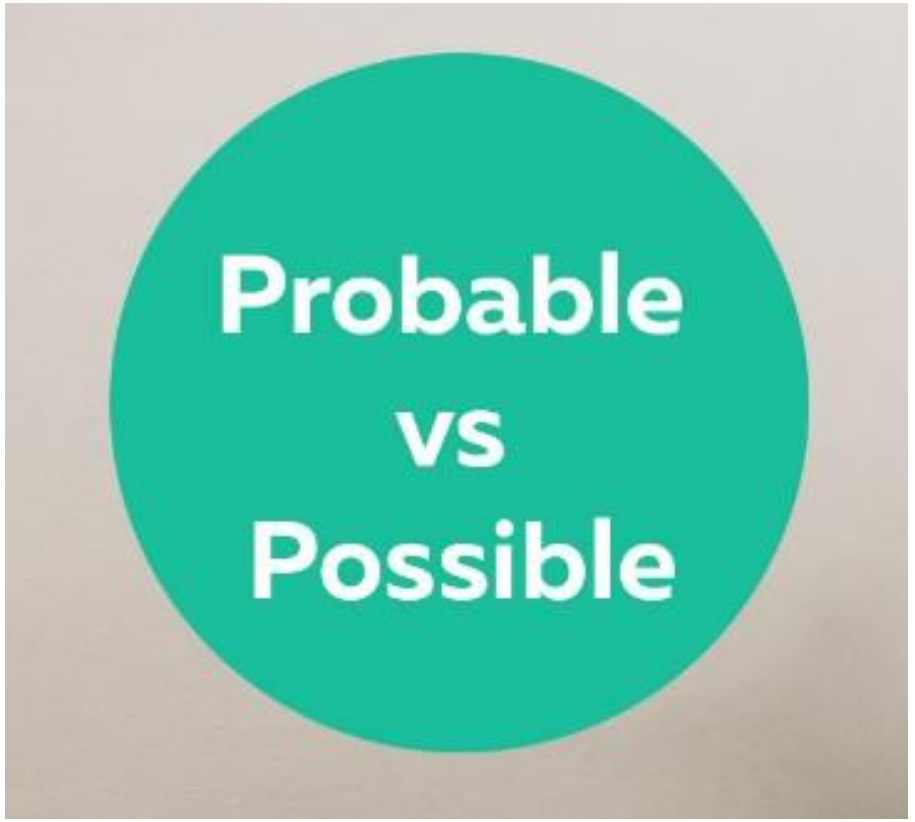
# Possible or Probable? How to Assess the Risk




Presented by:

**Macha/PAR – Everything Payments - Everywhere**

Jessica Lelii, AAP, APRP

Director of Education

www.macha.org

jlelii@macha.org

# DISCLAIMER

Macha, through its Direct Membership in Nacha, is a specially recognized and licensed provider of ACH education, publications and support.

Payments Associations are directly engaged in the Nacha rulemaking process and Accredited ACH Professional (AAP) program.

Nacha owns the copyright for the Nacha Operating Rules & Guidelines.

The Accredited ACH Professional (AAP) and Accredited Payments Risk Professional (APRP) is a service mark of Nacha.

This material is derived from collaborative work product developed by Nacha and its member Payments Associations and is not intended to provide any warranties or legal advice and is intended for educational purposes only.

This material is not intended to provide any warranties or legal advice and is intended for educational purposes only.

This document could include technical inaccuracies or typographical errors and individual users are responsible for verifying any information contained herein.

