Cloud Computing in the Securities Industry

NCC Group’s Response to FINRA’s Request for Comment

Introduction

NCC Group is delighted to offer its observations in response to the Request for Comments made by the Financial Industry Regulatory Authority (FINRA).

We welcome FINRA’s aim to maintain an ongoing dialogue on the rapidly evolving use of cloud computing in the securities industry, the risks and opportunities this presents, and where guidance or modifications to rules may be desired to support cloud adoption. FINRA’s assessment of the key challenges facing firms in their cloud adoption journey – not least the cybersecurity and ‘lock-in’ risks associated with outsourcing cloud services to third-party vendors – aligns with our own experience, and we wholeheartedly agree with the need for sound risk management.

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

About NCC Group

With over 30 years’ experience protecting business critical software, data and information through escrow, secure verification testing, cloud hosted software continuity services, and designated third party (D3P) compliance services, as well as significant experience securing digital transformation programs, increasing resilience and reducing risk, NCC Group has followed regulatory developments regarding the use of cloud computing 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 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, 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 cloud and 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. 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.

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 organizations 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.

Comments for consideration

Cybersecurity

- FINRA describes the Cloud Security Shared Responsibility Model which is critical to understanding the responsibilities of both the service provider and the firm. Whilst the standard disciplines for assessing, managing and mitigating risk related to services provided using cloud resources are the same as for traditional IT deployment models, the risks are not, and each organization should prioritize understanding their new unique risk profile. In fact, it should be noted that in many cases the cloud service providers operating at scale provide superior risk mitigation capabilities compared to those at many firms.

- Firms should perform a comprehensive assessment of threats, vulnerabilities, impact and likelihood of occurrence on at least an annual basis to maintain a current view of overall technology risk including the cloud. The risk appetite and acceptance criteria of the firm will then dictate the implementation and ongoing maintenance of appropriate controls to mitigate risk to an acceptable level. In fact, there is little excuse not to leverage real-time risk mitigation capabilities available natively on the main cloud platforms.

Outsourcing/vendor management

- The risk profile and the ability of the cloud service provider to effectively assess, manage and mitigate risk is critical. The ability of a cloud service provider to demonstrate their ability to effectively mitigate risk is also key. The Federal Risk and Authorization Management Program (FedRAMP) began in 2011 to provide a common standard that allows providers of cloud services used by the US Government to demonstrate the effectiveness of their controls. The adoption of a similar scheme by FINRA would provide a similar common standard for reporting on the efficacy of controls by cloud service providers.

Resilience by Design

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

- The feasibility of exhaustively identifying cloud 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 broker-dealers, particularly where they embrace the concept of 'Resilience by Design'.

- This would assume cloud 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 broker-dealers 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 broker-dealers access to the source code, but, crucially, also the right to access the cloud environment where 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. 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.

    - Advance capabilities to automate risk tolerance at the application programable interface (API) gateways level 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 financial organizations 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 FINRA – and other financial services 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 broker-dealers and their thirdparty 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 and cloud portability solution, enabling contractual and technical portability.

    - Mandating the use single-tenanted cloud solutions, given the concentration risks associated with multi-tenanted cloud solutions.

- In addition, FINRA should consider updating its guidance to explicitly identify cloud services as a concentration risk, given that it meets all the main criteria of technology concentration risk[1].

[1] 1. Entity level concentration risk; 2. Activity level concentration risk; 3. Systemic concentration risk; 4. Geographical concentration risk

Further, we advocate greater information sharing to improve shared and contextualized understanding of concentration and systemic 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.

Record retention

- The growing complexity of cloud environments and the need for FINRA and the Securities and Exchange Commission (SEC) to access records stored in such environments under Exchange Act Rule 17a-4 point to the ongoing value of D3Ps in helping bring assurance that such records can be accessed if needed by a regulator. D3Ps are uniquely positioned to help address requests for records in the scenarios contemplated by the rule. Nonetheless, the rule has not anticipated developments in technology such as cloud-based storage and applications. Accordingly, additional regulatory guidance regarding the requirements and the rule would help assure a high level of compliance.

  - For instance, the Letter of Undertaking under the rule provides that the D3P will take "reasonable steps" to provide access to records under the rule. Over the years interpretations of what constitutes "reasonable steps" have varied across a broad spectrum. On one end, some have held that reasonable steps include an arrangement whereby upon request for access by a regulator, the broker dealer provides the D3P access to the environment and then the D3P will access requested records using previously compiled (and verified) information required for navigating the environment. At the other end of the spectrum, the D3P is provided ongoing administrator or other high-level access to cloud environment. Such broad ranging access to a broker dealer's cloud environment understandably introduces concerns regarding security which must be considered in terms of what are "reasonable steps" for access under the rule. On the other hand, obtaining access at the time of a request from the regulator introduces an element of cooperation between the D3P and the broker dealer. However, a certain level of ongoing cooperation between the D3P and broker dealer is inescapable under the rule.

  - Maintaining credentials for access to the broker dealer's cloud environment also introduces additional requirements on the D3P to ensure that the credentials remain active. Storage and handling of such credentials, including custom hardware, implicates security concerns as well. Such material should be stored in industry standard electronic or physical vaults with sufficient measures to ensure appropriate handling of such material.

  - In addition, cloud environments introduce nuances such as cold storage and production environments and real-time service level evolution and change. Testing and accessing records in such environments require different procedures and processes. In addition, timeframes for accessing cold storage can be significantly different.

- Lastly, the escrow requirements for Transfer Agents (17 CFR 240.17 Ad-7 (f)(5)(ii)) should be updated to reflect cloud-based environments.
    - While escrow is an important mechanism to help ensure meaningful access of the records under the rule, the current wording of the regulation assumes an on-premises application based on its requirement that the source code be stored in escrow (in addition to other helpful items). In many cases this source code will not be provided by a cloud provider and, even if in escrow, it would likely not be useful due to the complexities of compiling the code and attempting to create a cloud environment.

Conclusion

NCC Group very much welcomes the opportunity to contribute to the Request for Comment. We have positively contributed to other regulatory authorities' consideration of third-party cloud risk management – including the Federal Reserve System, the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency ongoing review of their interagency guidance on third-party relationships – and would welcome the opportunity to engage in more proactive dialogue with FINRA to support its objectives to assess the risks and benefits associated with the increasing use of cloud computing in the securities industry and consider the role of guidance in mitigating these risks and maximizing the benefits. 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.