Risky Business Basics

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

Macha PAYMENTS UNIVERSITY

Risk Management

The total process required to identify, control and minimize the impact of uncertain events

Macha
PAYMENTS UNIVERSITY

Risk Management

Identify

- Risk Assessment

Measure

- Risk Analysis or Evaluation

Mitigate

- Implement controls

Monitor

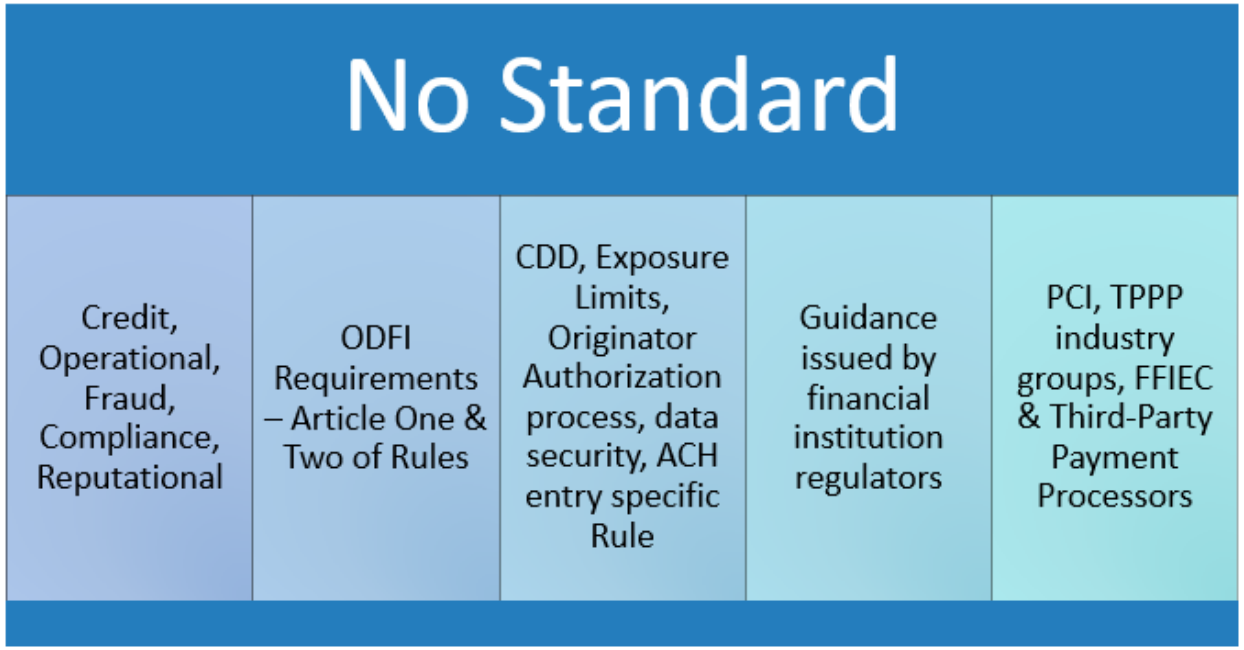
- Tracking and reporting

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

- Should include a review of broad risk topics
- Frequency is typically annually unless something changes
  - New product/service
  - Merger/acquisition
  - Geographic expansion
  - New business line



Macha PAYMENTS UNIVERSITY

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

Types of Risk

Macha
EVERYTHING PAYMENTS - EVERYWHERE
PAYMENTS UNIVERSITY

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.

Primary Risks and Controls

What is a Control?

- A process designed to provide assurance regarding the achievement of objectives relating to operations, reporting and compliance
- Policies, procedures or other safeguards put into place to reduce the amount of risk posed to your institution
- Controls reduce risk and help ensure management's directives to mitigate risk

Procedures

- All payment activities should have written procedures
- Procedures should include, in detail:
- Who is responsible
  - Primary and secondary
- What needs to be done
- Applications
- Where the information can be found
  - i.e. name or reports
- Timeframe for completion
  - Time of day, frequency, deadlines

Origination Agreement - Requirements

- Authorize the ODFI to originate entries
- Bind Originator to the Rules
- No entries that violate US law
- Restrictions on types of entries that can be originated
- Right of the ODFI to suspend or terminate agreement
- Right of the ODFI to audit the Originator's compliance with the Rules

- Restrictions on Nested Third-Party Senders
- TPS will enter into an agreement with all Originators and Nested TPS
- Nested TPS will enter an agreement with all Originators

- Exposure limits*
- Risk Assessments*

ACH Origination Agreement

- Agreements should also include:
  - Risk management requirements
  - Security requirements
  - Assumption/allocation of risk
  - Assumption/allocation of loss
  - Processing requirements/Schedule
  - Settlement

Macha PAYMENTS UNIVERSITY

Compliance 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.