# Agenda

- Risk Assessment and the ACH Rules
- Risk Assessment
- FFIEC
- The National Infrastructure Protection Plan (NIPP)
- Risk Assessment Methodologies
- Types of Risk
- Areas/Activities to be Assessed

# Possible vs. Probable

- Pos si ble
  - *adjective*
  - able to be done; within the power or capacity of someone or something
- Prob a ble
  - *adjective*
  - likely to be the case or happen

*Oxford's English Dictionaries*

# Risk Management

Identify

Risk Assessment

Measure

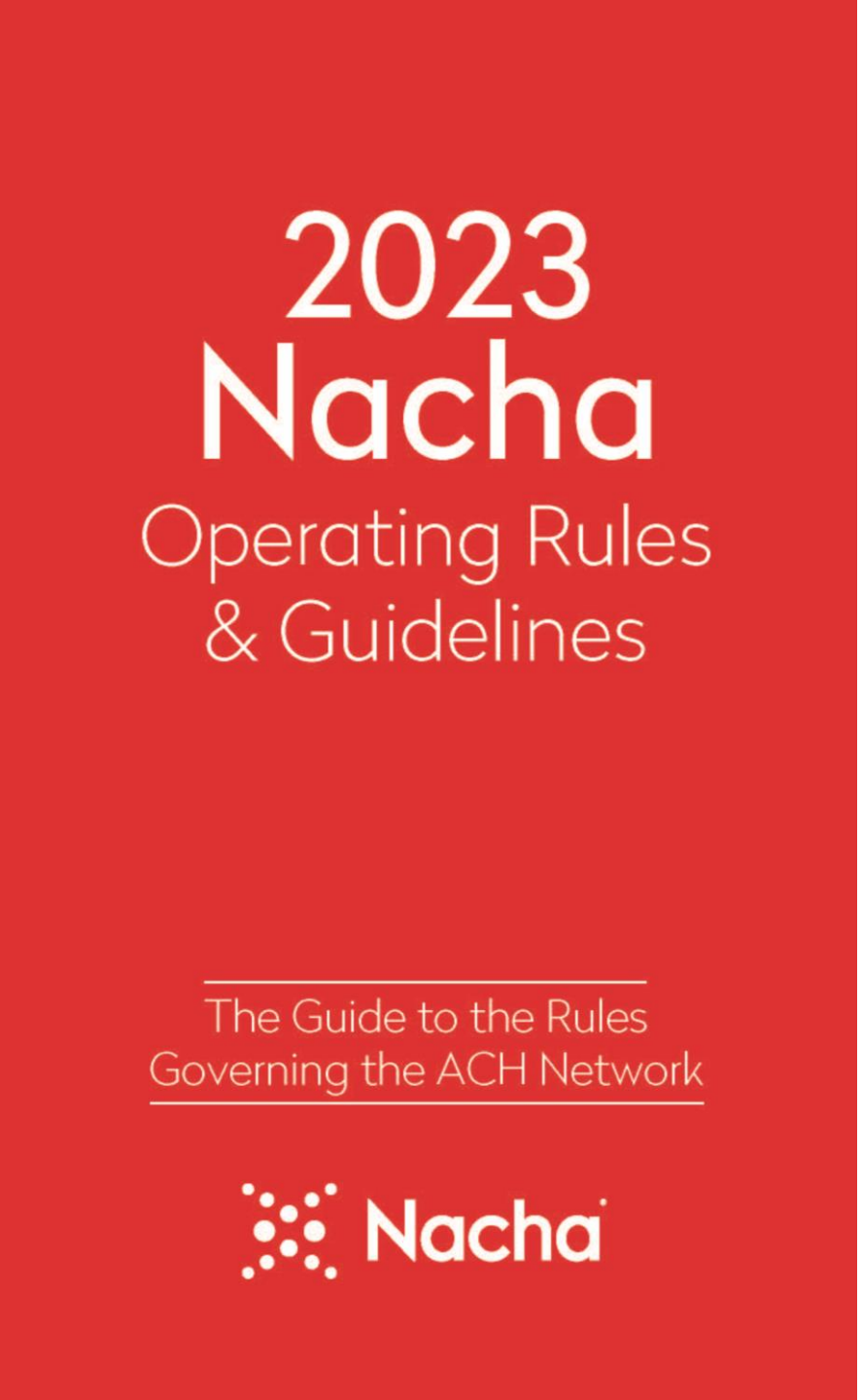
