

# The Building Blocks of an Effective Risk Management Program Jenga Style

Nanci McKenzie, Juris Masters  
Financial Regulation &  
Compliance, AAP, APRP  
Federal Reserve Bank of  
Atlanta  
Payments Expert



Federal Reserve  
Bank *of* Atlanta

The views expressed here are of the presenter's and may not reflect the views of the Federal Reserve Bank of Atlanta or Federal Reserve System.

# About The Speaker



**Nanci McKenzie JM, AAP, APRP**

Payments Expert  
Research Division  
Federal Reserve Bank of Atlanta

[Nanci.mckenzie@atl.frb.org](mailto:Nanci.mckenzie@atl.frb.org)

[Nanci McKenzie | LinkedIn](#)



# Key Take A-ways

- Why is a Risk Management Program Important?
- What controls are included in a solid and stable risk management program?
- Who are great resources for risk management direction?
- How many Inherent Risks does it take to make the Risk Management Tower (JENGA) fall?

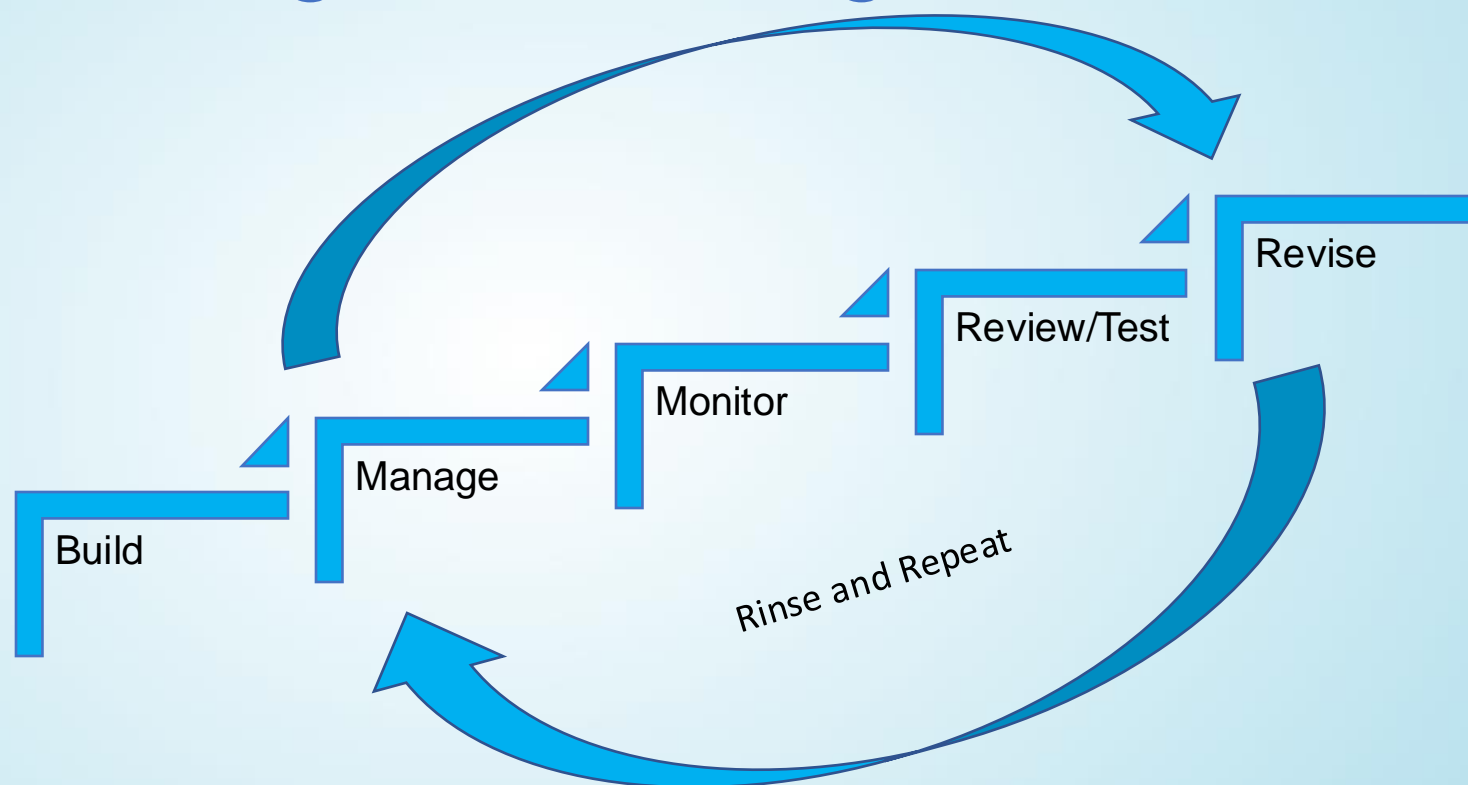
# Definition of JENGA



Copilot

The word “**Jenga**” is derived from the **Swahili** word “**kujenga**”, which means “**to build**”. In the **Jenga** game, players construct a tower using wooden blocks (known as **Jenga blocks**). The objective is to remove one block at a time from the tower and place it on top, creating a progressively more unstable structure. The name perfectly captures the essence of the game—building and balancing!

# Risk Management Program





A large group of skydivers are captured in mid-fall against a clear, bright blue sky. The divers are scattered across the frame, with a dense cluster in the center and others more sparsely distributed towards the edges. They are wearing a variety of colorful jumpsuits in shades of red, blue, yellow, green, and black. Their poses are dynamic and varied, with arms and legs extended in different directions, suggesting a sense of movement and freedom. The overall composition is vibrant and energetic.