Macha PAYMENTS UNIVERSITY

Compliance Risk

- Compliance is comprised of the actions taken by a financial institution to comply with payment system rules and policies, regulation and applicable US and state law.
- Examples of compliance risk:
  - Failure to comply with the ACH Rules
  - Failure to follow proper error resolution, as required by Regulation E
  - Failure to comply with customer due diligence, as required by BSA

Compliance Risk – Legal Framework

- Private Sector Rules
  - Nacha
  - ECCHO
  - RTP
  - FRB Operating Circulars
  - SWIFT
- Regulations (i.e., CC, D, E, J, P, Z)
- UDAAP
- Uniform Commercial Code
- BSA
- USA PATRIOT Act
- OFAC
- Code of Federal Regulations

Macha PAYMENTS UNIVERSITY

Compliance Risk - Controls

- Ensure the institution maintains compliance with all applicable U.S. laws, regulations and rules
- Implement strong internal policies and procedures
- Comprehensive and continuing staff training
- Control Self-Assessments
- Annual Rules compliance audit
- ACH Origination Agreements

Compliance Risk - Controls

- Accredited payments professionals on staff
  - **AAP** - Accredited ACH Professional (Nacha)
  - **APRP** - Accredited Payments Risk Professional (Nacha)
  - **NCP** – National Check Payments Certification (ECCHO)
  - **CTP** – Certified Treasury Professional (Association for Financial Professionals)
  - **CAFP** – Certified AML and Fraud Professional (ABA)
  - **CERP** – Certified Enterprise Risk Professional (ABA)
  - **CRCM** – Certified Regulatory Compliance Manager (ABA)

Macha PAYMENTS UNIVERSITY

Credit Risk

Credit Risk is the 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.

Macha PAYMENTS UNIVERSITY

Credit Risk - ACH

- Credit Entries
  - Period of time between the initiation of an ACH credit file and when the company funds the account
  - Amount of risk based on total amount of the file
    - Up to 2 business days
- Debit Entries
  - Date funds available to originator until debits can no longer be returned by RDFI
    - 2 Banking days
    - Up to 60 calendar days from settlement
    - Unauthorized could be returned as ODFI warrants authorization
  - Amount of risk based on amount of returned ACH debit
- NOTE: Statute of Limitations – for most states the ODFI would still be liable for 7 years

Credit Risk - Controls

- Establish a Credit Policy
  - Clear, written guidelines that set the terms and conditions for supplying services on credit
- Conduct risk rating on Originators and Third-Party Senders
  - Assess the nature of the Originator's and Third-Party Sender's activity and the risk it represents
- Conduct credit analysis to determine creditworthiness of Originators and Third-Party Senders
- Establish, implement, and periodically review exposure limits
  - Exposure limits should reflect risk rating, creditworthiness, activity and anticipated volume
  - Establish procedures for over-limit situations
- Pre-funding of credit files
- ACH Origination Agreement
- Monitor origination and return volume across multiple settlement date

Fraud Risk

Fraud Risk occurs when a payment transaction is initiated or altered by any party to the transaction (i.e., employees, interlopers or organizations) in an attempt to misdirect or misappropriate funds with fraudulent intent.

Macha PAYMENTS UNIVERSITY

Fraud Risk

- Fraud risk is affected by internal and external factors.
- Examples of fraud risk:
  - Misappropriation of funds
  - Misdirected payment
  - Account compromise/takeover
  - Business email compromise
  - Vendor impersonation

Macha PAYMENTS UNIVERSITY

Who commits fraud?

- Dissatisfied, disgruntled, desperate or dishonest employees
- Interlopers
- Hackers
- Fraudsters
- Dishonest or unscrupulous vendors
- Dishonest or unscrupulous Originators or Receivers

Fraud Risk - Controls

- Data security
- Audit Trail
- Staff and consumer education
- Dual control
- Physical access controls
- Privilege based user access controls
  - System access should be aligned with job function
- Segregation of duties
- Anomalous activity/Fraud detection
- Multi-factor authentication
- ACH Origination Agreement
- Change Management
- Out of band verification
- KYC and KYCC

