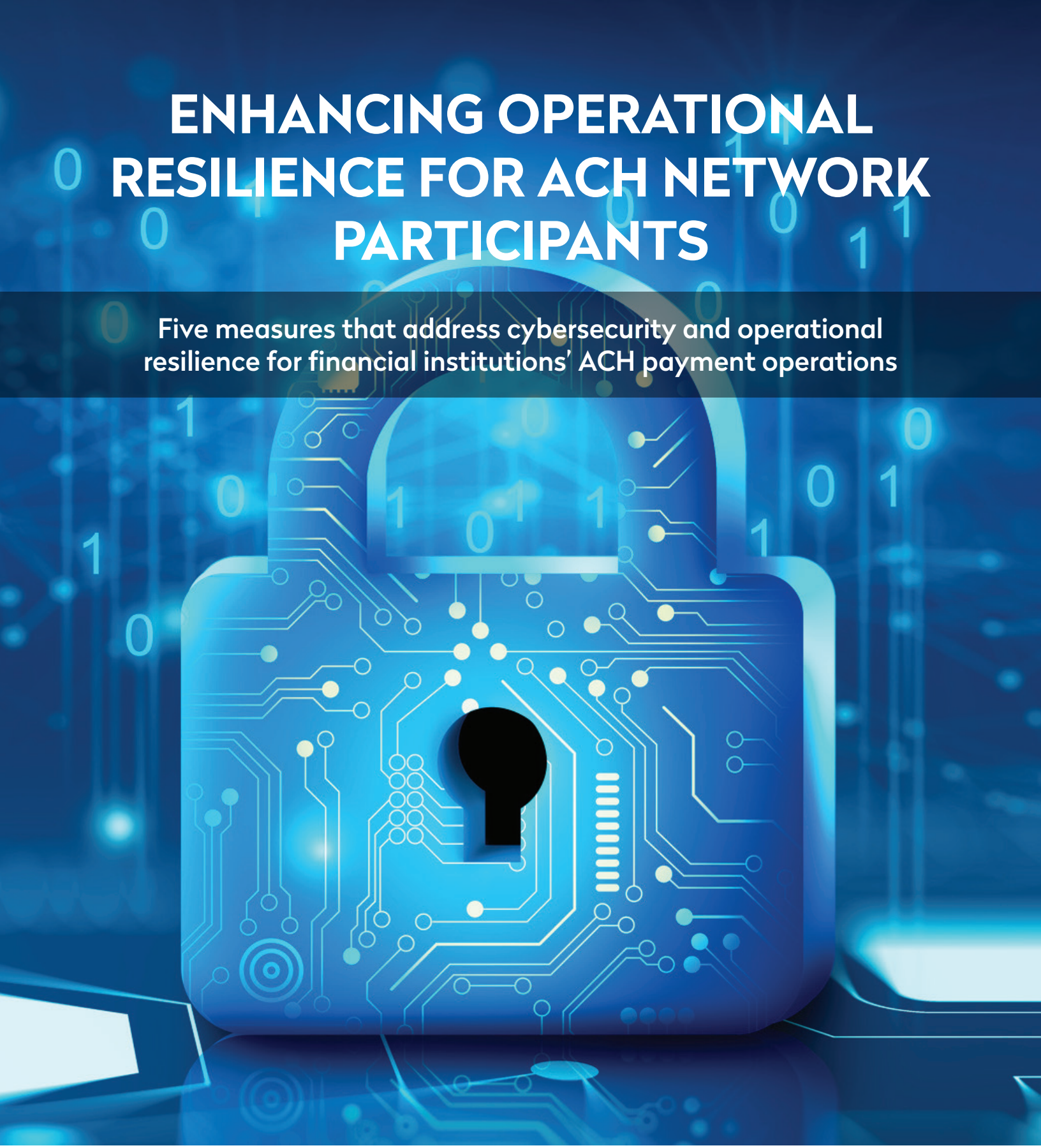
ENHANCING OPERATIONAL RESILIENCE FOR ACH NETWORK PARTICIPANTS

Five measures that address cybersecurity and operational resilience for financial institutions' ACH payment operations