# It's All About Risk Management

# Data Data Everywhere



- Core
- Online Banking
- Fraud Detection Program
- Archive – Cold Storage
- OFAC Screening Program
- Loan Processing Platform
- FedLine – Federal Reserve or EPN
- Accounts Payable Platform
- Credit Card Processing Platform
- ATM Processing Platform
- Cash Management Platform
- IT/Network Folders
- Wire Transfer Program
- Remote Deposit Capture (RDC) Program
- Mobile Program
- Zelle
- Correspondent Bank/CU
- Etc. Etc. Etc.





# Organizing Your Data

## Get it in one place



# Why is Risk Management so Important?

Effective: June 6, 2023

[The Fed - Interagency Guidance on Third-Party Relationships: Risk Management \(federalreserve.gov\)](https://www.federalreserve.gov/interagencyguidance/interagencyguidance.htm)

**FEDERAL RESERVE SYSTEM**  
[Docket No. OP-1752]

**FEDERAL DEPOSIT INSURANCE CORPORATION**  
RIN 3064-ZA26

**DEPARTMENT OF THE TREASURY**  
Office of the Comptroller of the Currency  
[Docket ID OCC-2021-0011]

**Interagency Guidance on Third-Party Relationships: Risk Management**

**AGENCY:** The Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC), Treasury.

**ACTION:** Final interagency guidance.

**SUMMARY:** The Board, FDIC, and OCC (collectively, the agencies) are issuing final guidance on managing risks associated with third-party relationships. The final guidance offers the agencies' views on sound risk management principles for banking organizations when developing and implementing risk management practices for all

# Stages of the Risk Management Life Cycle

## Risk Management

### Third-Party Relationship Life Cycle

1. Planning
2. Due Diligence and Third-Party Selection
3. Contract Negotiation
4. Ongoing Monitoring
5. Termination

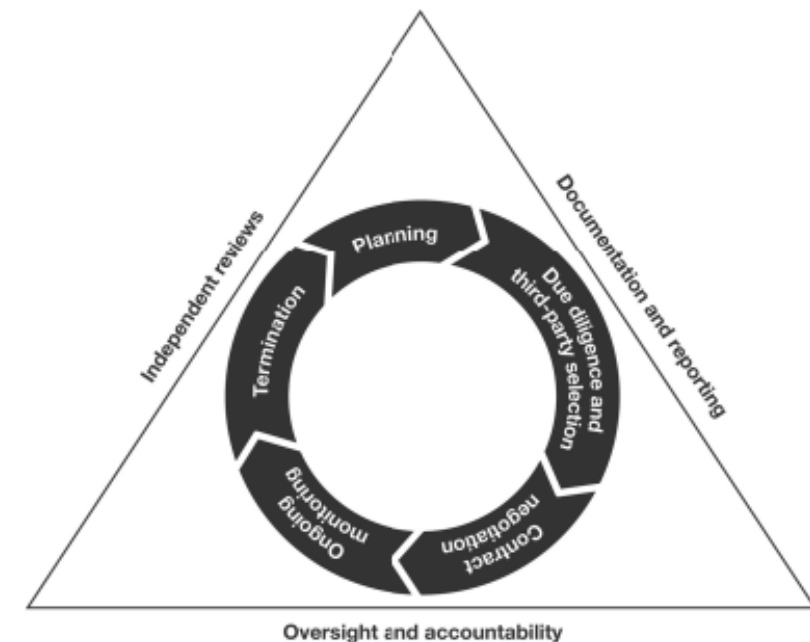
## Governance

1. Oversight and Accountability
2. Independent Reviews
3. Documentation and Reporting

## Supervisory Reviews of Third-Party Relationships

Pgs. 4-23

**Figure 1: Stages of the Risk Management Life Cycle**





- Third-Party Relationships: Interagency Guidance on Risk Management | OCC
    - Third-Party Relationships: Risk Management Guidance | OCC
    - Third-Party Relationships: Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks | OCC
    - Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29 | OCC
    - Automated Clearing House Activities: Risk Management Guidance | OCC
- OCC Guidance Pg. 4



# Third-Party Relationship: Risk Management

A banking organization's use of third parties does not diminish its responsibility to meet these requirements to the same extent as if its activities were performed by the banking organization in-house. To operate in a **safe and sound manner**, a banking organization establishes risk management practices to effectively manage the risks arising from its activities, including from third-party relationships.<sup>5</sup>

<sup>5</sup>This guidance is relevant for all third-party relationships, including situations in which a supervised banking organization provides services to another supervised banking organization.

Pgs. 2-3 (Emphasis added)







# What is a Third-Party Relationship?

This guidance addresses any business arrangement between a banking organization and another entity, by contract or otherwise. A third-party relationship may exist **despite a lack of a contract or remuneration**. Third-party relationships can include, **but are not limited to**, outsourced services, use of independent consultants, referral arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, and joint ventures. Pg. 2 (Emphasis added)

# What is a Third-Party Relationship?

Some banking organizations may form third-party relationships with new or novel structures and features – such as those observed in relationships with some financial technology (**fintech**) companies. The respective roles and responsibilities of a banking organization and a third party may differ, based on the specific circumstances of the relationship. Where the third-party relationship involves the *provision of products or services to*, or other interaction with, **customers**, the banking organization and the third party may have varying degrees of interaction with those customers.

