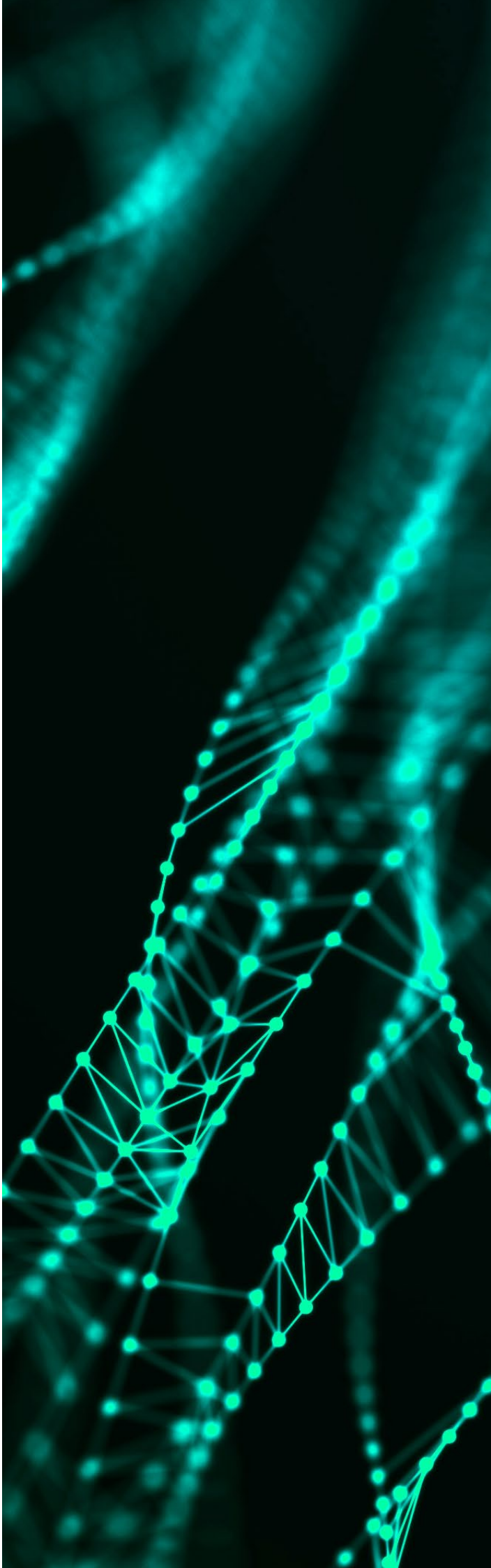
Building resilience in a changing regulatory landscape

A guide for financial organizations in the US

In the midst of rapid digital transformation, operational resilience is more important than ever. An increasing reliance on third parties and outsourced IT solutions, combined with the risk posed by cyber threats and other sources of business interruption, has led to new approaches from regulatory bodies across the US and overseas.

In recent years, a range of agencies in the US have released guidance on managing the risks associated with third-party relationships. While different organizations govern different business areas, many of the key principles overlap - and all are aimed at helping banking and financial services organizations to identify, assess and manage third-party IT risks.



Federal Reserve: guidance on managing outsourcing risk

About the Federal Reserve

The Federal Reserve System is the central bank of the United States, and aims to promote the effective operation of the US economy in the interest of the public.

What is it?

Guidance on managing outsourcing risk for all financial institutions supervised by the Federal Reserve, including those with $10 billion or less in consolidated assets.

Key guidance

- The outsourcer should be responsible for addressing the characteristics, governance and operational effectiveness of risk management programmes for outsourced activities.
- Exit strategies should be in place for all contracts that will minimize impact to business operations and services.
- Financial institutions should have robust arrangements in place for shared or outsourced services needed to maintain critical operations, and should develop strategies and contingency plans for the continuity or replacement of these services.

https://www.federalreserve.gov/supervisionreg/srletters/sr1319.htm

Federal Deposit Insurance Contribution (FDIC): guidance for managing third-party risk

About the FDIC

The Federal Deposit Insurance Corporation (FDIC) is an independent agency created to maintain stability and public confidence in the nation's financial system by addressing risk.