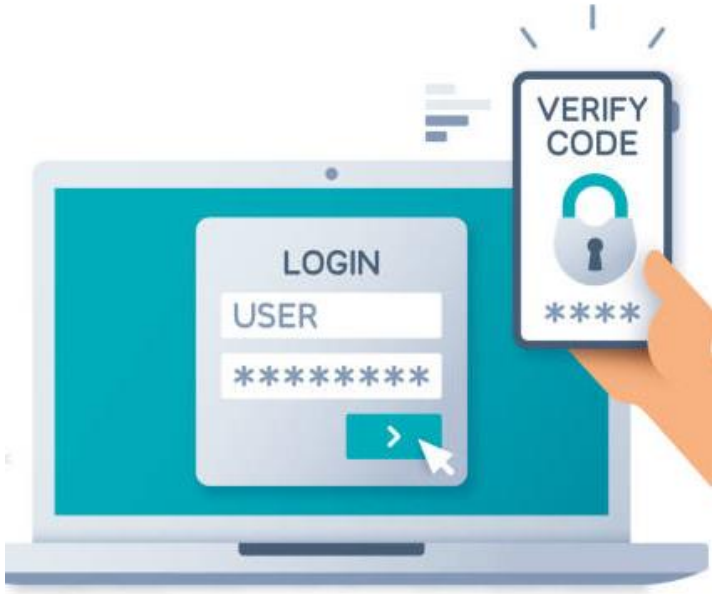
Uniform Commercial Code 4A

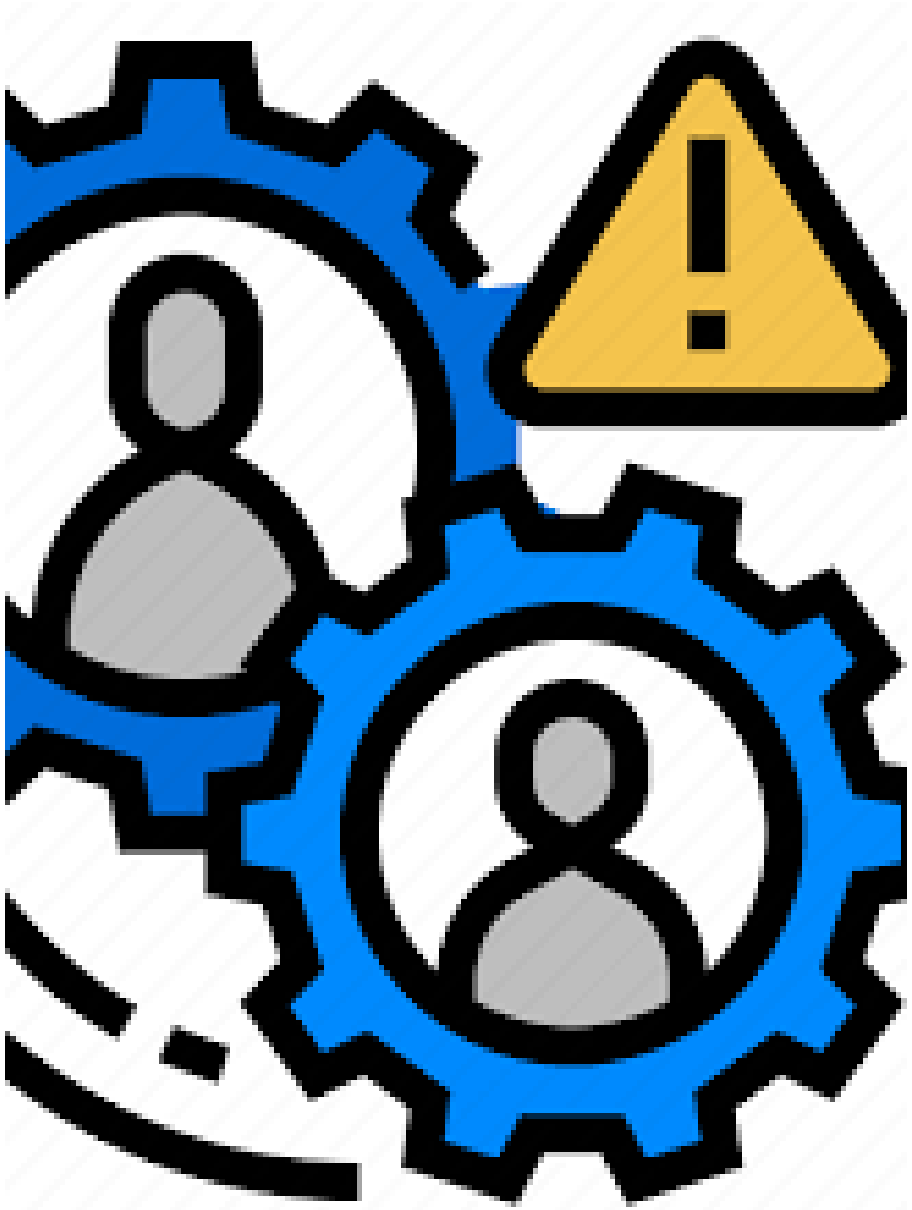
- Commercial reasonableness of a security procedure is determined by:
  - Considering the wishes of the accountholder expressed to the FI
  - The circumstances of the customer known to the FI
  - Alternative security procedures offered to the accountholder
  - **Security procedures used by accountholders and FIs similarly situated**

acha
PAYMENTS UNIVERSITY

Multi-Factor Authentication

- Multi-Factor Authentication uses a combination of two or more authentication factors
- Multi-Factor Authentication considered ‘commercially reasonable” for verifying identity in electronic access
- Three Authentication Factors:
  - Something the user knows
    - Password, PIN
  - Something the user has
    - Token, mobile device
  - Something the user is
    - Biometric characteristic