Risk Analysis or Evaluation

Mitigate

Implement controls

Monitor

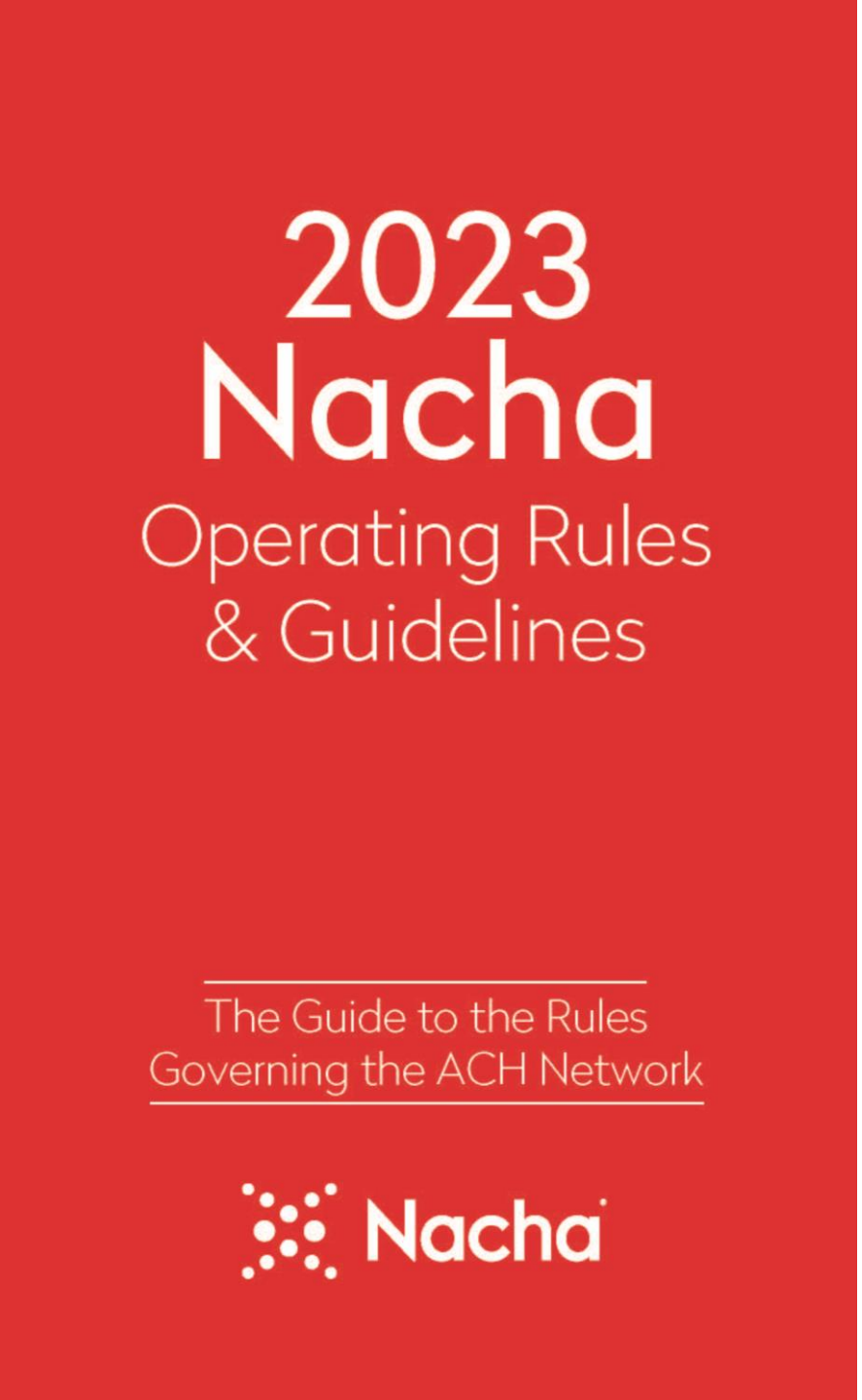
Tracking and reporting




# Risk Assessment Requirement

- A Participating DFI and a (Nested) Third-Party Sender must:
  - (a) conduct, or have conducted, an assessment of the risks of its ACH activities;
  - (b) implement, or have implemented, a risk management program based on such an assessment; and
  - (c) comply with the requirements of its regulator(s) with respect to such assessment and risk management program.