Pg. 3 (Emphasis added)



# Risk Management & Risk Assessments

Not all relationships present the same level of risk, and therefore not all relationships require the same level or type of oversight or risk management. As part of sound risk management, a banking organization analyzes the risks associated with each third-party relationship and tailors risk management practices, commensurate with the banking organization's size, complexity, and risk profile and with the nature of the third-party relationship. Maintaining a complete inventory of its third-party relationships and periodically conducting **risk assessments** for each third-party relationship supports a banking organization's determination of whether risks have changed over time and to update risk management practices accordingly.

Pg. 2-3 (Emphasis added)





# Oversight and Accountability



Proper oversight and accountability are important aspects of third-party risk management because they help enable a banking organization to minimize adverse financial, operational, or other consequences. A banking organization's **board of directors has ultimate responsibility for providing oversight for third-party risk management and holding management accountable.** The board also provides clear guidance regarding acceptable risk appetite, approves appropriate policies, and ensures that appropriate procedures and practices have been established. A banking organization's management is responsible for developing and implementing third-party risk management policies, procedures, and practices, commensurate with the banking organization's risk appetite and the level of risk and complexity of its third-party relationships.

Pgs. 20 (Emphasis added)



# Performance Measures and Benchmarks



## *b. Performance Measures or Benchmarks*

For certain relationships, **clearly defined performance measures can assist a banking organization in evaluating the performance of a third party**. In particular, a service-level agreement between the banking organization and the third party can help specify the measures surrounding the expectations and responsibilities for both parties, including conformance with policies and procedures and compliance with applicable laws and regulations. Such measures can be used to monitor performance, penalize poor performance, or reward outstanding performance. It is important to negotiate performance measures that do not incentivize imprudent performance or behavior, such as encouraging processing volume or speed without regard for accuracy, compliance requirements, or adverse effects on the banking organization or customers.

Pg. 12 (Emphasis added)

# Supervisory Reviews of Third-Party Relationships

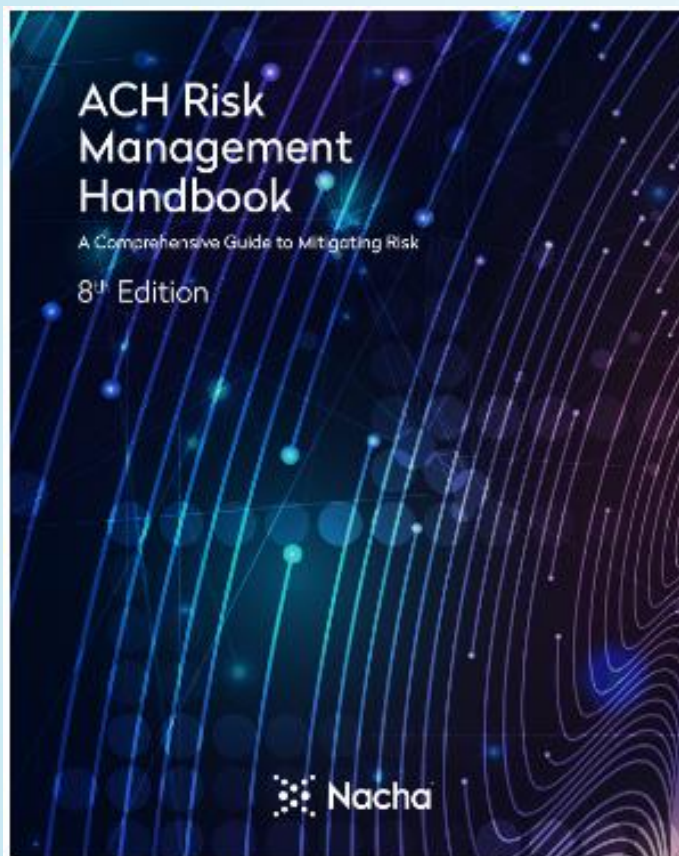


***Each agency will review its supervised banking organizations' risk management of third-party relationships as part of its standard supervisory processes.***

*Page 23 (Emphasis added )*



# ACH Risk Management Framework



[Risk Management | NACHA](https://www.nacha.org/content/risk-management)  
<https://www.nacha.org/content/risk-management>





---

# NOTICE OF AMENDMENT TO THE 2024 NACHA OPERATING RULES

April 12, 2024  
SUPPLEMENT #1-2024



# 2024 ACH Risk Management Rules

- **Fraud monitoring** by all parties in ACH except consumers
  - ODFIs, Originators, Third-Parties
  - RDFI **monitoring** of inbound ACH credits
- Effective March 20, 2026
  - **Fraud monitoring** (by ODFIs)
  - **Fraud monitoring** (by [non-consumer] Originators, TPSPs, and TPSs w/ 2023 ACH origination volume 6 Million or >)
  - ACH credit **monitoring** by RDFIs > 10 million received in 2023
  - [Nacha Operating Rules - New Rules | Nacha](#)

# 2024 ACH Risk Management Rules

- Effective June 22, 2026
  - **Fraud monitoring** (by all other non-consumer Originators, TPSP, and TPS)
  - ACH credit **monitoring** by all RDFIs
  - [Nacha Operating Rules - New Rules | Nacha](#)

👉👉👉 **THIS! In both these Rules** 👉👉👉

- “(b) at least annually review such processes and procedures and make appropriate updates to address evolving risks.”