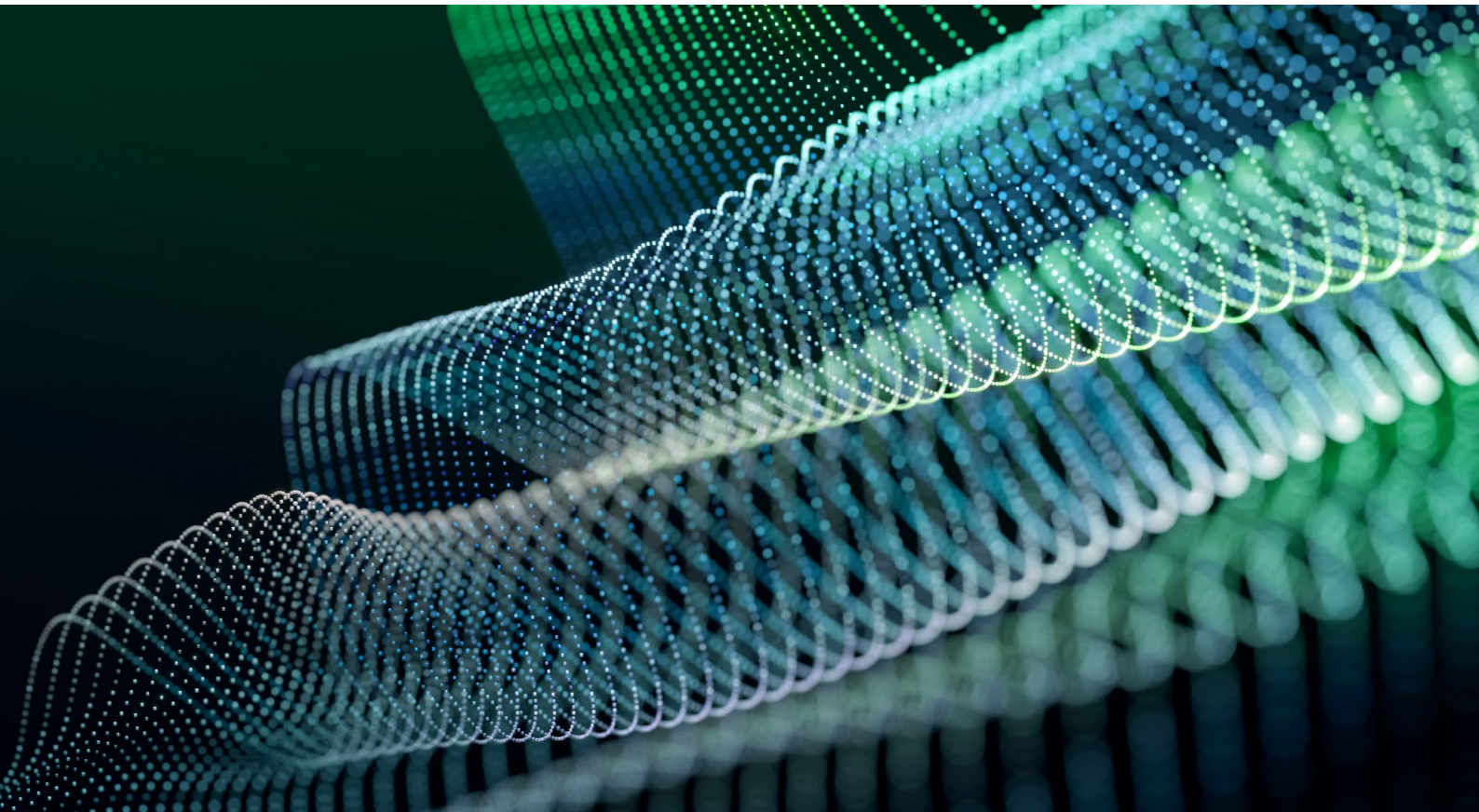
What is it?

A general framework that financial institutions should use for oversight and risk management of significant third-party relationships.