*Nacha Operating Rules, Article One, Subsection 1.2.4 Risk Assessments*




# Risk Assessment

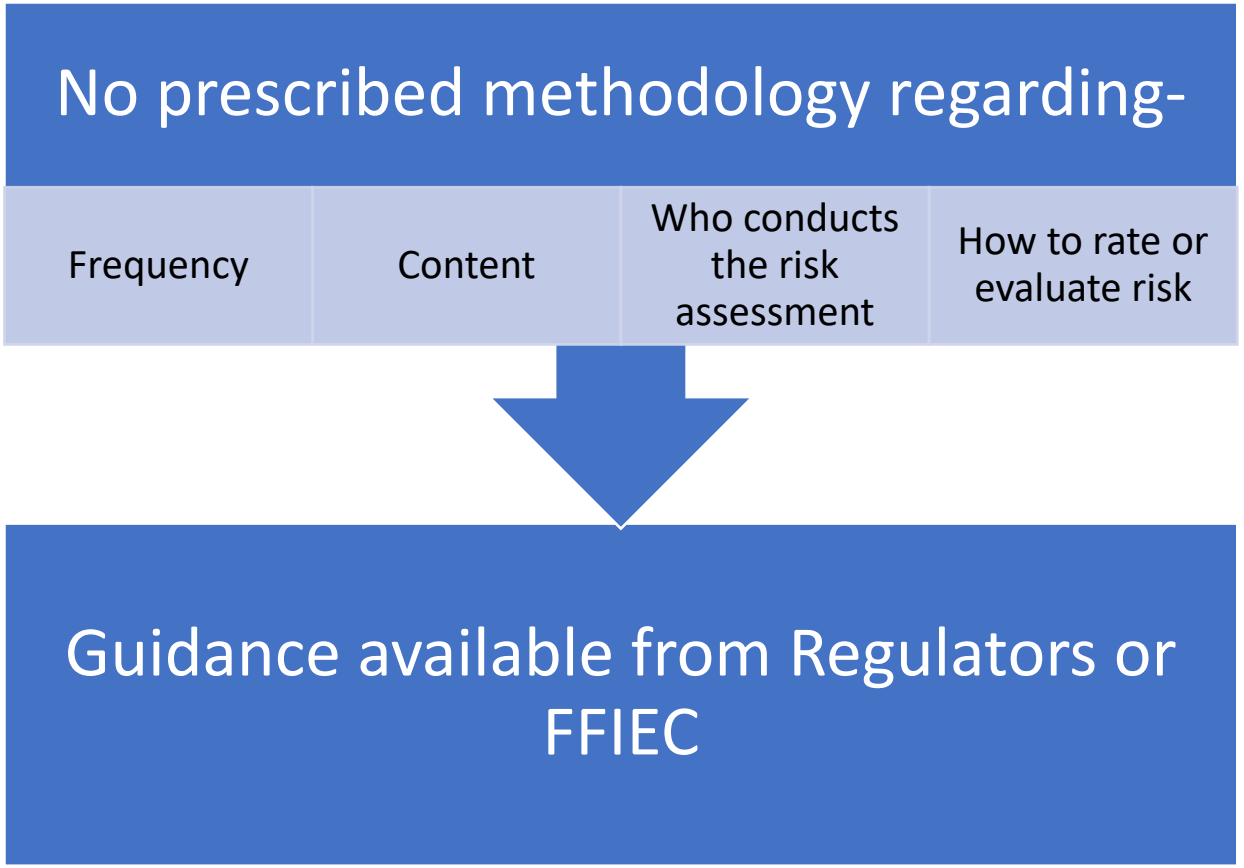
- Generally, regulators stress the importance of:
  - Assessing the nature of risks associated with ACH activity
  - Performing appropriate know-your-customer due diligence
  - Establishing controls for Originators, third-parties, and direct-access to ACH Operator relationships
  - Having adequate management, information and reporting systems to monitor and mitigate risk