# Guidance From Nacha on What to Look For



- [RMAG Guidance on Credit-Push Fraud Response Checklists for Originators](#)
- [RMAG: Preventing and Recovering from Operational Errors and Accidents](#)
- [A Checklist Approach to Reduce Fraud in Payroll Origination](#)
- [RMAG Guidance on RDFI Credit-Push Fraud Response Checklists | Nacha](#)
- [RMAG Guidance on ODFI Credit-Push Fraud Response Checklists | Nacha](#)
- [RMAG Meets to Begin Implementation of New Risk Management Framework | Nacha](#)

# Transaction Monitoring

What are we monitoring for?

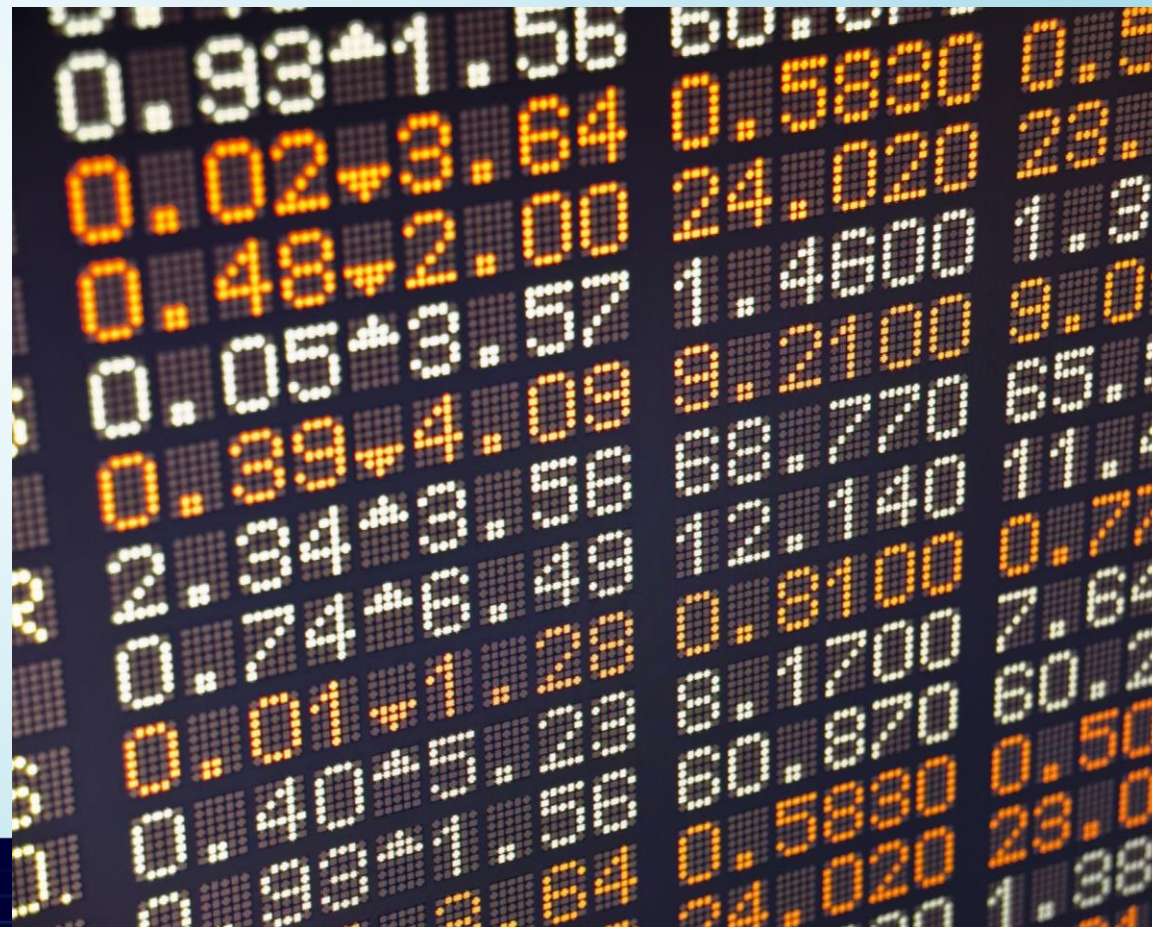
- Suspicious activity
- Fraud
- Financial crimes





# Fraud Detection System vs. Fraud Monitoring System

- Fraud Detection identifies fraudulent attempts in real-time or shortly after the fact
  - OFAC screening
  - Anti-Money Laundering Act monitoring
  - Unauthorized transactions
  - Channel specific (credit cards, ACH, wires, etc.)
- Fraud Monitoring continuous session monitoring across channels and devices
  - Customer/member activity as a whole
  - On customer/member themselves and their behavior





