# Proposed Interagency Guidance on Third-Party Relationships: Risk Management

# NCC Group Response to Request for Comment

## Introduction

NCC Group is delighted to offer its observations in response to the Request for Comments made by the Federal Reserve System, the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency (together, the agencies).

We commend the agencies' intent to promote consistency, and articulate risk-based principles to assist regulated banking organisations to identify, assess and manage third party risks in a way that is commensurate with the level and complexity of risk involved. We wholeheartedly agree that banking organisations' expanded use of third parties for core banking services, improved functionality of services, and platforms to provide services often adds complexity, and requires sound risk management.

We note that the agencies' work follows that of their fellow regulatory authorities internationally: authorities in Europe, the UK, Ireland and Canada alongside the Financial Stability Board have all recently considered improvements in their guidance and supervisory statement as regards financial institutions' third-party risk management in light of an ever-growing reliance on third party technologies in an ever more digital economy.

We have focused our contribution on high level general comments that, we believe, offer additional consideration and expanded scope to the agencies' proposed guidance to future-proof it further, and provide banking organizations with additional resources practically to implement the required sound risk management of third-party technologies and services.

## About NCC Group

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 global banks and other financial services firms, digital banking start-ups, community banks, crypto, insurance and payment providers. We hold a unique position where we see compliance from the end-user's perspective as well as from the viewpoint of the IT provider, and try to assist both in achieving their aims.

NCC Group is a global cyber-security business headquartered in the UK, but, through its recent $220m acquisition of Iron Mountain's Intellectual Property Management division (IPM), has an established and significant footprint in North America, alongside our existing presence in the Middle East and Asia Pacific. This means we are able to take an international perspective to regulatory approaches to third party risk management. The IPM business has been operating in the North America regulatory market for over 30 years and has a strong track record of working within the financial services sector including on the banking infrastructure in the US. 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.

Throughout the pandemic, NCC Group has experienced a considerable increase in the number of organizations reviewing their existing escrow contracts and agreements. This doesn't necessarily result in changes to the contracts, but organisations are ensuring that their contracts cover them for any heightened risks brought upon by the pandemic, once more indicating the ever-changing 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. Rather than what might have previously been seen as maybe a 'box-ticking' exercise (of merely putting a software escrow contract in place), many financial services institutions have intertwined the IT element of their supply chain with their business continuity/disaster recovery planning and ensured that detailed verification 'dry-runs' are carried out within the release cycle of business critical software applications.

## General comments on the proposed Interagency Guidance

NCC Group is passionate in its advocacy for a greater regulatory-driven focus on the adoption of cloud, software and technology escrow solutions as the baseline implementation of Resilience by Design, to meet the financial system's increased demand for risk management, business continuity and operational resilience.

In that context, we acknowledge and welcome that the agencies' existing guidance clearly encourages banking organizations to establish escrow agreements where they purchase software, to provide access to source code and programs under certain conditions.

However, we believe that banking organizations very rarely "purchase" software any more in the traditional sense.

It is well understood that 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 or what the key components are. 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.

Further, most major financial institutions have established their own FinTech investment arm(s) and/or incubator(s), meaning financial software is increasingly being sold or licensed from one financial institution to another.

In line with understanding cloud service provision to constitute business arrangements, we believe that the agencies' guidance should be expanded to instances where banking organizations "develop, purchase, invest in, license and subscribe to" software so as even more explicitly bring cloud service provision into scope and thus future-proof the harmonised guidance from the outset.

In addition, we argue that there are additional elements of third-party risk management that warrant explicit recognition of the benefit and value of cloud, software and technology escrow agreements, for example in relation to:

- The continuation of business functions where problems affect third party operations, such as provisions for transferring data to other third parties;

- Potential issues regarding end-of-life issues with software programming language, computer platforms or data storage technologies that may impact operational resilience; and
- The means to transition services in a timely manner, including handling of intellectual property.

## Additional comments for consideration

NCC Group emphasizes the following aspects and would ask the agencies to consider these in finalizing their Interagency Guidance:

- 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.
- For that reason, no less, we do believe that cloud, software and technology escrow solutions offer legal, technical and proportional assurance to banking organizations, particularly where they embrace the concept of what we are calling 'Resilience by Design'.
- This would assume supplier failure by default, regardless of their risk profile, and encourage or mandate using cloud, software and technology escrow agreements together with the 'dry-run' verification services, as a proportionate and cost-effective solution for banking organizations 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 and verification services act as a technical insurance policy and business continuity strategy, safeguarding the long-term availability of business-critical technologies and applications while protecting intellectual property.
- Establishing cloud, software and technology escrow agreements with supporting verification services will create a baseline to:
    - Grant banking organizations access to the source code (as very much recognized by agencies' existing guidance), but, crucially, also the 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 / insolvency; 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. 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.
- Many financial institutions already 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 cloud hosted 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 believe that there is still insufficiently widespread awareness of the benefits of software and technology escrow solutions, and the role they can play in addressing regulatory requirements on outsourcing and third-party risk management.
- To address this lack of awareness, we believe that there is a role for the agencies to do more to promote and educate other regulatory authorities and financial institutions on the benefits of cloud, 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.
- 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, particularly through the release lifecycle of critical applications
  - 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.
    - We believe that the European Commission's proposed Data Act offers an interesting proposal in this regard. The Act includes proposals to mandate cloud computing portability obligation, with the intent to make it possible for organizations to switch between cloud computing service providers, or port data back to on-premises IT systems without contractual, technical or economic barriers, offering clarity on what the technical requirements and timeframes are for 'cloud switching', as preconditions for portability of infrastructure, platform and software cloud services.

        - We believe that cloud escrow solutions, much like those offered by NCC Group, would act as a practical supplier failure & cloud portability solution, enabling contractual and technical portability.

- In addition, we advocate for greater information sharing to improve shared and contextualised understanding of concentration and system risk through elements including:
    - 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; and
    - Failed stressed exit plans, particularly where these plans relate to larger suppliers.

## Conclusion

NCC Group very much welcomes the opportunity to contribute to the Interagency Guidance. We have positively contributed to other regulatory authorities' consideration of third-party risk management and would welcome the opportunity to engage in more proactive dialogue with the agencies to support its objectives to promote a safe, digitally robust and resilience banking system now and in the future. NCC Group is able to offer interactive dialogue with its IT technical experts, solutions architects and qualified legal advisers each of which have years of experience in navigating the mitigation of these risks for clients.