*Nacha Operating Guidelines, Section One, Chapter 4 General Rules*

# Risk Assessment

- Measures the effectiveness of the control activities to determine the level of residual risk remaining
  - Residual risk – the portion of risk remaining after mitigation measures have been applied
- Mapping the risks to each control helps the organization find any gaps remaining in its compliance program
- Risk assessment should:
  - Estimate the significance of the risk
  - Assess the likelihood or frequency of the risk occurring
  - Consider how the risk should be managed and assess what action must be taken

# Risk Assessment




# Risk Assessment and FFIEC

# FFIEC- Federal Financial Institution Examinations Council

- A formal inter-agency body empowered to prescribe uniform examination principles and standards for the federal examination of financial institutions
- Comprised of-
  - Board of Governors of the Federal Reserve Systems (FRB)
  - Federal Deposit Insurance Corporation (FDIC)
  - National Credit Union Administration (NCUA)
  - Office of the Comptroller of the Currency (OCC)
  - Consumer Financial Protection Bureau (CFPB)

# FFIEC Guidance on Risk Assessment

- Risk assessment is the process of identifying risks to operations, organizational assets, individuals, and other organizations
- Incorporates threat and vulnerability analyses and addresses the appropriate mitigations
- Risk assessment should be commensurate with the entity's risk and complexity
- Includes:
  - Risk Identification
  - Risk Analysis

*FFIEC IT Examination Handbook, Business Continuity Management*

# Why Do We Assess Risk?

- All activities within a financial institution present a degree of risk
  - **Inherent Risk:** risks before applying controls and other mitigations
- Senior management should make risk management decisions based on a full understanding of identified risks
- Determine if inherent risks are within the institution's risk appetite or risk tolerance
- Determine if risk treatment is necessary

*FFIEC IT Examination Handbook, Management*

# Risk Appetite and Tolerance

- **Risk Appetite:** the amount of risk, on a broad level, an entity is willing to accept in pursuit of value
  - Reflects the entity's risk management philosophy
  - Influences the entity's culture and operating style
  - Guides resource allocation

- **Risk Tolerance:** the acceptable level of variation relative to achievement of a specific objective
  - Operating within your risk tolerance helps ensure that the entity remains within its risk appetite

# Risk Treatments

- **Risk acceptance** – the informed decision to accept or take a particular risk
  - **With treatment** – risk will be mitigated, monitored and reviewed to ensure it remains within the risk appetite
  - **Without treatment** – risk is accepted as tolerable and falls within the risk appetite
- **Risk avoidance** – the informed decision to withdraw from or not become involved with an activity in order to avoid exposure to unwanted or unacceptable risk
- **Risk sharing** – an agreed-upon distribution of risk with other parties

# Risk Identification

- Management should identify and inventory the entity's internal and external assets, types of threats and hazards, and existing controls as an important part of effective risk identification.
- Management should identify interconnectivity points between the entity and its third-party service providers, as well as between other entities and third-party service providers.
  - Documenting the flow of transactions, such as developing formal process diagrams, may help management identify interdependencies and end-to-end processes.

*FFIEC IT Examination Handbook, Business Continuity Management*

# Risk Analysis

- Risks may range from those with a high likelihood of occurrence and low impact, to those with a low probability of occurrence and high impact.
- As part of the assessment, management should quantify the impacts and define loss criteria as either quantitative (financial) or qualitative (e.g., impact to customers, reputational impact).

*FFIEC IT Examination Handbook, Business Continuity Management*

# Risk Scoring

In establishing a scoring system, the board of directors and management should ensure the system is understandable, considers all relevant risk factors, and, to the extent possible, avoids subjectivity.