# Let's LOOK at BSA/AML Monitoring



Adobe Firefly

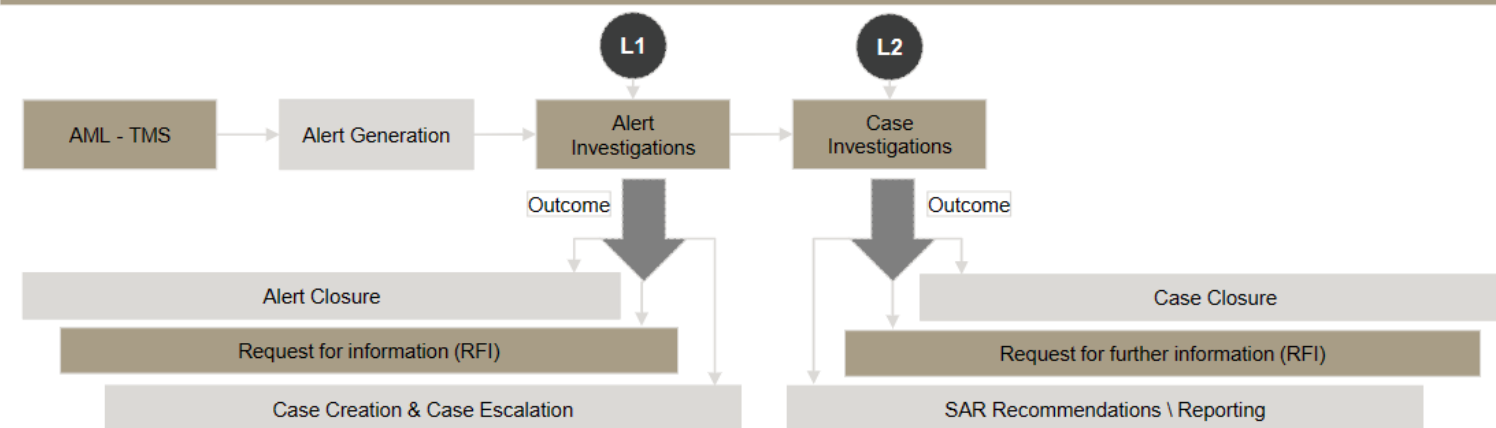
# Bank Secrecy Act (BSA) Anti-Money Laundering (AML)

- Monitoring
  - Alert Investigations
  - Case Investigations

## Client Requirement

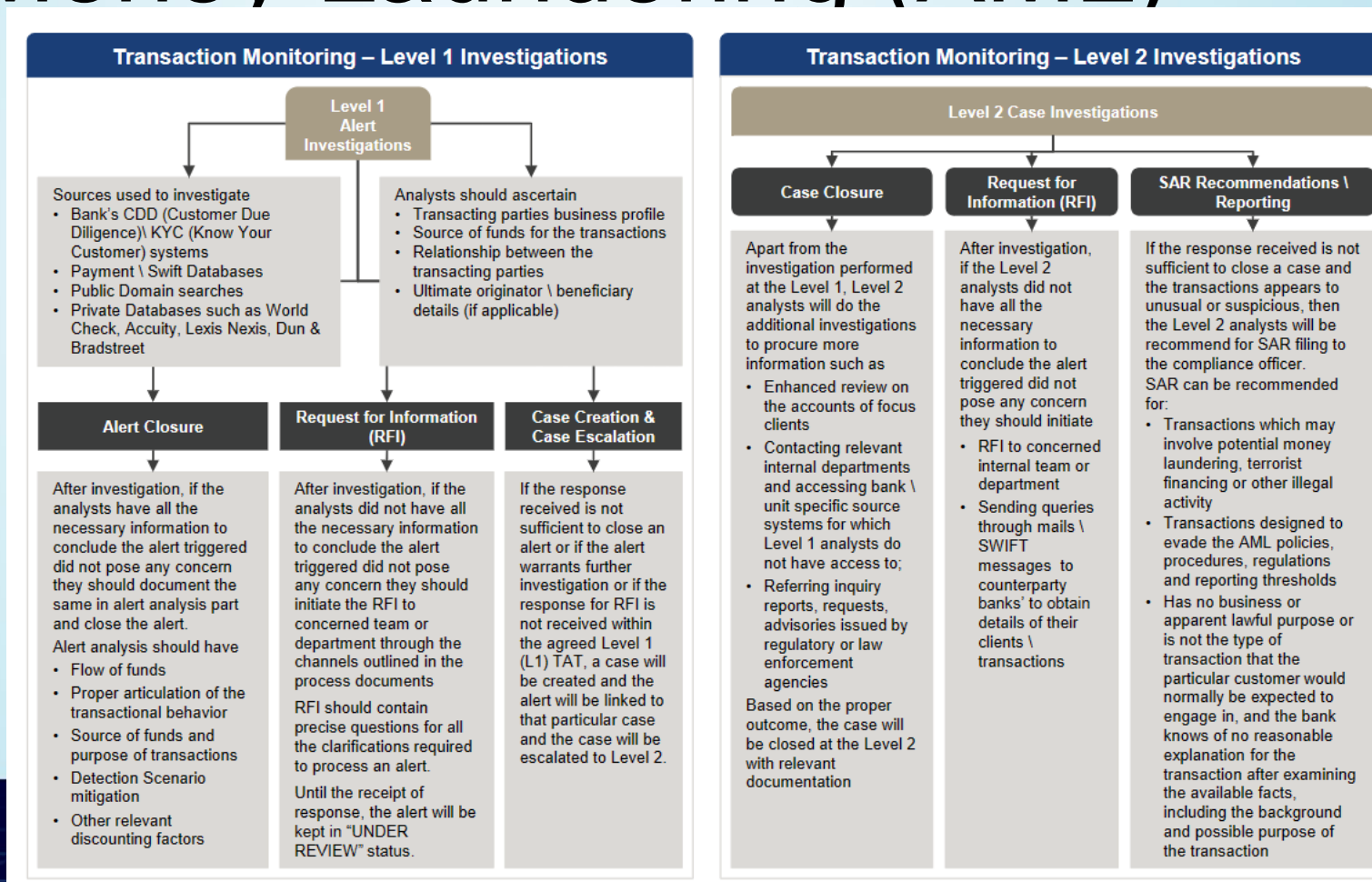
- Reviewing the alerts triggered by the Anti-Money Laundering - Transaction Monitoring system (AML-TMS) to detect potentially unusual or suspicious pattern of transactions
- Suspicious Activity Report (SAR) reporting of suspicious cases for regulatory purpose.
- Identifying the scenarios which are resulting in more false positives and to identify the processes which can be automated effectively
- 100% quality within the Turn Around Time (TAT) \ Service Level Agreement (SLA) with effective closure & potential escalations.