ACH Network

Global Resilience Federation

Nacha®

A Joint Paper by the Global Resilience Federation and Nacha

Executive Summary

Growing cybersecurity threats and regulatory concerns have amplified the need for increased operational resilience around all critical banking and payments functions. Nacha's Risk Management Advisory Group (RMAG)[1] and the Global Resilience Federation (GRF) believe the five measures outlined in this document are significant to the operational resilience of ACH processing by financial institutions and third parties. Specifically, Originating Depository Financial Institutions (ODFIs) and Receiving Depository Financial Institutions (RDFIs) should consider these measures to enhance the operational resilience of their ACH processing:

1) **Develop, review, and update annually all ACH incident and recovery plans that address disruption or impairment to ACH Critical Services.**

2) **Define minimum ACH service levels that can satisfy the needs of customers, partners and counterparties before the service is no longer useful.** These are the Minimum Viable Service Levels (MVSLs) for ACH services which define the "lowest possible level of service delivery (i) to enable customers, partners, and counterparties to continue their operations without significant disruption to the delivery of their critical services to their own customers, partners, and counterparties; or (ii) if the customer is an individual, to minimize consumer harm."

3) **Establish Service Delivery Objectives for how quickly ACH services can be restored to a target impaired state with considerations of both business and technical dependencies.**

4) **Implement recovery environment, processes, and mechanisms to meet Service Delivery Objectives for ACH services.**

5) **Independently evaluate and test ACH service restoration processes against Service Delivery Objectives.**

Nacha and the GRF offer these measures for several reasons:

1. Paradigm Shift – business process impairment is no longer limited to physical threats. Continuity and recovery plans must adapt to account for non-physical threats.
    - Malicious and sophisticated cyberattacks from nation states, cybercriminals, and hacktivists pose an increasing threat to organizations and individuals. These advanced and persistent threats make recovery an ongoing challenge for targeted organizations.
    - In the past, cyberattacks mostly sought to carry out fraud or disruption. Now, destructive malware attacks result in both primary and backup systems becoming compromised either through encryption from ransomware or from wiperware capable of destroying core operating systems, backups, networks, devices, and systems architecture.

[1] The Risk Management Advisory Group serves in an advisory capacity to the Nacha executive management and Board of Directors on risk management related topics to assure ongoing strength, stability, and continued high quality of the ACH Network. The Group works with Nacha staff and key industry stakeholders to produce sound business practices, business cases for rules proposals, Board Policy Statements, tools, white papers and other communications vehicles, and to collaborate and coordinate with payments professionals across payments channels.

2) Regulatory Attention – U.S. financial regulators, through the Federal Financial Institutions Examination Council[2], want financial institutions of all sizes to address Operational Resilience.

   - FFIEC IT Examination Handbooks provide guidance to financial institution examiners on a range of topics. Its booklets "Business Continuity Management", "Information Security", and "Architecture, Infrastructure, and Operations" each emphasize important aspects of resilience.

The discipline of Operational Resilience evolved out of traditional Business Continuity and Recovery Management functions. A key concept of Operational Resilience is for firms to establish Minimal Viable Service Levels (MVSLs) for their Operations Critical services. Operations Critical components are the data, systems, and processes that require near-continuous functioning to limit service disruptions and impacts to customers, business partners, and other counterparties. Operational Resilience transcends disciplines and encompasses strategic considerations rather than a set of discrete actions associated with traditional business continuity management. Operational Resilience coordinates management of risk assessments, risk monitoring and execution of controls that impact workforce, processes, facilities, technology, and third parties across various risk domains in delivery of business services such as ACH. Organizations in which ACH services fall into the category of Operations Critical can benefit from a focus on Operational Resilience.

Background: The Operational Resilience Framework

The Global Resilience Federation (GRF) is a nonprofit corporation that supports 17 different information sharing communities. One of these groups is the Business Resilience Council (BRC). The BRC is a multi-sector, all-hazards information sharing initiative that developed the Operational Resilience Framework (ORF). The framework provides rules and implementation aids that support a company's recovery of immutable data while uniquely allowing it to minimize service disruptions in the face of destructive attacks and events. The ORF Work Group within the BRC developed the ORF to be broadly applicable and aligned with existing controls like those from the National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO).