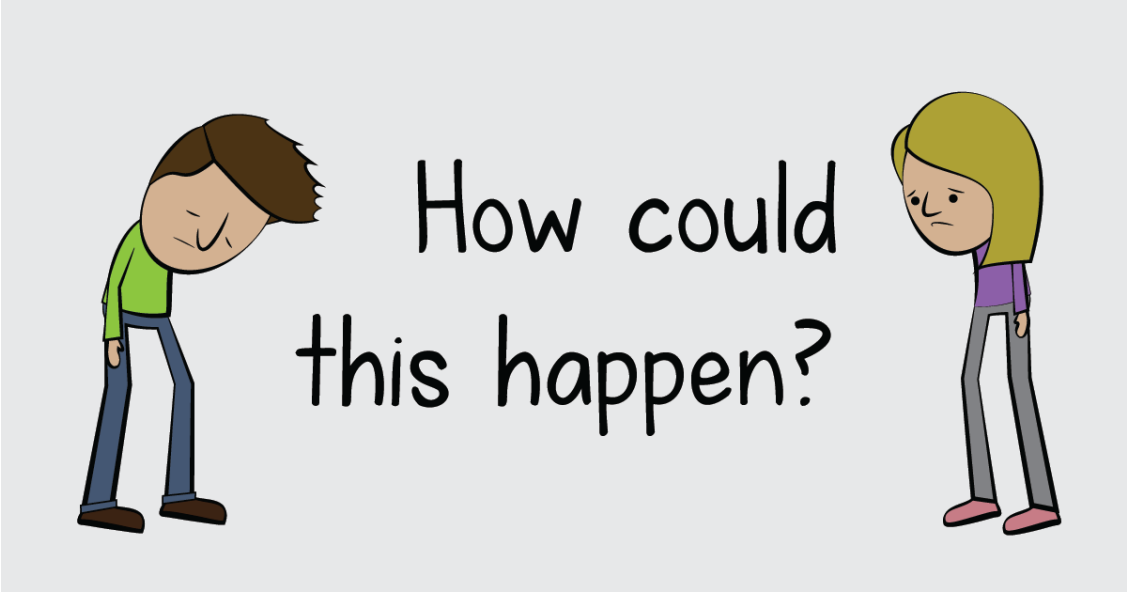
Operational Risk

Operational Risk occurs when a transaction is altered or delayed due to an unintended error. (i.e. clerical error, hardware and/or software failure)

Macha
PAYMENTS UNIVERSITY

Operational Risk

- Operational risk can result from:
  - Technology failures
  - Power failure
  - Human error
  - Staffing problems
  - Natural disasters
  - Inadequate procedures
  - Inadequate training



Macha PAYMENTS UNIVERSITY

Operational Risk - Controls

- Separation of duties
- Maintain systems – update and patch software appropriately
- Problem resolution procedures
- Physical security
- Strong policies and procedures
- Adequate and continuing training program
- Cross-training
- Audit program
- BCP Plans – develop and test disaster recovery plans

Secondary Risks and Controls

Legal Risk

Legal Risk occurs from an institution's failure to enact appropriate policies, procedures or controls to ensure it conforms to laws, regulations, contractual arrangements and other legally binding agreements and requirements.

Macha PAYMENTS UNIVERSITY

Legal Risk – Controls

- Review contractual relationships to ensure they are sound and appropriate and allocate risk sharing responsibilities
- Appropriate controls to ensure primary risk mitigation

Reputation Risk

Reputation Risk occurs when negative publicity regarding an institution's business practices leads to a loss of revenue or litigation.

Reputation Risk

- For retail payment-related systems, reputation risk is linked to consumer expectations regarding the delivery of retail payment services, and the institution's ability to meet its regulatory and consumer protection obligations related to those services.
- Errors or fraud can have serious impacts to the public opinion of a Financial Institution.

Reputation Risk - Controls

- Effective public relations program
- Internal controls to prevent errors
- Appropriate controls to ensure primary risk mitigation

Third-Party Risk

Use of third parties reduces management's direct control of activities and may introduce new or increased existing risks, specifically, operational, compliance, reputation, strategic, and credit risks and the interrelationship of these risks.

Third-Party Risk - Controls

- Vendor Management Program
  - Due diligence
  - Ongoing monitoring
- Third-Party agreements

Questions?

Macha
EVERYTHING PAYMENTS - EVERYWHERE
PAYMENTS UNIVERSITY