Securities and Exchange Commission's (SEC) proposed amendments to Regulation Systems Compliance and Integrity (SCI)

NCC Group's response, June 2023

Introduction

NCC Group is pleased to offer its observations in response to the Securities and Exchange Commission's (SEC) proposed amendments.

Against a backdrop of increasing reliance on third-party suppliers, we support SEC's objectives to ensure the capacity, integrity, resiliency, availability, and security of the technology infrastructure of the U.S. securities markets (SCI entities). To this end, we believe that in finalizing the Regulation the SEC should:

- promote **continuous independent assessment of cyber risk**;
- publish clear guidance on **risk tolerance and acceptance**; and,
- provide SCI entities with **appropriate guidance on the practical steps** they can take to implement the required sound risk management of third-party technologies and services, including cloud, software and technology escrow agreements.

The need for continuous assessment of cyber risk

The current approach to assessing third party cyber risk is largely based on self-assessment and is point in time in nature. This approach is limited in providing SCI entities and regulators with an accurate and current picture of cyber risk. The rate of change with respect to both the threat landscape and technology necessitates a real time approach to the problem. It is therefore **vital that the state of practice in this area advances to continuous assessment of cyber risk that includes an objective verification of both risk and the effectiveness of mitigating controls**.

The need for clear guidance on risk tolerance and acceptance

Given that it is not possible to reduce risk to zero, **SCI entities must be provided with clear guidance to inform their processes regarding risk tolerance and acceptance**. This should be based on a common scoring method for cyber risk including how controls which reduce inherent cyber risk are valued and measured. There are currently a wide range of approaches to this issue which leads to uncertainty. Clarity on the subject would be welcome among both the SCI entities and regulators.

Role of cloud, software and technology escrow agreements

The revised Rule 1001(a) requires SCI entities to assess third-party providers' risks and controls. However, we would emphasize the difficulties in exhaustively identifying a suppliers' risk profile, given it is generally the result of a combination of a multitude of factors. The traditional approach of identifying all possible scenarios is likely disproportionate to its potential benefits. This in turn may

prove to be counter-productive as it would likely lead to increasing costs and create barriers to innovation.

Cloud, software, and technology escrow solutions can offer legal, technical and proportional assurance to firms in dealing with their third-party suppliers, particularly where they embrace the concept of '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 as a proportionate and cost-effective solution for regulated entities to mitigate against this**. Indeed, 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 organizations access to the source code and the right to access the cloud environment in which it is hosted, where an application is material to the organization's operational continuity, if the service is deployed in the cloud, or if the application presents a concentration risk. Indeed, the role of escrow agreements is reflected in CISA's guidance on ransomware[1] which states that, in being prepared for a ransomware incident, organizations should ensure the availability of source code through backups or escrow agreements. The details of any access rights and conditions will be set out in individual 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 compromise or failure. This goes beyond cyber risk, taking a broader view which includes non-technical risks such as bankruptcy, failure to maintain or inability to fix the service, and transfer of ownership of intellectual property rights to the software. Principally, critical infrastructure relies 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.

- Advance capabilities to automate risk tolerance at the application programable interface (API) gateways to permit control to gracefully failsafe services or providers who may go out of compliance, removing exposure latency in a real-time digital economy.

Many organizations – particularly those in the financial services sector – 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 a banking technology provider on developing a cloud escrow solution. The provider's cloud hosted digital banking software-as-a-service (SaaS) solutions support more than 6,000 loan and deposit products serving over 14 million end customers worldwide. Working with NCC Group, the provider 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 the provider'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.

[1] Ransomware Guide | CISA

However, we believe that there is still insufficiently widespread awareness of the benefits of cloud, 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 SEC – working with other agencies and global counterparts – to do more to promote and educate organizations on the benefits of cloud, software, and technology escrow solutions** as a practical means to meet outsourcing and risk management requirements. This could be through explicitly encouraging the mandating of escrow solutions or by encouraging much greater inclusion of it in implementation guidance. This would align with approaches taken by other regulators, particularly those in the financial services sector[2], as well as CISA's aforementioned guidance on ransomware.

Additional 'Resilience by Design' measures could include:

- Ensuring SCI entities consider **cloud portability**[3], as we have seen other regulators globally recommend such as the Canadian Office of the Superintendent of Financial Institutions[4]; and,
- Explicitly requiring SCI entities to review risks and criticality associated **with intragroup outsourcing arrangements**, as required by other global regulators[5].