## Approach & Execution





# Bank Secrecy Act (BSA) Anti-Money Laundering (AML)



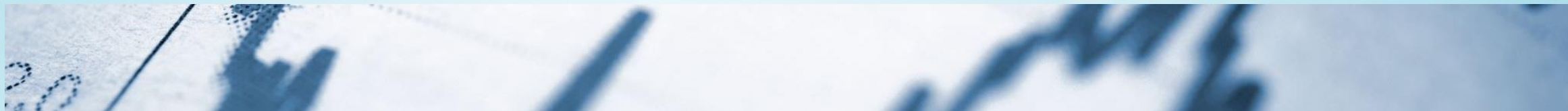
© 2017 CRISIL Ltd. All rights reserved.

# Data is Telling Us What?



- RDFI's
  - Is it normal for the customer/member to get this type of credit?
  - Is the \$\$\$ and frequency unusual for the customer/member?
  - Is the money being moved out of the account quickly using an app or wire?
  - Is the IP address typical for customer/member using online banking?
  - Is the velocity of deposit and withdrawals unusual for customer/member?
  - Is the name on the entry different than on the account?
  - Is the account a new (or newer) account opened by online options?
  - Has the customer/member been claiming unauthorized transactions often?
  - Has there been any red flags while speaking with customer/member in-person, on the phone, live chat, email, etc.?

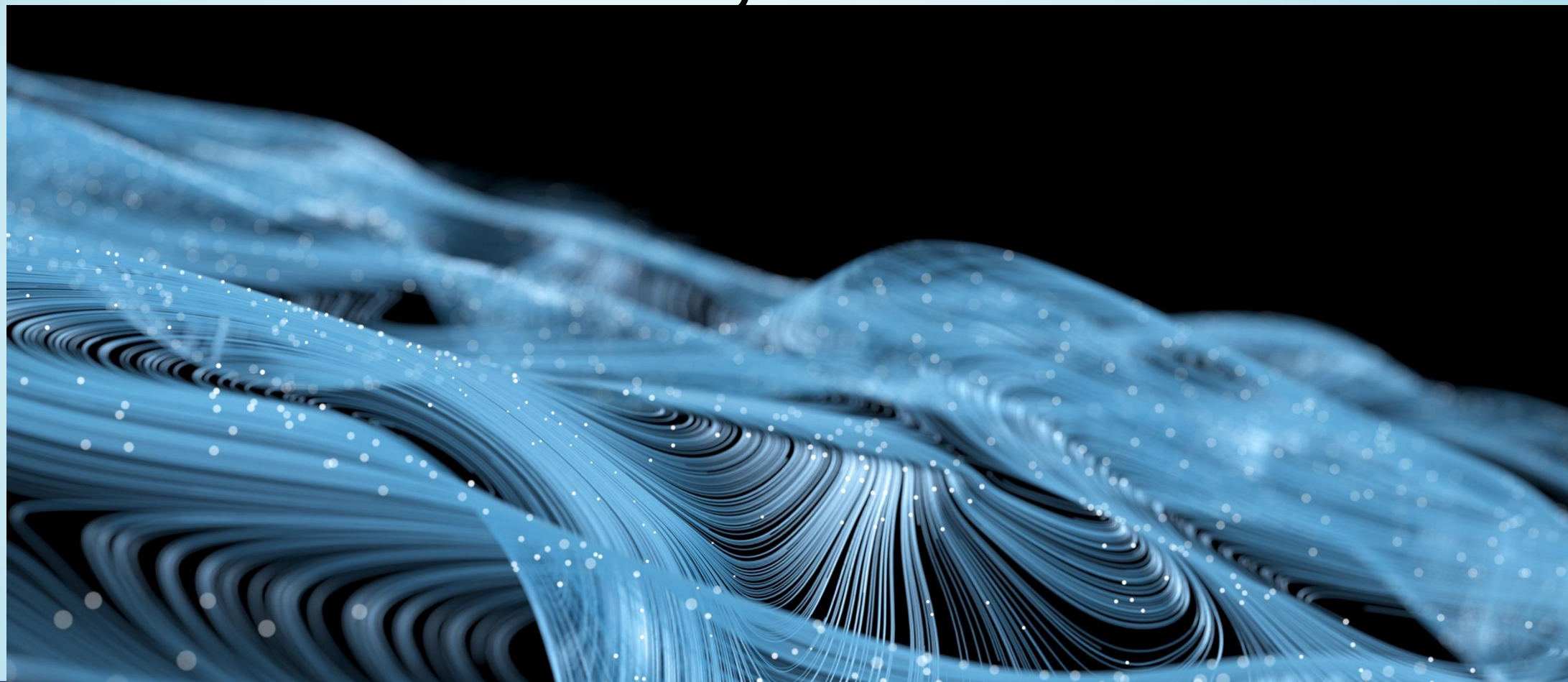
# Data is Telling Us What?



- ODFI's/Originators
  - Is it normal for Originator to send credits?
  - Is the \$\$\$ and frequency unusual for the Originator?
  - Are you getting contacted to allow credit returns for certain Originators?
  - Are the POA names different than unauthorized claims received from RDFI?
  - Have the \$\$\$ of entries/files increased?
  - Are the entries in a batch/file all going to the same routing number?
  - Do the entries have Company Entry Description that would lead you to believe they have changed their business line? (ie. Cannabis or crypto)
  - Do you have a TPS/TPPP that has a new Originator that you were not made aware of?