Key guidance

- Business resumption and contingency plans should be in place for all outsourcing agreements.
- Any third-party contracts should have appropriate measures for backing up information and maintaining disaster recovery and contingency plans.
- Contracts with third-party relationships should also state termination and notification requirements, with operating requirements and time frames to allow for the orderly conversion to another entity.

https://www.fdic.gov/news/financial-institution-letters/2008/fil08044.html



The Office for the Comptroller of the Currency (OCC): third-party relationships - risk management guidance

About the OCC

As an independent bureau of the US Department of the Treasury, the OCC charters, regulates and supervises all national banks and federal savings associations, as well as federal branches and agencies of foreign banks.

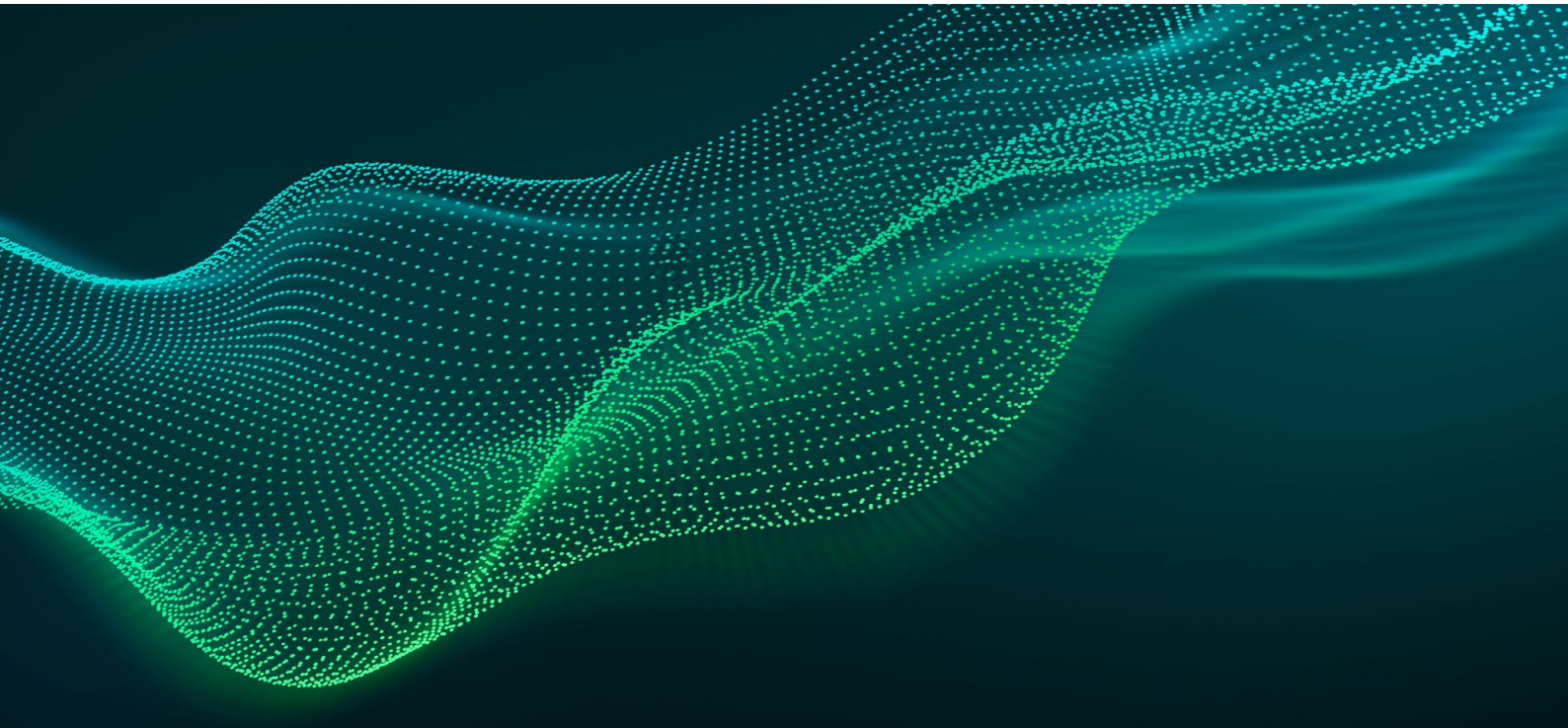
What is it?