Answers to questions

61. Do commenters believe it is appropriate to require, as in proposed Rule 1001(a)(2)(ix), that each SCI entity have a program to manage and oversee third-party providers that provide functionality, support or service, directly or indirectly, for its SCI systems and, for purposes of security standards, indirect SCI systems?

Yes. The evolving risks associated with increasing reliance on third party providers – including supplier failure, service deterioration, and concentration risk - require sound risk management and improved business continuity.

b) Do commenters believe that such a program should require an initial and periodic review of contracts with such providers for consistency with the SCI entity's obligations under Regulation SCI?

Yes, with the additional recommendation of continuous testing to provide ongoing assurance regarding the performance of the third party providers as required by those contracts.

---

[2] This includes:
• The UK Prudential Regulation Authority: https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss221-march-21.pdf
• The Hong Kong Monetary Authority: https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-G-1.pdf
• The Reserve Bank of New Zealand: https://www.rbnz.govt.nz/-/media/project/sites/rbnz/files/regulation-and-supervision/banks/policy/2017-09-19---final-bs11-redraft_2.pdf
• The Indonesian Financial Services Authority: https://www.ojk.go.id/id/kanal/perbankan/regulasi/surat-edaran-ojk/Documents/SAL%20SEOJK%2021%20-%20MRTI.pdf
• The State Bank of Pakistan: https://www.sbp.org.pk/bprd/2019/C6-Annex-II.pdf
• The Securities and Exchange Board of India: https://www.sebi.gov.in/sebi_data/commondocs/jul-2021/Chapter%202%20-%20Trading%20Software%20and%20Technology_p.pdf
• The Monetary Authority of Singapore: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf

[3] As defined in NIST-SP 500-291: https://www.nist.gov/publications/nist-sp-500-291-nist-cloud-computing-standards-roadmap

[4] https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b10_dft_2022.aspx

[5] Including: https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b10_dft_2022.aspx; https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/digital-finance-council-adopts-digital-operational-resilience-act/; https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/outsourcing-and-third-party-risk-management-ss .

62. Do commenters believe that it is appropriate to require each SCI entity to include a risk-based assessment of each third-party provider's criticality to the SCI entity, including analyses of third-party provider concentration, of key dependencies if the third-party provider's functionality, support, or service were to become unavailable or materially impaired, and of any potential security, including cybersecurity, risks posed? Why or why not?

Yes. More critical systems/services will require a more stringent approach to third-party risk management, as proposed by SEC. As noted above, this should be based on a common scoring method for cyber risk including how controls which reduce inherent cyber risk are valued and measured. There are currently a wide range of approaches to this problem which leads to uncertainty. Clarity on the subject would be welcome among both the entities and regulators.

64. Are there other aspects of third-party provider management that commenters believe should be included in the proposed rule provision? If so, please describe

As outlined in detail above, we believe that SEC should:

- recommend practical resilience solutions such as software, technology, and cloud escrow agreements;
- promote the continuous objective assessment of cyber risk; and,
- provide SCI entities with clear guidance to inform their processes regarding risk tolerance and acceptance.

65. Do commenters agree with the proposed revisions to Rule 1001(a)(2)(v) to require the BC/DR plans of SCI entities to be reasonably designed to address the unavailability of any third-party provider that provides functionality, support, or service to the SCI entity without which there would be a material impact on any of its critical SCI systems?

Yes. In doing so, SCI entities should assume supplier failure by default – adopting a Resilience by Design approach that includes:

- prevention of supply chain failure (through cyber resilience solutions); and,
- mitigation of the risk and impact of supply chain failure (through technology and software escrow agreements).

Conclusion

NCC Group welcomes the opportunity to contribute to SEC's draft amendments. We have positively contributed to other regulatory authorities' consideration of cybersecurity, operational resilience and third-party risk management. We would welcome the opportunity to engage in more proactive dialogue with SEC to support its objectives. 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 risks for clients.

About NCC Group

With **over 30 years' experience protecting business critical software, data and information through escrow, secure verification testing, and cloud hosted software continuity services,** as well as significant experience securing digital transformation programs, increasing resilience and reducing

risk. NCC Group has followed regulatory developments regarding supply chain risks and third-party arrangements closely, not least to ensure that we, too, are able to meet our customers' evolving demands as regulatory requirements change. We work with customers operating across critical infrastructure sectors 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. 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 cybersecurity business headquartered in the UK. Through its $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 Europe, the Middle East and Asia Pacific**. This means we are able to take an international perspective to regulatory approaches to cybersecurity and third-party risk management. The IPM business has been operating in the North America regulatory market for over 30 years. 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 organizations to meet regulatory requirements in the most effective way.