belief that the Commission should seek to improve digital operational resilience of the sector through a principles-based framework providing guidance and base-level standards all financial services firms should aim to meet as a minimum.

60. Where exactly do you expect your company to put most efforts in order to comply with future enhanced ICT risk management measures and with increased safeguards in the digital environment? For instance, in respect to your current ICT security baseline, do you foresee a focus on investing more in upgrading technologies, introducing a corporate discipline, ensuring compliance with new provisions such as testing requirements, etc.?

Please provide details.

Barclays has not provided an answer to this question.

61. Which administrative formalities or requirements in respect to the ICT risks are today the most burdensome, human-resource intensive or cost-inefficient from an economic perspective? And how would you suggest they should be addressed?

Please provide details.

Barclays has not provided an answer to this question.

62. Do you have an estimation of the costs (immediate and subsequent) that your company incurred because of ICT incidents and in particular cyber-attacks? If yes, to the extent possible, please provide any useful information (in relative or absolute) terms that you may disclose.

Please provide details.

Barclays has not provided an answer to this question.