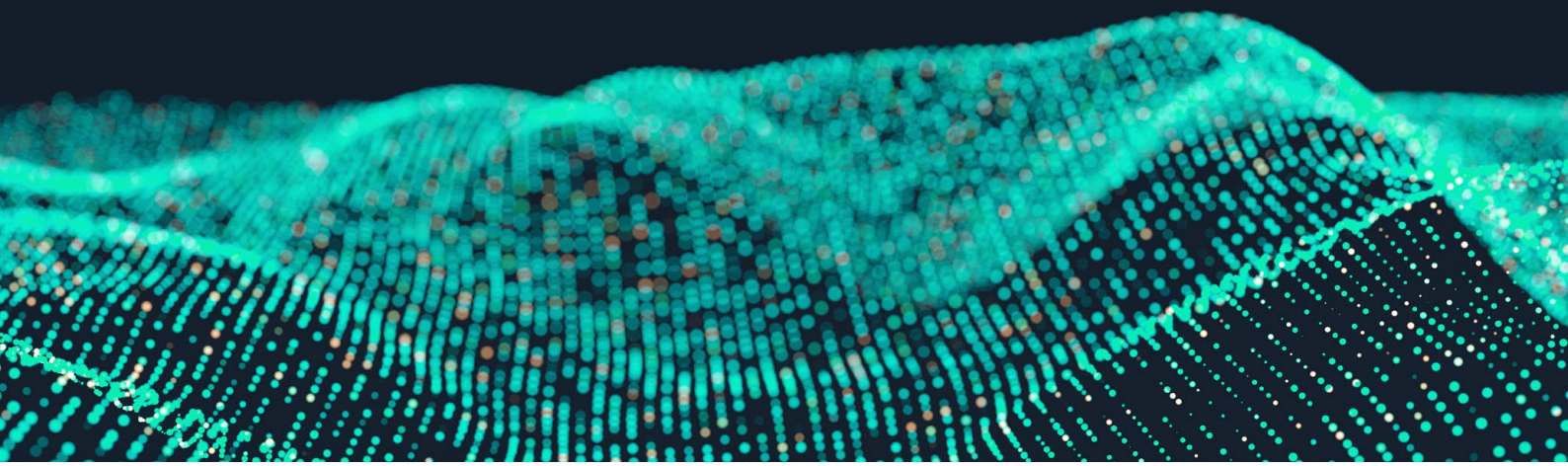
Guidance for banks for assessing and managing risks associated with third-party relationships.

Key guidance

- Adapt risk management processes in line with the level of risk and complexity of the third-party relationships in question
- Put in place plans to transition to alternative vendors or bring services in-house to mitigate risk in the event of contract defaults or termination, covering timeframes for transition, risks in relation to data retention and handling of joint intellectual property.
- If purchasing software, establish escrow agreements to ensure the bank's continuous access to source code and programs under certain conditions (e.g. insolvency of the third-party).

https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html





FINRA: members' responsibilities when outsourcing activities to third-party service providers

About FINRA

FINRA is a government-authorized, not-for-profit organization that oversees US broker-dealers.