*FFIEC IT Examination Handbook, Audit*

# Major risk factors commonly used in scoring systems include:

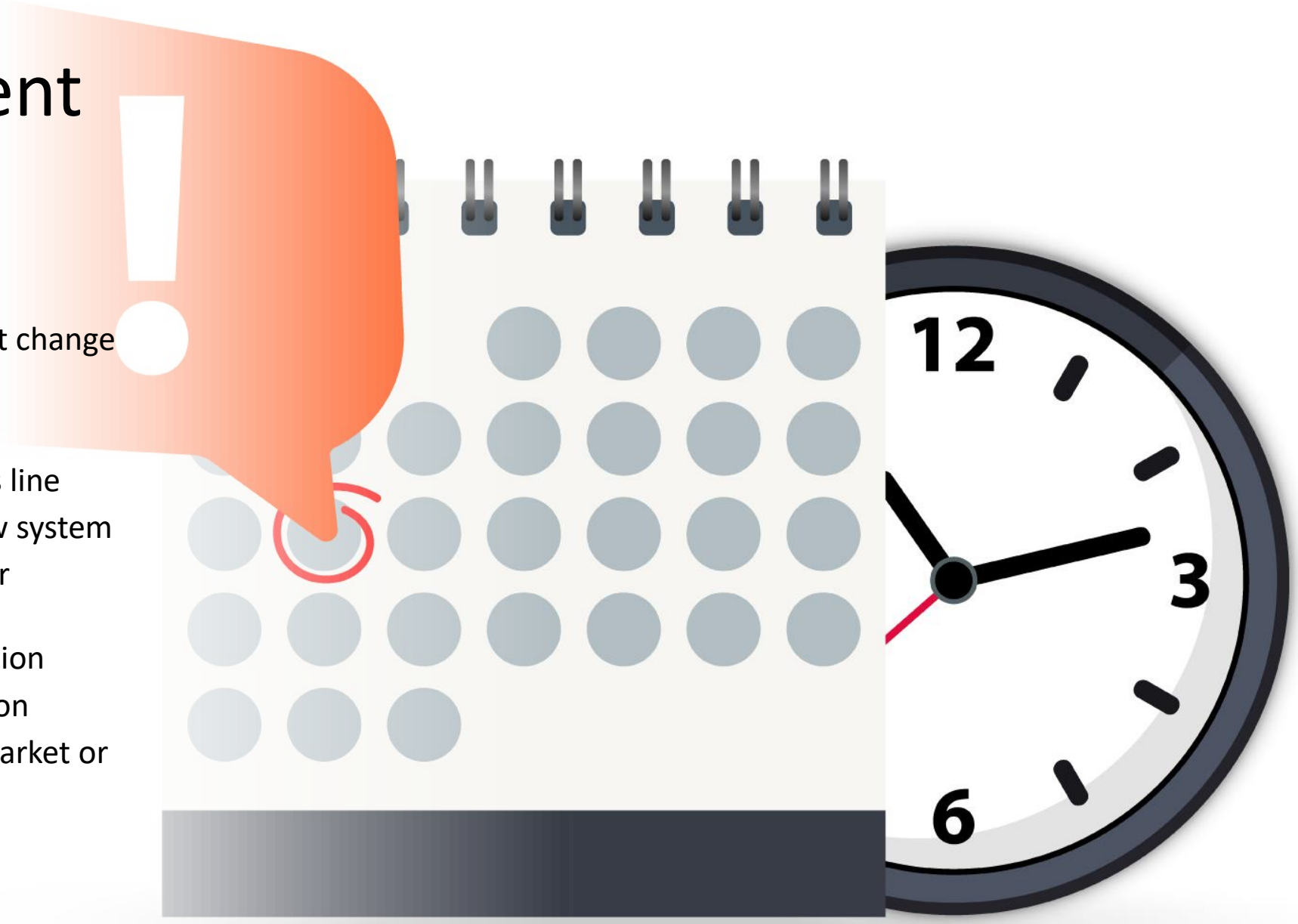
- Adequacy of internal controls
- Nature of transactions
  - Number, dollar volumes, complexity
- Age of the system or application
- Physical and logical security of information, equipment, and premises
- Adequacy of operating management oversight and monitoring
- Nature of operating environment
- Senior management oversight
- Previous regulatory and audit results and management's responsiveness
- Human resources
  - Experience of management and staff, turnover, technical competence and degree of delegation

# Risk Assessment Policy

- Frequency or timing
- Who will conduct
- Methodologies
- Documentation requirements to support scoring
- Acceptable risk treatments
- Board approval
- Guidelines of overriding risk assessments in special cases and the circumstances under which they can be overridden
  - Who can override?
  - How is it approved, reported and documented?