The ORF Work Group pursues specific objectives and follows clear guiding principles:

- Address regulatory requirements by providing an outcome-based rather than a prescriptive solution to operational resilience and recovery concerns arising from adverse events.
- Support continuity and recovery of critical data, systems, and processes required to minimize service disruptions to customers, business partners, and other counterparties.
- Utilize a risk-based approach to drive appropriate investment in operational resilience activities across people, processes, and technology.
- Align to broadly adopted industry standards and minimize use of new terminology.

[2] The Federal Financial Institutions Examination Council (FFIEC) is the interagency organization whose members include the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB). The FFIEC's State Liaison Committee (SLC) includes representatives from the Conference of State Bank Supervisors (CSBS), the American Council of State Savings Supervisors (ACSSS), and the National Association of State Credit Union Supervisors (NASCUS).

- Contribute significantly to the operational resilience of organizations that follow the framework.
- Identify an operational resilience maturity model that organizations can follow regardless of size or sophistication.
- Address significant disruption of business operations from adverse events regardless of the cause.

The ORF is the result of two years of development by over 100 organizations to meet the stated objectives. The ORF consists of 37 rules that enterprises can use as a path to achieve operational resilience across critical systems and processes for their respective organizations. Version 1.0 of the ORF is available at www.grf.org/orf.

Threat Assessment

Threats to financial institutions can have a severe and potentially debilitating impact to Operations Critical functions. The five recommended operational resilience measures address the impact these threats can have:

- Sophisticated social engineering attacks often bypass cybersecurity identity management, detection, and prevention solutions. As a result, a threat actor can gain access to critical systems to successfully infect the targeted operations.
- Ransomware and wiperware attacks often target both critical operations and data backup, thus making access and recovery impossible.
- Devices, applications, and system architectures can be completely wiped by certain variants of destructive malware.
- Cloud providers may be compromised and may become unavailable during a massive distributed denial of service (DDoS) or destructive malware attack.

Appreciating the evolution of cyberthreats to financial institutions can help one gain a better understanding of why operational resilience has become an important topic.

1) Account Takeover

Starting in 2008-2010, threat actors began to launch phishing attacks against businesses and financial institutions. Successful phishing attacks dropped banking trojans into the systems of targeted organizations. The trojans allowed the cybercriminals to access online banking systems used by the targeted organization and move funds out of financial institutions. The schemes used ACH and other payment methods to send the funds within the U.S. to bank accounts held by money mules. The money mules would then use international wire transfer instructions or money transfer companies to send the funds to the cybercriminals mostly located in Russia and Eastern European countries.

When the money mule networks were disrupted by law enforcement, the cybercriminals began to wire funds overseas directly from the targeted organization's bank or convert the funds to cryptocurrency.

2) Business Email Compromise (BEC) and Impersonation Fraud

Initially, both financial institutions and their business customers were targeted with BEC schemes. These schemes vary and continue to evolve, but three examples illustrate the concept:

a) Emails, telephone, or written instructions to the targeted organization instruct payors to change an invoice's payee account number and payee bank to the fraudster's account. (This scenario is also known as Vendor Impersonation.)

b) Instructions to the accounts payable department, CFO, or other authority within the targeted company that appear to be coming from the CEO or other executive request that funds be moved immediately to what turns out to be an account set up by the perpetrator. (This scenario is also known as Impostor Fraud.)

c) Instructions that appear to come from a legitimate employee instruct an employer's payroll department to change routing and account numbers for the employee's Direct Deposit account. (This scenario is also known as Payroll Impersonation.)

Financial institutions have implemented security procedures and multifactor authentication tools to reduce this type of fraud against institutions' staff. However, BEC attacks remain common among business and consumer customers of the institutions. Between October 2013 and December 2022, the FBI's Internet Crimes Complaint Center (IC3) received victim complaints of more than $17 billion in losses due to BEC fraud.[3]

3) Distributed Denial of Service (DDoS)

DDoS attacks have targeted financial institutions and businesses for over 10 years. For financial institutions, threat actors generally target online banking systems, causing a loss of access to accounts by legitimate users. The threat actors utilize botnets to create large-bandwidth attacks against online banking systems, ranging as high as 3 1/2 terabytes per second. Attacks can disrupt online banking services for extended periods.

