Core Principles for effective banking supervision

NCC Group's response to the Basel Committee's consultative document, October 2023

About NCC Group

As a global cybersecurity and software resilience business, NCC Group is pleased to offer its observations in response to the Basel Committee's consultation.

NCC Group has over 30 years' experience protecting business critical software, data and information through escrow, secure verification testing and cloud hosted software continuity services. We have followed regulatory developments regarding supply chain risks and third-party arrangements closely, not least to ensure that we are able to meet our customers' evolving demands as regulatory requirements change. We work with customers operating across financial services who understand how cybersecurity and software resilience can add value and represent a competitive advantage both in their own business, as well as across their portfolios. Headquartered in the UK, NCC Group has an established and significant footprint in North America and Europe, with a growing presence in Asia Pacific. This means we are able to take an international perspective to regulatory approaches to cybersecurity and third-party risk management.

Our response focuses on those principles where our expertise and experience enable us to provide informed commentary and feedback, namely Principles 19 (Concentration risk and large exposure limits) and 25 (Operational risk and operational resilience).

Response

As the Committee rightly highlights, against a backdrop of increasing reliance on third-party providers, it is essential that sound risk management and improved business continuity is embedded in financial systems' supply chains. Risks such as supplier failure, service deterioration and concentration risk need to be understood and managed. With financial authorities globally developing and implementing new frameworks and rules to ensure that these risks are mitigated against, we welcome the Committee's efforts to update its Core Principles.

We broadly support the Committee's proposed updates to Principles 19 and 25, which we hope will promote consistency across borders and ensures the full lifecycle of third-party relationships is considered. That said, there are a number of technical changes that would enhance the Committee's principles, ensuring that the full range of risks and (proven) mitigations associated with third-party risk management are reflected:

Principle 19 - Concentration risk and large exposure limits:

- We are pleased to see the focus on addressing concentration risk, but note that this principle, at present, only refers to risks associated financial transactions. As noted under Principle 25 (section 40.58), operational risks associated with third party suppliers can also present common points of exposure and vulnerability across banks. Governments globally are looking to tackle these risks head on through new laws and regulations such as the EU's Digital Operational Resilience Act and the UK's Financial Services and Markets Act. We therefore recommend that

Principle 19 is updated to reflect concentration risk presented by systemically important suppliers, linking to section 40.58 under principle 25.

Principle 25 – Operational risk and operational resilience:

- 40.57(5) should be amended to include not only "disruption" at a service provider, but also "supplier failure".
- 40.57(8) should be expanded to ensure that reporting mechanisms include provisions on reporting supplier failure, the ramifications of that failure and the overall cost of settlement.
- 40.57 (9)f should be expanded to:
    - Require the development of "stressed" exit strategies. A stressed exit is when the contract is ended due to the failure or insolvency of the service provider, and therefore is more unexpected than a non-stressed exit, which could be due to commercial, performance or strategic reasons. Stressed exit strategies form an important part of business continuity plans, ensuring a bank's continued provision of important business services and limiting the impact of disruption on the entity, it's customers and the wider financial market as a whole. Financial regulators globally, such as the UK's PRA, require financial institutions to develop such plan.
    - Reflect the passing of the management of a failed service to a third party, in addition to bringing the activity back in-house, as a viable option within a business continuity plan.

Conclusion

NCC Group welcomes the opportunity to contribute to the Committee's consultation. We have positively contributed to other regulatory authorities' consideration of cyber security, operational resilience and third-party risk management. We would welcome the opportunity to engage in more proactive dialogue with the Committee to support its objectives. We are able to offer interactive consultations with our IT technical experts, solutions architects and qualified legal advisers, each of whom have years of experience navigating the mitigation of risks for clients.