# Risk Assessment Frequency

- Annually, or when a significant change occurs
- Significant changes include:
  - New product or business line
  - Implementation of a new system
  - Application conversion or upgrade
  - Changes to the organization
    - Merger or acquisition
    - Growth into new market or geographic location
  - Staffing changes



# The National Infrastructure Protection Plan (NIPP)

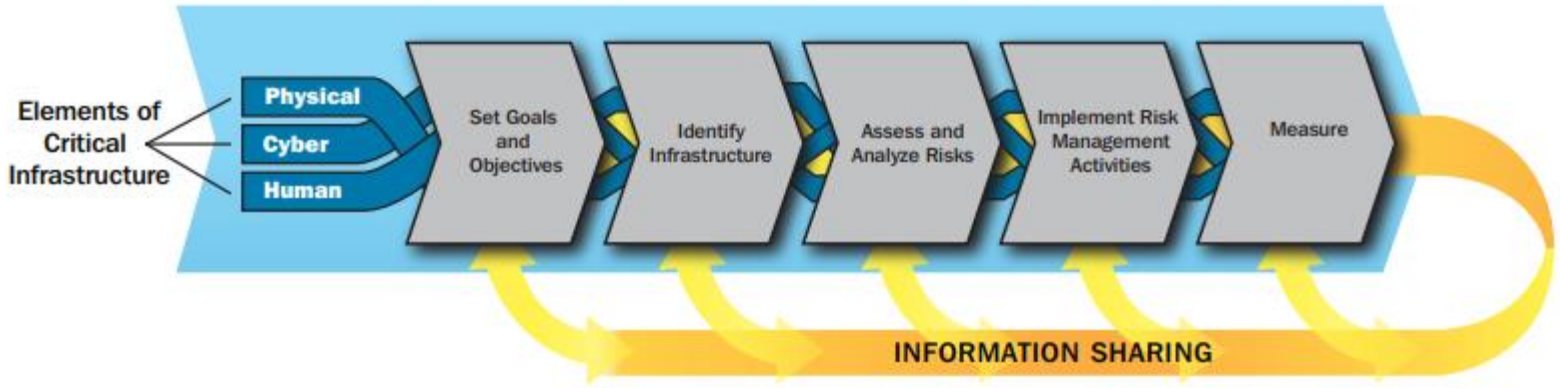
Executing a Critical Infrastructure Risk Management Approach

# Executing a Critical Infrastructure Risk Management Approach

The Department of Homeland Security's (DHS) National Infrastructure Protection Plan19 provides examples of risk measurement processes and methodologies to help analyze risks.

https://www.cisa.gov/sites/default/files/publications/NIPP-2013-Supplement-Executing-a-CI-Risk-Mgmt-Approach-508.pdf

Figure 1: Critical Infrastructure Risk Management Framework



# Assess and Analyze Risks

- Evaluate the risk, taking into consideration the potential direct and indirect consequences of an incident, known vulnerabilities to various potential threats or hazards, and general or specific threat information.
- Risks can be assessed in terms of their likelihood and potential consequences.
- It is important to think of risk as influenced by the nature and magnitude of a threat or hazard, the vulnerabilities to that threat or hazard, and the consequences that could result.

https://www.cisa.gov/sites/default/files/publications/NIPP-2013-Supplement-Executing-a-CI-Risk-Mgmt-Approach-508.pdf

# Assess and Analyze Risks

- **Threat:** A natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.
- **Vulnerability:** A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given threat or hazard.
- **Consequence:** The effect of an event, incident, or occurrence. It reflects the level, duration, and nature of the loss resulting from the incident.