4) Ransomware

Cybercriminals have used ransomware to encrypt data of targeted organizations, then extorted money from the victims to release decryption keys. Ransomware has targeted many different sectors, including financial services, healthcare, education, defense industry, retailers, and government. In some cases, the data can be restored by either employing a company with capabilities to decrypt the data or by paying the ransom. Nation states have used ransomware to disguise attacks against other countries' critical infrastructures. The actor may appear to ask for a ransom, but offers no viable way to pay the ransom, so the victim's systems remain encrypted and inaccessible.

[3] FBI Public Service Announcement Alert Number I-060923-PSA, June 9, 2023.

5) Destructive Wiperware

Destructive wiperware has been used as an espionage tool between nation states. Stuxnet was an attack that destroyed centrifuges used by Iran for its nuclear development program. The wiperware known as Shamoon was used to attack Saudi Aramco and RasGas, which resulted in the deletion of three-quarters of the companies' data and destruction of more than 30,000 computers that had to be replaced.

Nation state actions involving wiperware have also targeted critical infrastructure and private enterprises. For example, North Korea has targeted banks in South Korea, delivering malware disguised as patch management updates. North Korea also targeted Sony Pictures and wiped its systems so that Sony could not produce financials for six months.

More recently, Russia has been identified as one of the primary threat actors that has used destructive malware to target critical infrastructure, including financial services. A Russian hacking firm known as Vulcan is providing critical infrastructure target data for the Russian government. The Western press learned this from a Russian employee of Vulcan who is a Ukrainian war dissenter.

Federal Response

Following the Russian invasion of Ukraine, the United States, United Kingdom, Canada, Australia and New Zealand cybersecurity authorities issued a Cybersecurity Advisory (CSA) (revised May 9, 2022, CISA Alert AA22-110A). The CSA provided intelligence concerning technical details for Russian-sponsored cyber operations against NATO countries' critical infrastructure, and the infrastructure of other countries that back sanctions against Russia.

Since the issue of the CSA, the Biden administration's top cybersecurity aide, Anne Neuberger, has described an increase in "preparatory activity," such as scanning websites and hunting for vulnerabilities. More recently, the FBI has identified at least five U.S. energy companies that have been targeted, and dozens of other companies targeted in the financial, defense industrial base, and information technology sectors. The FBI issued an alert regarding destructive malware against critical infrastructure.

On April 6, 2022, the Justice Department announced that the FBI had secretly and successfully disabled and removed "Cyclops Blink" botnet globally, preempting a Russian cyberattack. The botnet was operated by the GRU, the intelligence arm of the Russian military. The reason given for this action was the increased willingness of Russia to cause digital damage against U.S. critical infrastructure in energy, financial institutions, and communications.

Emphasis on Operational Resilience by U.S. Banking Regulators

Starting in 2019, the FFIEC has issued guidance and recommendations to strengthen operational resilience for the financial institutions it regulates.

From the FFIEC "Business Continuity Management" Booklet:

"Disruptions such as cyber events, natural disasters, or man-made events can interrupt an entity's operations and can have a broader impact on the financial sector. Resilience incorporates proactive measures to mitigate disruptive events and evaluate an entity's recovery capabilities.

Management should evaluate whether there are appropriate resources to ensure resilience, including an accessible, off-site repository of software, configuration settings, and related documentation, appropriate backups of data, and off-site infrastructure to operate recovery systems.

Furthermore, management should discuss potential disaster scenarios with the entity's third-party service providers to prepare for an event. Subsequently, management should assess the entity's immediate or short-term space requirements, systems, and personnel capacity to assume or transfer failed operations. Additionally, management should assess critical third-party service providers' susceptibility to simultaneous attacks and verify their resilience capabilities.

... a firm also should identify and address the resilience of other operations, services, and functions for which a disruption could have a significant adverse impact on the firm or its customers as part of operational resilience planning. Critical operations and core business lines are defined as follows: 1) Critical operations are those operations of the firm, including associated services, functions, and support, 2) the failure or discontinuance of which would pose a threat to the financial stability of the United States, 3) Core business lines are those business lines of the firm, including associated operations, services, functions, and support, that, in the view of the firm, upon failure would result in a material loss of revenue, profit, or franchise value."[4]

[4] FFIEC IT Booklet, "Business Continuity Management," FFIEC IT Examination Handbook InfoBase - Home.