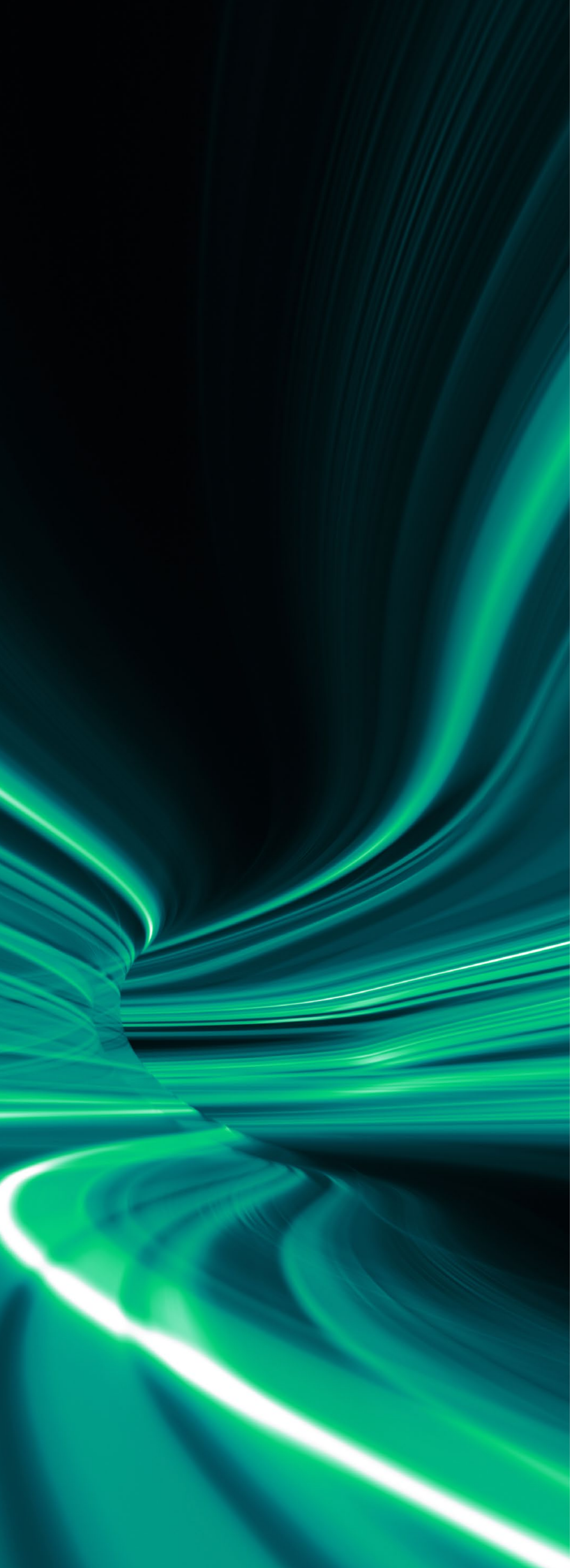
What is it?

Considerations for firms that use—or are contemplating using—third-party vendors, to establish whether their procedures and controls for outsourced activities and functions are sufficient.

https://www.finra.org/rules-guidance/notices/21-29

Key guidance

- Firms should create and maintain a written business continuity plan with procedures that are designed to enable firms to meet existing obligations to customers, counterparties and other broker-dealers during an emergency or significant business disruption.
- Organizations must have written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information that are reasonably designed to:
  1. ensure the security and confidentiality of customer records and information;
  2. protect against any anticipated threats or hazards to the security or integrity of customer records and information;
  3. protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.



How can organizations ensure compliance?

Financial institutions should focus on mitigating third-party risk from the outset when establishing new outsourcing agreements, as well as evaluating existing agreements.

This can include:

- Ensuring that audits and risk assessments of supply chains are regularly carried out
- Implementing a software escrow solution to protect business-critical data and applications
- Having a robust exit strategy in place as part of agreements with third parties wherever possible
- Reviewing existing contracts to understand risks, and what efforts can be taken to remediate or reduce those risks
- Recognizing that cloud/SaaS deployments carry different risks than on-premises providers, and further scrutiny and consultation is encouraged.

With this foundation of strong operational resilience in place, organizations will be well positioned to grow, innovate, and remain compliant amidst a changing landscape.

To find out more about how your organization can boost resilience and compliance, get in touch today.

nccgroup | SOFTWARE RESILIENCE

For support in starting your journey to SaaS Resilience, or for more information on how NCC Group Software Resilience solutions can support your business, get in touch with our team of in-house legal and technical experts at:

response@nccgroup.com

www.softwareresilience.nccgroup.com