NCC Group response to the Financial Stability Board's (FSB) Discussion Paper on 'Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships'

A. Introduction

NCC Group is delighted to offers its observations in response to the FSB's Discussion Paper.

We welcome the FSB's support for global dialogue on challenges facing regulatory authorities around the world, particularly on the basis of a shared desire to update frameworks on risk management, business continuity and operational resilience, to allow for best practice approaches to be shared and adopted more widely, enabling global consistency, and, ideally, raising standards everywhere.

We believe strongly in the potential of appropriate regulatory measures to unleash the innovative ingenuity of adjacent services sectors to develop practical solutions that allow organisations to meet regulatory requirements in the most effective way.

With over 30 years' experience in software escrow, protecting business critical software, data and information through escrow, secure verification testing and cloud hosted software continuity services, NCC Group has followed regulatory developments regarding outsourcing and third party arrangements closely, not least to ensure that we, too, are able to meet our customers' evolving demands as regulatory requirements change. Our current customers include over half of the FTSE 100's Financial Services firms, digital banking start-ups, community banks, crypto, insurance and payment providers.

B. Call for Action

In simple terms, we advocate for a greater regulatory-driven focus on the adoption of software and technology escrow solutions as the baseline implementation of Resilience by Design, to meet the global financial system's increased demand for risk management, business continuity and operational resilience:

- While headquartered in the UK, and thus closely engaged with the Bank of England and Prudential Regulation Authority's work on third party risk management (notably CP30/19), NCC Group is a global organisation with local presence in the Middle East and Asia Pacific, allowing us to review and assess international regulators' approaches to business continuity management.
- Our own research of global regulatory regimes has shown regulators' shared emphasis of the importance of protecting continuity of services, and testing this continuity accordingly, irrespective of whether services are on-premise or cloud-hosted applications.
- However, we also found that regulators' willingness to detail solutions to meet their business continuity requirements varies. The Hong Kong Monetary Authority (HKMA) is one of the few regulatory authorities that does so, stating in its Outsourcing Manual for Authorised Institutions (AIs) that, "for mission-critical software packages, AIs may consider including in the contracts an escrow agreement, which allows them to obtain access to the source code of software packages under certain circumstances, such as when the software vendors cease their business".

- We do believe that software and technology escrow solutions offer legal, technical and proportional assurance to financial institutions. Many financial institutions do use escrow solutions as part of their comprehensive business continuity planning when mitigating supplier risk, and some third party service providers themselves have opted to build these solutions into their offer to support their customers' compliance with regulatory requirements. By way of example, NCC Group has worked with banking technology provider Mambu on developing a cloud escrow solution. Built within Amazon Web Services (AWS) infrastructure, Mambu's cloudhosted digital banking software-as-a-service (SaaS) solutions supports more than 6000 loan and deposit products serving over 14 million end customers worldwide. Working with NCC Group, Mambu adopted a cloud escrow solution to establish a robust approach to its customers' regulatory compliance, offering business continuity assurance by ensuring that financial institutions deploying Mambu's solution would have access to their application and specific cloud environment as well as support for the ongoing maintenance and management of their application.
- However, we do not believe that there is sufficiently widespread awareness of the benefits of software and technology escrow solutions at present, and the role they can play in addressing regulatory requirements on outsourcing and third party risk management all around the world.
- To address this lack of awareness, we believe that there is a role for the Financial Stability Board to promote and educate regulatory authorities and financial institutions globally on the benefits of software and technology escrow solutions as a practical means, and a baseline Resilience by Design solution, to meet regulatory outsourcing and risk management requirements, be that through explicitly encouraging the mandating of escrow solutions, or by encouraging much greater inclusion of it in implementation guidance.

C. Response to consultation questions

Beyond our main call for action, we have outlined below our response to the FSB's specific questions:

1. **What do you consider the key challenges in identifying, managing and mitigating the risks relating to outsourcing and third-party relationships, including risks in sub-contractors and the broader supply chain?**

We principally agree with the FSB's conclusions regarding shared challenges across regulatory authorities including: rights to access in contractual agreements; full supply chain visibility; effectiveness of business continuity and exit plans to recover from outage and failure; and systemic risk.

We would add the following considerations:

- The feasibility of exhaustively identifying supplier risk is questionable. A supplier's overall risk profile is generally the result of a combination of a multitude of factors. Identifying all possible scenarios is likely disproportionate to its potential benefits, and risks increasing costs, creating barriers to innovation, and subsequently reducing access to financial services.
- Many software products are a combination of other products that are often not detailed in license agreements making it, at best, very difficult for end users to have a complete view of what their service actually entails. This is complicated further where suppliers deploy their services via the

cloud. In on-premise deployments, end users at least have a view of the architecture of the deployment, but they often lack that visibility in cloud deployments.