The FDIC invited GRF leadership to a meeting in December 2022 to discuss GRF's Operational Resilience Framework. This resulted in an invitation to meet with all the FFIEC agencies in March 2023 to explain the core concepts of the ORF and to seek FFIEC input regarding the 37 rules contained in the ORF.

Representatives of the FFIEC member agencies expressed general consensus that the ORF meets many of the goals set forth by the various regulators and provides a private sector-driven approach to operational resilience. The ORF provides a roadmap for implementing the concepts of the FFIEC IT Examination Handbook "Business Continuity Management."

Operational Resilience Measures for ACH Participants

These five measures address operational resilience for ODFIs and RDFIs. Nacha and the GRF believe these measures may significantly mitigate the impact of an event designed to cause a significant disruption of service for ACH participants. ODFIs, RDFIs, and Third-Party Service Providers should consider the application of these measures to their operations:

1) **Develop, review, and update annually all ACH incident and recovery plans that address disruption or impairment to ACH Critical Services.**

   a. ACH business continuity and crisis management plans would need to be expanded to include provisions for disruption or impairment to the delivery of ACH services due to destructive attacks.

   b. ACH incident and recovery plans would need to be developed and updated annually.

2) **Define minimum ACH service levels that can satisfy the needs of customers, partners and counterparties before the service is no longer useful.**

   a. This is a study of the extent of service disruption regardless of root cause. By way of example, consider a bridge with two of three lanes closed. It is not important to consider why the lanes are closed, only that the capacity of the bridge to process traffic may be one-third or less when the lanes are closed.

   b. For ODFIs, minimal ACH service levels could be defined as later or less frequent deadlines for submitting ACH files for origination.

   c. For RDFIs, minimal ACH service levels could be defined as later ACH postings or availability of funds than typically provided or required.

Financial institution might consider whether to address minimum service levels in customer agreements.

3) **Establish Service Delivery Objectives for how quickly ACH services can be restored to a target impaired state with considerations of both business and technical dependencies.**

   a. Considerations can be made for off-ramping ACH processing to separate air-gapped, geographically dispersed platforms.

   b. Separate ACH processing platforms should be tested periodically to ensure minimal service disruption.

   c. Decisions must be made on what is an acceptable impaired state, including speed of ACH processing, time delays in restarting ACH processing, and relaxation of security, operational risk, and other controls.

4) **Implement recovery environment, processes, and mechanisms to meet Service Delivery Objectives for ACH services.**

   a. Recovery environment solutions should focus on both physical and cyber-destructive events.

   b. Cloud providers may be able to offer recovery solutions that meet ACH minimal service level requirements as defined by an institution for both origination and receipt/posting of ACH payments.

   c. Financial institutions may want to arrange with other FIs to handle their ACH origination volume in case of a major disruption of service availability. Systems architecture highlights the interdependence of key systems during a destructive event. The ability to receive and post ACH payments to customers' accounts can be challenging or even impossible if both ACH and demand deposit/savings account systems are impacted.

5) **Independently evaluate and test ACH service restoration processes against Service Delivery Objectives.**

   a. Ensure minimum viable ACH service levels are met as defined in Measure No. 1.

   b. Ensure Service Delivery Objectives are met in a targeted impaired state as defined in Measure No. 2.

Conclusion

Traditional and novel threats can disrupt business processes from desired states of operation that wide sectors of the economy and society depend upon in everyday life. Malicious actors seek to disrupt these processes for a variety of reasons. Payment systems and their participants are certainly targets of malicious actors, and of course are vulnerable to natural disasters as well. Whatever the cause of disruption, Nacha and the Global Resilience Federation believe the measures outlined in this document, which derive from the Operational Risk Framework developed by the GRF's Business Resilience Council, can help ensure the operational resilience of ACH processing by financial institutions and third parties that experience disruption from known or emerging threats, as well as address regulatory expectations regarding business continuity. Both organizations appreciate the reader's engagement with the topics addressed in this paper.

Appendix 1 - ORF Key Terms

Operational Resilience Executive – Qualified executive with the responsibility and authority to ensure appropriate organizational support, implementation, and oversight for Operational Resilience.

