

CERTIFIED VENDOR MANAGEMENT PROFESSIONAL

Certification Web-Based Training Curriculum

The Framework of Third-Party Risk Management (TPRM)

Risk Mindset

Compliance Risk

Compliance Considerations- Stephanie Lyon

Regulatory Guidance for TPRM

Interagency Guidance

Definition

Risk Management

Life Cycle

Governance

Supervisory Review

NCUA Guidance

Third Party Relationships

Planning & Risk Assessment

Financial Projections

Due Diligence

Risk Management

Part 748

CFPB Guidance

Expectations

TP & UDAAP

FFIEC Guidance

Expectations

TPSP & Gramm Leach Bliley Act (GLBA)

Compliance

Basics

PCI DSS Responsibilities

Definition

Requirements

Managing Risk

Other Rules

Certifications

Contractual Risk

Review

Responsibility

Recourse

General Data Protection Regulation (GDPR)

What and Who

Definitions

Requirements

Fines

Operational/Transactional Risk

Definition

Risk Exposure

Concentration Risk

Over Reliance

Geographic Concentration

Cloud Centration

Subcontractor

Reputation Risk

Risk Exposure

Environmental, Social, and Governance Risk

Risk Mitigation

Strategic Risk

Strategic Risk & TP Life Cycle

Risk Considerations

Credit Risk

Potential Impact

Considerations

Timing

Program Elements

Policy Requirements

Oversight

Components

Digital Assets

Culture Mindset

Culture & TP Management

Culture Evolution

Considerations for Culture

The Three Lines & TPRM

First Line

Second Line

Third Line

A Guide to Organizational Involvement- TPRM Roles

Vendor Owners/Stakeholders

TPRM Program Requirements

Senior Management & Board Oversight

Teamwork & TPRM

Internal Audit

IT/Information Security

Third Party Classification

The Why

Classify by Potential Impact

Classify by Data Access

Tier Classifications

Best Practice Framework

Program Evaluation

Exam and Audit Preparation- Rafael DeLeon

Best Practice Reporting

Onboarding Reporting

Ongoing Monitoring

Insurance & Licensing

Incident Reporting

TP Complaint

Gap Identification

Key Risk & Performance Indicators

The Intersection Points of TPRM

Business Continuity & TPRM

Continuity Partners

Reliance vs Resiliency

Hosting Types

Due Diligence Documents

Business Impact Analysis

Crisis Management & Disaster Recovery

Pandemic Planning

Pandemic & Contracts

Remote Work

Incident Response & Third Parties

Defining Incidents

Response

Policy/Plan

Partnering with TP

Risk Considerations

Responding to a TP Incident

Postmortem

Incident & Breach Notification

Data Governance and Protection

Data Governance and Protection

Data Definitions

Access Controls

Cloud Security & Hosting

Agreements & Policies

Data & Cyber Security- Jon Bowker & Frank Fede

Subcontractor Risk & Responsibilities

Responsibilities

Risk Mitigation

Partnering with Fintech

Regulatory Guidance

Mitigating Risk with Due Diligence

Alignment of Strategic Vision

Vendor as a Control- Michael Carpenter

Third-Party Risk Management (TPRM) Life Cycle

Planning & Due Diligence/Third Party Selection

Planning & Due Diligence

Strategies & Goals

Legal & Regulatory Compliance

Financial Condition

Business Experience

Qualifications & Background

Risk Management

Information System & Management of

Operational Resilience

Insurance

Subcontractors

Incident Reporting

Physical Security

Cost Benefit Analysis

Regulatory Guidance

Framework

Cost & Benefit

Request for Proposal

Contract Negotiation

Structure & Review

Term and Termination

Business Resiliency and Audits

Confidentiality & Security

Miscellaneous Contract Provisions

Different Vendor Types

Ongoing TPRM Monitoring and Due Diligence

Ongoing Monitoring

Purpose & Timing

Regulatory Expectations

Document Collection

Organizational Involvement

Tracking Service Disputes and Incidents

Outsourcing

Reasons to Outsource

Responsibilities & Risk

Pricing

Foreign Based Providers

Third Party Off Boarding

Relationship Evaluation

Considerations

Benefit of Exploring Options

Planning to Exit

Considerations

Contract & Exit Notice

Data Destruction & Securement

Deep Dive into the Documents of TPRM

SSAE 18/SOC

SOC 1 vs. SOC 2 vs. SOC 3

A Tour around a SOC- Cathy Ryan

SOC 2 Trust Services Categories

SOC 2 Reports

Trust Services Criteria

Security

CC6 : Logical and Physical Access

CC7: System Operations

CC8: Change Management

CC9: Risk Mitigation

Availability

Process Integrity

Confidentiality

Privacy

The Alignment of Trust Services Criteria & the COSO Framework

COSO Framework

COSO & SOC 2

CC1: Control Environment

CC2: Communication & Information

CC3: Risk Assessment

CC4: Control Monitoring

CC5: Control Activities

A Guide to Complementary User Entity Controls (CUEC)

What and Where to Find Them

Other Names

Response & Management

Complementary Subservice Organization Controls

Evaluation of Audit Opinion on a SOC Report

Where to Find

Opinion Outcomes

Scope

Dates

Reviewing SOC Testing

Types

Procedures

Financial Review

Financial Review Overview- Karianne Nink

Public Companies

Types of Public Reports

Form 10-k

Annual Report

10-Q

Form 8-K

S-1

S-4

10-K Section Review

Overview & Organization

Business

Risk Factors

Legal Proceedings

Management Discussion & Analysis

In depth Review of Financial Statements

Balance Sheet

Leverage

Interest Coverage Ratio

Income Statement

Statement of Cash Flows

Private Company Financials

Considerations

Guidance

Alternative Options

Reputation Review

Why Manage

Better Business Bureau

Complaints & Enforcement Actions

Lawsuits & Litigation

Insurance and License Review

Considerations

Types

Policy Considerations

Insured Entities

Licensing

Policy & Procedures

Data Protection & Governance Policies

Information Security Program

Data Security Policy

Record Retention & Data Destruction Policy

Policies & Procedures of your Third Parties

Business Continuity

Hiring/HR

Compliance Management

Vendor Management

Change Management

Social Media

Navigating TPSP Testing Documents

Penetration testing results

Business continuity testing results

Disaster recovery testing results