# Consider: Data Analytics



# Why is a Risk Management Program so Important?

- Federal Financial Institution Examination Council (FFIEC) – Interagency Guidance on Risk Management (OCC, FDIC, FRB, NCUA, CFPB & State)
  - [FFIEC Home Page](#)



FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL

*Promoting uniformity and consistency in the supervision of financial institutions*

**Ask a Question**  
Get answers from experts





- **SafeGuarding Rule** - Revisions approved by FTC as part of the Gramm-Leach Bliley Act (GLBA) December 9, 2021
  - Effective June 9, 2023 (Information Security Program)
  - Last prior change was 2016
  - Newest approval of Safeguards Rule November 13, 2023 effective May 13, 2024 (FIs requirement to report to the FTC events where unencrypted customer information of 500+ consumers)
- [Federal Register :: Standards for Safeguarding Customer Information – Effective May 13, 2024](#)
- [Federal Register :: Standards for Safeguarding Customer Information – Effective June 9, 2023](#)
- [FTC Safeguards Rule: What Your Business Needs to Know | Federal Trade Commission](#)

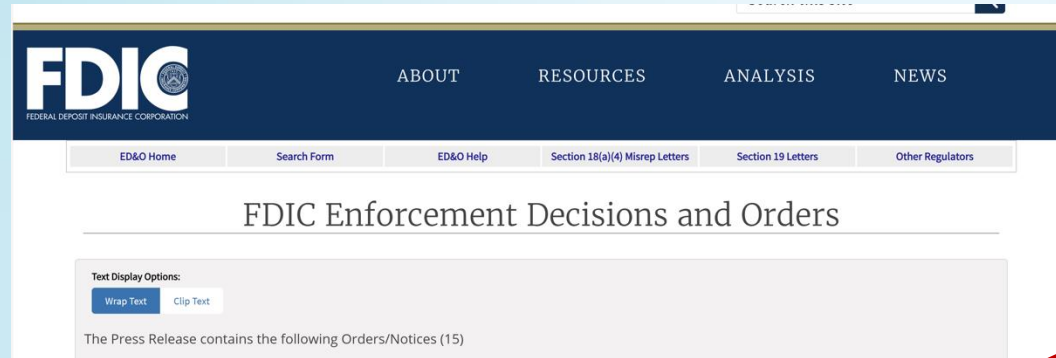


# SafeGuards Rule



- Places additional requirements on financial institutions which now include **third parties**:
  - **Appointing a Qualified Employee for Oversight**
  - **Conduct a Risk Assessment**
  - **Periodic Review Access Controls**
  - **Data and Systems Inventory.**
  - **Encryption of all customer information in transit and at rest**
  - **Assess Apps**
  - **Multi-Factor Authentication**
  - **Secure data disposal**
  - **Change Management**
  - **Intrusion Detection**
  - **Training of Staff on the Information Security Program**
  - **Incident Response Plan**
  - **Qualified Individual Report to the Board of Directors**

# Why is a Risk Management Program so Important?



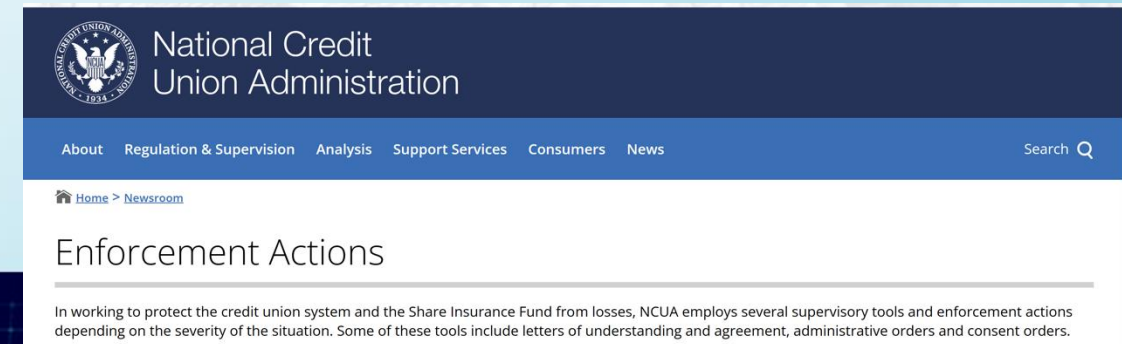
[FDIC: Enforcement Decisions and Orders - Press Release Orders](#)



[OCC Announces Enforcement Actions for February 2024 | OCC](#)

