Vendor Management

Bryan Fury, MSISM, CISSP, CRISC

bfury@corporateone.coop

614-825-9378

Third Party Risk Foundations

- Third Party Risk Management Overview
- Governance
- Policy Management
- Compliance
- Contract Management
- Data – Types and Locations

Third Party Risk Foundations

- Moving past vendor management
- Scope too narrow
  - Not inclusive of all agreement types
  - Target hack
- Not risk-based
  - Decisioning made on wrong information

Defining Third Party

- A Third Party is defined as an entity or persons working on behalf of the organization but are not its employees.
  - Vendors
  - Consultants
  - Suppliers
  - 4th Parties

Scope

- Third parties that:
  - Access in any manner customer or company **confidential** data or have systems that interact with that data.
  - Represent significant risk to your organization's reputation.
  - Are a integral piece of your organization's strategic plan.
  - Could negatively impact your balance sheet.
  - Provide a unique service that would be difficult to replace.

Third Party Risk Management

- A process for identifying and managing risks created when hiring a third party to provide good or services.
- Usually focused on data security controls.
- Scope should depend on the nature of the agreement.

Emerging Vendor Risks

- Vendor relationships becoming more and more complicated.
- Popular target for cyber attacks.
- Vendors are increasingly targeted by criminals.
- Complex regulatory environment.

Laying the Ground Work

- Know your third parties
  - Who are your third party service providers?
  - What services do they provide?
  - What data/systems do they have access to?
- Most credit unions do not maintain a current, comprehensive list!

Vendor Risk Program

rateOne FEDERAL CREDIT UNION
It's where you belong.

Formalized Governance Structure

- Establish a formal governance model or organizational structure to manage third party risk
  - Define clear roles and responsibilities
  - Create a risk management framework to focus approach
  - Scale your structure based on risk profile
    - Identify emerging risks that affect your program
    - Determine frequency of reviews
    - Identify the level of formality needed
    - Identify key processes in scope

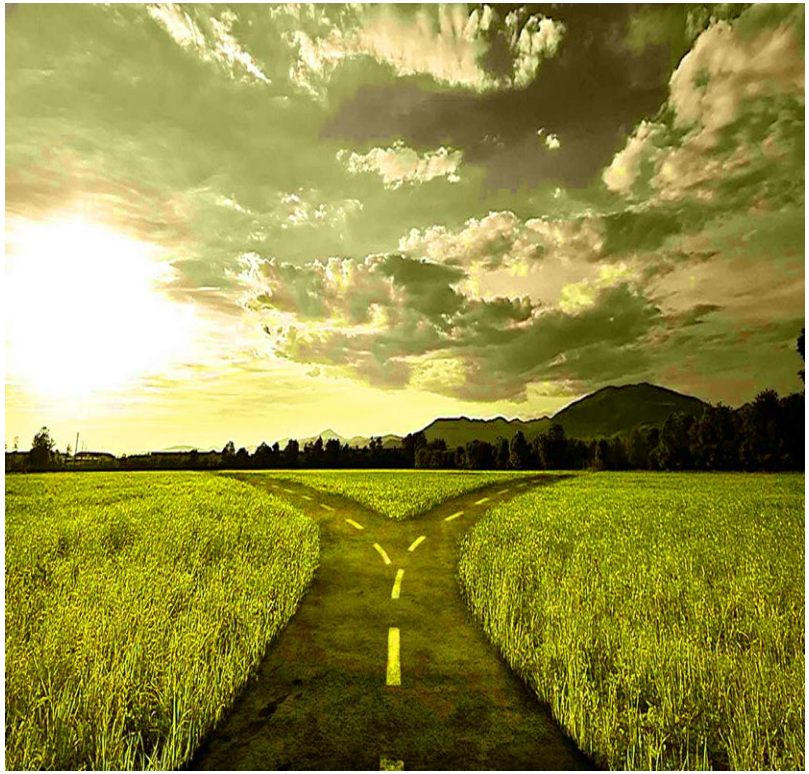
Defined Program Goals

- Establish clearly defined strategies, goals and objectives
  - Communication plan
  - Alignment to strategic plan
  - Realistic expectations
  - Sufficient resources
  - Define a third party life cycle

Governance

- Vendor risk assessment program operations can be in one of two structures:

1. Centralized
2. Decentralized



Policies, Standards & Procedures

A comprehensive set of policies, standards and procedures is the foundation for every effective third party risk management program

Policies

- Policies should be:
  - Defined at an enterprise level
  - Include all relevant credit union functions
  - They are the ”why” you are doing this.
  - A good policy is no more than 3 pages

Standards

- Standards are:
  - How you execute, take action, to enforce policies
    - Establish enterprise standards for risk tiers, ratings and classifications
    - Consider all relevant regulatory guidelines and industry best practices
  - Implemented by comprehensive guidelines and/or procedures
    - These should be separate from policies to facilitate updates and revisions over time

Procedures

- Procedures are:
  - Implementation guidelines and procedures
  - They are the “what” you are to do to implement your policies

Due Diligence

- Due Diligence Standard
  - Set at the enterprise level
  - Consider regulatory environment
  - Nature of services being outsourced
  - Data classification
  - Level-set vendor selection process
  - Developed in consideration of risk appetite

Risk Based Vendor Ranking

- Vendors should be ranked based on the risk they present to the credit union
- Establish standards for tiers based on risk tolerance
- Consistent assignment of vendor risk classification
- Validation should be included in periodic reviews

Contract Management

- Identify formal policies that impact/influence the contract process
- Identify key roles involved
- Establish guidelines for determining vendor “ownership”

Board Reporting

- Regulatory Awareness
- Self-assessments & independent assurance
- Integrated with strategic planing initiatives
- Internal & external trends
- Implications of enforcement actions

Management Oversight

- Ability to identify, assess and monitor third party risks
- Agreement on key control activities
- Timelines of corrective actions
- Adequacy of contracts
- Alignment with strategic plan

Compliance

- Identify all applicable requirements
  - Internal, Regulatory, Industry Standards
- Assessing existing level of compliance
- Organizations may have a need to demonstrate compliance to one or more regulation or standard

Compliance

- Assessing compliance as defined in the contract generally falls into 1 of 4 areas:
  1. Administrative policy compliance
  2. Technology requirements compliance
  3. Regulatory compliance
  4. Adherence to published standards

Contract Management

- Establish key roles
  - What areas of the organization should be involved and what is their role?
    - Business units, IT, Security, Legal, DR/BCP, Call Center, Other
- Establish procedures for contract exception review and approval

Mandatory Contract Provisions

- Standards for mandatory contract provisions
  - IT/security, privacy
  - Audit/assessment
  - Termination
  - Outsourcing (4th parties)
  - Incident reporting

4th Parties

- Contract provisions specifically addressing vendor outsourcing
  - Prior notice required
  - Risk assessment required prior to granting access to data
  - Your vendor should be required to have their own documented TPRM program in place

Standards for Termination

- Types of Termination
  - Normal: business relationship no longer needed
  - Cause: irreparable violation of contract terms
  - Convenience: better arrangement/opportunity
  - Regulatory/Supervisory – self explanatory

Data Types

- Knowing specific types of data a third party has access to is vital
  - Personally Identifiable Information (PII)
  - Protected Health Information (PHI)
  - Card Holder Data (CHD)
  - Payment Card Industry (PCI)
  - Confidential/Intellectual Property/Sensitive (CIPS)

PII

- Per Dept. of Homeland Security: any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as SSN, DOB, Mother's Maiden Name or biometric records; and (2) any other information that is linked or linkable to an individual such as medical, educational, financial and employment information.
- **FOR EXAMPLE…**a user's IP address as used in a communication exchange is classified as PII.

Types of PII

- Two types
  - Basic
    - Physical: Last name, first name, phone #, street address
    - Logical: email address, IP address
  - Sensitive – used in conjunction with basic PII
    - SSN or other federal government ID
    - Driver's License or other state/municipality ID
    - DOB

Data Location

- It is critically important that third parties provide both the physical and logical location for all data
  - Require data maps
  - Identify any boarder issues
  - Identify backup locations
  - Identify use of 4th parties

Additional Resources

- https://ithandbook.ffiec.gov
- https://www.pcisecuritystandards.org
- http://ssae18.com/index.html
- http://www.nist.gov
- http://www.isaca.org
- http://www.iso.org

Contact Information

Bryan Fury

VP Enterprise Risk Management

Corporate One FCU

614.825.9378 (O)

614.701.7561 (C)

bfury@corporateone.coop