ACA Aponix
Cybersecurity and Risk
2018
THE M&A ADVISOR
TURNAROUND AWARD WINNER
AI 2016 HEDGE FUND awards WINNER
ACA Compliance Group Best FinServ Compliance Solutions Provider - USA & Best Co-Sourcing Provider: ACA Aponix
hedgeweek
AWARD WINNER 2017
2015 - 2017

Scaling your third-party cybersecurity risk management program

ACA Aponix
Cybersecurity and Risk

ABOUT ACA APONIX

OUR TEAM

Our team of highly experienced technologists have worked in senior roles at companies including:

- Goldman Sachs
- Merrill Lynch
- American Express
- Morgan Stanley
- Kepos Capital
- Highbridge Capital
- Trilogy Global Advisors
- U.S. Securities and Exchange Commission
- AIG
- Frontpoint Partners
- JAT Capital
- Diamondback Capital
- Sloane Robinson
- Buckingham Asset Management

Select ACA Aponix staff have held military clearance. Staff certifications/accreditations include:
CISSP, CISM, CISA, CEH, CRISC, ECSA, GSEC, OSCP, OSCE, CGEIT, CNE, GWAPT, GPEN, GXPN, GCIH, GCIA, GSLC, GCFE, GCCC, MCSE, MCSP, CCA, SSA, CSPO, A+, Network+, Security+, MCSA, CCNP R&S, CCNA Security, SixSigma Black, CMAA, ISO27001:2013, ISO22301:2013, CIPT, CIPP, CTPRP, MBA, CFA, PMP, JD, PhD

OUR MISSION

To help our clients reduce cybersecurity and IT risk by:

- Applying a balanced and holistic approach to identify and remediate risks through: Assessment, Remediation, Policies, Controls, and Training
- Building a robust security posture which starts with a thorough and thoughtful review of business process and technology
- “Raising the risk fences broadly” rather than focusing on the network perimeter alone

BACKGROUND

Third-party regulatory requirements are broad and can be widely interpreted depending on the size of your organization and the specifics of your regulatory agency.

Several best practices have been chosen for today's discussion. Given the investment in your program and the regulatory jurisdiction, some may be more applicable than others.

Assumptions have been made that you all have your program up and running and are past initial recommendations, such as:

- Creating a vendor inventory
- Prioritizing your vendor assessments
- Monitoring your vendors, including but not limited to financial analysis

REGULATORY JURISDICTION

This presentation is consistent with requirements stated in the following U.S. bulletins:

- OCC 2013-29, 2017-17, 2017-7
- FFIEC IT Handbook on Outsourced Technology Services
- FFIEC BSA/AML Examination Manual – Third-Payment Processors
- FRB Guidance on Managing Outsourcing Risk
- CFPB – Compliance Bulletin and Policy Guidance; 2016-02, Service Providers
- FDIC FIL 50-2016
- SEC OCIE Risk Alerts: Volume VI, Issue 5 and Volume IV, Issue 8

ACTIVE GOVERNANCE

- Effective enterprise risk programs govern their organization.
- Boards and senior managers are held accountable by regulators for all third-party relationships.
    - "A bank's use of third parties **does not diminish the responsibility of its board** of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws.[1]"

[1] OCC 2013-29 Third-Party Relationships: Risk Management Guidance

OVERSIGHT FRAMEWORK

Board of Directors

- Approve risk policies that govern third-party management
- Review and approve management plans for using third parties
- Ensure management takes appropriate actions to remedy material risk

Senior Management

- Establish risk based policies to govern third-parties
- Ensure commensurate due diligence and monitoring of third-parties
- Oversee third-parties through the life of the relationship

Third Party Risk Management

- Define enterprise scope and minimum requirements based on applicable regulations and risk tolerance
- Develop program guidelines and templates
- Test program compliance
- Monitor program metrics, enterprise reporting, and escalations

Business Management

- Traditional matrix organization
  - Ensure third-parties comply with bank policy and program
  - Ensure issues are identified and remediated
  - Escalate issues to appropriate oversight body
  - Ensure third-parties regularly test and implement agreed-upon remediation

	H.R	Marketing	R&D	Operations	Tech
Regulatory Comp.					
Information Security					
Operational Risk					

OVERSIGHT ASSIGNMENT

- Effective programs engage the appropriate oversight body consistently.
- Each firm will define activity risk based on their definition of **activity criticality** and **risk tolerance.**

The model uses 4 tier segmentation to determine oversight:

- **Critical** – board/executive oversight
- **High** – LOB executive oversight
- **Medium** – department oversight
- **Low** – minimum program requirements

Activity Risk Examples:

- **Critical** – settlement processor
- **High** – payroll
- **Medium** – project management

Tiering Model

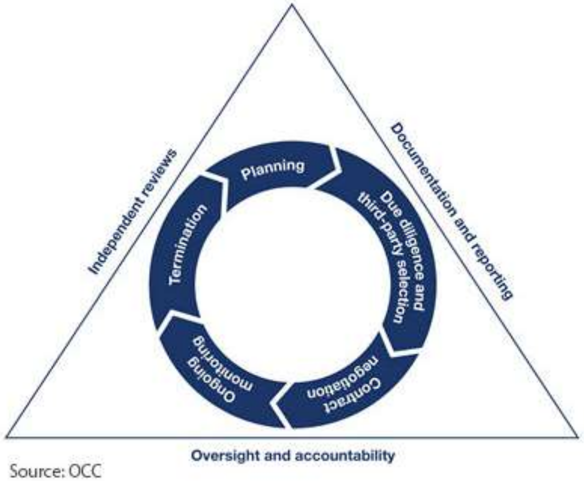
Enterprise Impact

Med	Med	High	Critical
Low	Med	High	High
Low	Med	Med	High
Low	Low	Med	Med

Activity Risk

RISK MANAGEMENT

Effective programs govern vendors throughout the lifecycle of the relationship with heavy emphasis on pre-contract due diligence and contract execution.