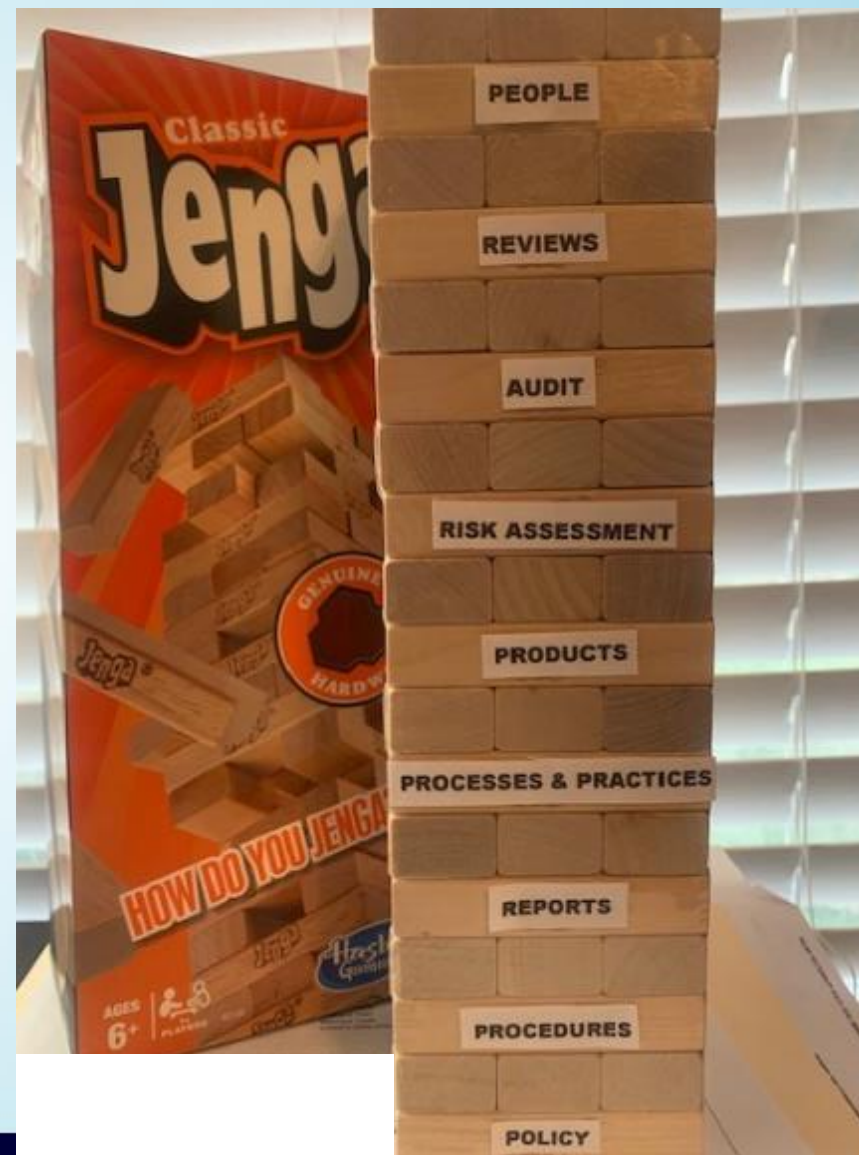


[The Fed - Enforcement Actions \(federalreserve.gov\)](#)



# JENGA Style

Let's Build a Risk  
Management  
Program!





# Risk Management Program Controls

Policy

Procedures

Reports

Processes & Practices

Products

Risk Assessment

Audit

Reviews

People




# Risk Management Program Controls

- People
  - Training/Education
  - Dispensable
  - Experience





# Risk Management Program Controls

- Reviews
    - Vendor Risk Management
    - Corporate Customer Risk Review
    - Security and Data Risk Reviews
- 




# What's the Difference?



- Self Assessment = Looking at one self
- Risk Review = Corporate Customer due diligence review
- Risk Assessment = Risk identification of risk environment and determination of effective controls to mitigate those risks




# Risk Management Program Controls

- Processes & Practices
    - Culture of Compliance
    - Routine/Schedule
    - Connected P & Ps
- 




# Risk Management Program Controls

- Risk Assessment
    - Identify Inherent Risks
    - Performed Repeatedly Based on Level of Risk
    - Assess Effectiveness of Controls
- 






# Risk Management Program Controls

- Audit
    - Test Controls - Operating as Intended
    - Compliance
    - Necessary Remediation of Control
- 




# Risk Management Program Controls

- Reports
    - Tell Your Story
    - At-A-Glance Control Effectiveness
    - Stay Informed
- 




# Risk Management Program Controls

- Procedures
    - All Inclusive of Activities
    - “How” from “What” Policy Stated
    - Reviewed (Periodically or shift in environment)
- 





# Risk Management Program Controls

- Policy
    - Identify Risks
    - Approved by BOD (Annually or a shift of environment)
    - “What” to Mitigate Risks
- 

# Thank You!



Federal Reserve  
Bank of Atlanta

**Nanci McKenzie, Juris Masters Financial  
Regulation & Compliance, AAP, APRP  
Payments Expert**

[Nanci.mckenzie@atl.frb.org](mailto:Nanci.mckenzie@atl.frb.org)



Federal Reserve  
Bank *of* Atlanta



# Connect with us @Atlanta Fed

---



Federal Reserve  
Bank of Atlanta

# Inherent Risks

- Security incident happens with one of your third parties
- Pandemic – CDC Health warnings
- Staff exodus
- Audit or examination findings
- Lack of BCP testing
- Fraudulent ACH file transmitted
- Ransomware attack
- Email compromise
- Fraudulent wire transfer sent
- Account Takeover of customer
- Lack of BOD education of risks
- ACH Audit not completed by Dec 31
- Customer Reviews not completed based on risk rating
- Policies are not reviewed and approved by the Board
- Security patches not applied
- No risk assessment completed
- Remediation of findings are not completed
- Lack of Leadership support
- Poor site of emerging risks – It's not just about the past! Use AI to determine future risks
- Failure to prioritize risks
- Ineffective communication – Internally and externally
- Not testing program – lack/ineffective/inconsistent of audits
- Lack of Risk Assessments
- Inadequate resources – no budget, lack of bodies, lack of solutions
- Checklist of compliance and of considering of risks (culture of compliance is important but risks are out of the box thinking)