# Risk Assessment Methodologies

# Risk Assessment Methodologies

- Quantitative
- Qualitative
- Semi-quantitative
- Asset-based
- Vulnerability-based
- Threat-based

https://drata.com/blog/risk-assessment-methodologies

# Risk Assessment Methodologies

**Quantitative**

- Assets and risks receive dollar values
- Results can be presented in financial terms
- Cost-benefit analysis can help prioritize mitigation options

**Qualitative**

- Assessors use employee input to categorize risk on scales such as high, medium, or low
- Provides a general picture of how risks affect operations

# Risk Assessment Methodologies

**Semi-quantitative**

- Combines quantitative and qualitative
- Uses a numerical scale (i.e., 1-100) to assign a value to risk
- Can be more objective and provide basis for prioritization

**Asset-based**

- Inventory all assets
- Evaluate the effectiveness of existing controls
- Identify the threats and vulnerabilities of each asset
- Assess each risk's potential impact

# Risk Assessment Methodologies

**Vulnerability-based**

- Expands the scope of risk assessment beyond an organization's assets
- Examination of the known weaknesses and deficiencies within organizational systems
- Identify possible threats and consequences

**Threat-based**

- Evaluate the conditions that create risk
- Look beyond physical infrastructure
- Includes an asset audit

# Risk Types

# Types of Risk

- **Compliance Risk** – occurs when a party to a transaction fails to comply, either knowingly or inadvertently, with payment system rules and policies, regulations and applicable US and state law
- **Counterparty Risk** – risk to each party of a contract that the counterparty will not live up to its contractual obligation
- **Credit Risk** – risk that a party to a transaction will not be able to provide the necessary funds, as contracted, for settlement to take place on the scheduled date
- **Cross-Channel Risk** – occurs when the movement of fraudulent or illegal payment transactions from one payments channel to another is met with inconsistent risk management practices and lack of information sharing across payment channels about fraud
- **Direct Access Risk** – a situation in which an Originator, Third-Party Sender or Third-Party Service Provider transmits ACH files directly to an ACH Operator using the ODFI's routing number and settlement account
  - *Specific to the ACH Network*

# Types of Risk

- **Fraud Risk** – occurs when a payment transaction is initiated or altered by any party to the transaction in an attempt to misdirect or misappropriate funds with fraudulent intent
- **Legal Risk** – occurs from an institution's failure to enact appropriate policies, procedures or controls to ensure it conforms to laws, regulations, contractual agreements and other legally binding agreements and requirements
- **Liquidity Risk** – involves the possibility that earnings or capital will be negatively affected by an institution's inability to meet its obligations when they come due
- **Operational Risk** – occurs when a transaction is altered or delayed due to an unintentional error
- **Reputation Risk** – occurs when negative publicity regarding an institution's business practices leads to a loss of revenue to litigation

# Types of Risk

- **Strategic Risk** – associated with the financial institution's mission and future business plans
- **Systemic Risk** – occurs when a funds transfer system participant is unable to settle its commitments, causing other participants to fail
- **Third-Party Risk** – use of third parties reduces management's direct control of activities and may introduce new or increased existing risk, specifically, operational, compliance, reputation, strategic and credit risks and the interrelationship of these risks
- **Transaction Risk** – the exchange rate risk associated with the time delay between entering into a contract and settling it.
- **Transit Risk** – risk of not successfully moving the payment between buyer and seller, or having the payment altered in some way during the transit process.

# Areas/Activities to be Assessed

# Areas/Activities to be Assessed

- Scope of the ACH program
- Management or Board oversight
- ACH audit
- Third-Party service providers
- Information security
- ACH Operations
- Staff training
- ACH receipt
- ACH originations
- High-risk activities
- Third-party senders
- Direct access to the Operator
- Regulations and laws
- Business continuity
- Emerging payment systems

# Questions

AAP™
Accredited
ACH Professional

APRP™
Accredited Payments
Risk Professional

# Continuing Education Credits

**Possible or Probable?**
**How to Assess the Risk**

**October 2023**

This session is worth 1.8 credits

(keep this slide for your records)