- Risk assessment needs to consider recovery time. Principally, financial institutions rely on failed services continuing to operate while full recovery plans are being implemented; that means that continuity and exit planning needs to take account of implementation, testing and training times that impact on the ability to exchange or replace products and services expediently, safely and compliantly.

2. **What are possible ways to address these challenges and mitigate related risks? Are there any concerns with potential approaches that might increase risks, complexity or costs?**

First and foremost, and as outlined above, we propose that the FSB consider the concept of Resilience by Design.

This would assume supplier failure by default, regardless of their risk profile, and encourage or mandate using software and technology escrow agreements as a proportionate and cost-effective solution for financial institutions to mitigate against supplier failure, by offering a minimum level of resilience through the legal and technical means to ensure continuity of incumbent services while alternative options are being implemented. In this sense, escrow agreements act as a technical insurance policy, safeguarding the long-term availability of business-critical technologies and applications while protecting intellectual property.

Establishing software and technology escrow agreements will create a baseline to:

- Grant financial institutions access to the source code, and right to access the cloud environment where it is hosted, where: an application is material to the institution's operational continuity, if the service is deployed in the cloud; or if the application presents a concentration risk. The details of any access rights and conditions will be set out in individual escrow agreements, offering a legal basis with full transparency for all involved parties over when any such rights can be invoked.
- Specify how the agreement and access rights are to be used in the event of supplier failure, including in the event of: bankruptcy / liquidation; failure to maintain / inability to fix the service; transfer of ownership of intellectual property rights to the software, or the supplier company as a whole, unless the new owners agree to keep in place the agreement.

While costs will vary depending on the detail of the escrow agreement in question, they range between £1,000 and £20,000: we do believe that this is a more proportionate investment in relation to the protection and resilience it delivers than a detailed risk assessment and mitigation exercise.

Above and beyond that baseline, additional Resilience by Design elements could include:

- Ensuring the development and regular testing requirements of business continuity and exit plans forms part of licensing or contractual agreements between financial institutions and their third party suppliers;
- Broadening exit and stressed exit plan requirements so that:
    - Cloud providers should advise their software vendors initiate stressed exit plans where the latter provide services to financial institutions.
    - Software contained within other solutions, as well as the internal infrastructure of third parties supplying software and technology solutions, should also be subject to stressed exit plans.

- Mandating interchangeability of services between cloud providers, and regular testing of the interchangeability.

3. **What are possible ways in which financial institutions, third-party service providers and supervisory authorities could collaborate to address these challenges on a cross-border basis?**

We believe that the greatest benefit of international collaboration will be in understanding concentration and systemic risk. That means sharing information across the ecosystem stakeholders on:

- Anonymous outsourcing arrangement audits to gain early insights and intelligence on emerging dependencies and criticalities;
- Firms' assessments of non-material outsourcing arrangements from the outset so as to be able to track trends over time, for example, where non-material services are supplied by a single provider to a large number of financial institutions;
- Failed stressed exit plans, particularly where these plans relate to larger suppliers.

4. **What lessons have been learned from the COVID-19 pandemic regarding managing and mitigating risks relating to outsourcing and third-party relationships, including risks arising in sub-contractors and the broader supply chain?**

On the basis of NCC Group's experience since the beginning of the pandemic in early 2020, we are able particularly to speak to two trends that were broadly expected in relation to third party outsourcing over the last ten to twelve months:

- An increased number of third party suppliers going out of business;
- An increased efforts by organisations to protect themselves against the, perceived, higher risk of third party supplier failure.

Our data to date does not support these binary outcomes. While we have seen disruption of procurement, testing and deployment of software projects across the board, our comparison of year-on-year data does not show a material increase in the number of software escrow release events (usually as the result of a third party supplier's insolvency).

The data does show the following trends, however:

- NCC Group has experienced a considerable increase in the number of organisations reviewing their existing escrow contracts and agreements. This doesn't necessarily result in changes to the contracts, however organisations reviewing to ensure their contracts cover them for any heightened risks brought upon them by the pandemic, once more indicating the dynamic nature of risk assessment.
- We have also seen an increase in software escrow consultancy/verification services, as an integral part of any software resilience engagement to ensure the completeness and viability of an escrow deposit for use in a supply chain failure/disruption scenario, indicating a greater sense of the potential reality of such an event.