Minimum Viable Service Level – The lowest possible level of service delivery (i) to enable customers, partners, and counterparties to continue their operations without significant disruption to the delivery of their critical services to their own customers, partners, and counterparties; or (ii) if the customer is an individual, to minimize consumer harm.

Operations Critical – Operations critical components are data, systems and processes that require near-continuous functioning to limit service disruptions and impacts to customers, business partners and other counterparties.

Business Critical – Business critical components are data, systems and processes required to prevent long-term disruption of business services required for the organization's continuity.

All Other Services (AOS) – Services necessary to support the business at pre-event levels.

Operations Critical and Business Critical Data Sets – Comprehensive data sets supporting recovery and restoration of critical services.

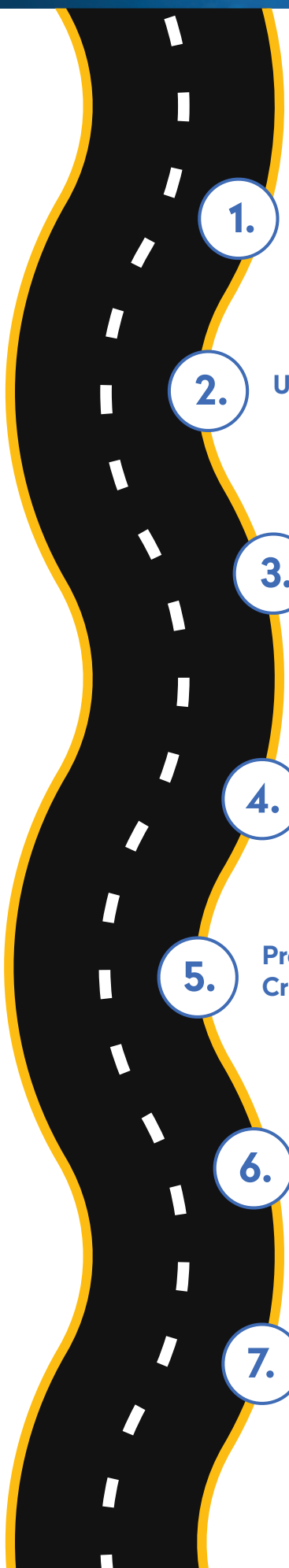
Service Delivery Objectives – The objectives that set the impaired level and time constraints for delivery of Critical Service in the event of a disruption.

Data Restoration Objectives – The objectives that define the specific data that must be restored to reach the impaired level of operationality set by the Operations Recovery Objectives.

Operational Resilience Plan – The plan used to guide an enterprise-wide response to an adverse event or destructive attack which ensures continuity of critical services to meet Service Delivery Objectives.

Appendix 2 - Path to Operational Resilience

Operational Resilience Framework Download ORF v1.0 here (www.grf.org/orf)



Path to Operational Resilience

1. Implement an industry-recognized IT, OT and cybersecurity control framework.
2. Understand the organization's role in the ecosystem.
3. Define the Minimum Viable Service Levels for each Operations Critical and Business Critical service.
4. Establish Service Delivery Objectives for each Operations Critical and Business Critical service.
5. Preserve the Data Sets necessary to support Operations Critical and Business Critical services.
6. Implement processes to enable recovery and restoration of Operations Critical and Business Critical services to meet Service Delivery Objectives.
7. Independently evaluate design and test periodically.

Appendix 3 - About the Sponsor Organizations

The Global Resilience Federation is a nonprofit corporation consisting of 17 different information sharing communities representing industries and organizations from finance, retail, education, energy, manufacturing, transportation, and professional services. GRF's mission is to share security best practices, threat intelligence, and other information which reduces risk and enhances the resilience of members and their respective sectors.

Nacha governs the ACH Network, the payment system that drives safe, smart, and fast Direct Deposits and Direct Payments with the capability to reach all U.S. bank and credit union accounts. Thirty billion ACH Network payments were made in 2022, valued at nearly $77 trillion. Through problem-solving and consensus-building among diverse payment industry stakeholders, Nacha advances innovation and interoperability in the payments system. Nacha develops rules and standards, provides industry solutions, and delivers education, accreditation, and advisory services.