Planning
Due diligence and third-party selection
Contract negotiation
Ongoing monitoring
Termination
Independent reviews
Documentation and reporting
Oversight and accountability

Source: OCC

Regulator Expected Contract Terms

- Nature and scope of arrangement
- Performance measures or benchmarks
- Responsibilities
- **The right to audit and require remediation**
- Compliance with applicable laws and regulations
- **Cost and compensation**
- Ownership and license
- Confidentiality and integrity
- Business resumption and contingency plans
- Indemnification
- Insurance
- **Dispute resolution**
- Limits on liability
- Default and termination
- **Customer complaints**
- Subcontracting
- Federal Supervision

ACA Aponix Cybersecurity and Risk

OPERATIONAL THIRD-PARTIES

- Effective third-party programs should include operational service providers (e.g., underwriting, risk management, audit).
- Most organizations' third-party programs focus solely on technology providers and risk (e.g., information security, information technology).
- The regulators are clear:
  - *Banks offering account services to processors should develop and maintain adequate policies, procedures, and processes to address risks related to these relationships. At a minimum, these policies should authenticate the processor's business operations and assess their risk level.*[2]

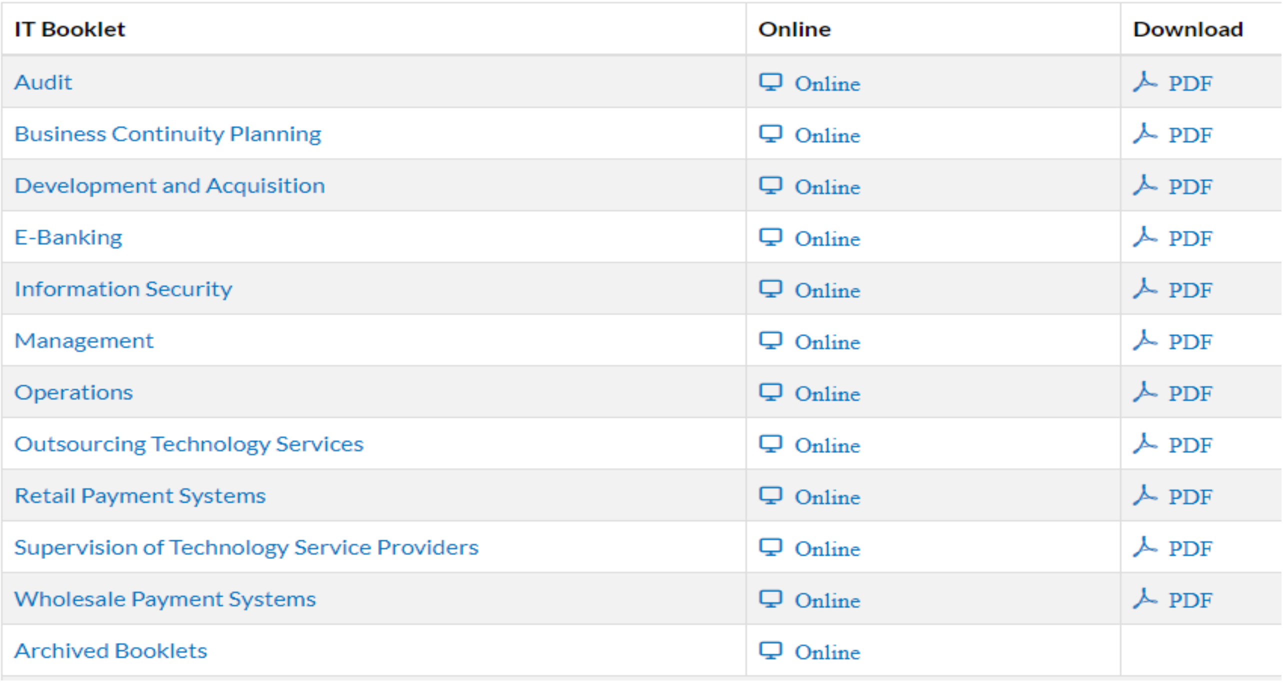
[2] FFIEC Bank Secrecy Act / Anti-Money Laundering Examination Manual

OPERATIONAL RISK METRICS

- Effective business units utilize external resources to enhance their operational risk metrics.
- FFIEC BSA/AML examination manual – third-party payment processors
  - Identify third-party payment processors
  - Identify major customers, locations and transaction volume
  - Validate the customers are operating a legitimate business
  - Monitor merchant relationships for unusual and suspicious activities
    - Merchant activities
    - Average dollar value and number of transactions
    - Charge-back history
    - **Consumer complaints** that suggest a third party processor is inappropriately obtaining personal account information for unauthorized transactions

FREE RESOURCES

FFIEC resources which include operational metrics:



IT Booklet	Online	Download
Audit	Online	PDF
Business Continuity Planning	Online	PDF
Development and Acquisition	Online	PDF
E-Banking	Online	PDF
Information Security	Online	PDF
Management	Online	PDF
Operations	Online	PDF
Outsourcing Technology Services	Online	PDF
Retail Payment Systems	Online	PDF
Supervision of Technology Service Providers	Online	PDF
Wholesale Payment Systems	Online	PDF
Archived Booklets	Online	

RISK THRESHOLDS & CONTROLS

- Effective programs clearly define risk thresholds and control assignment criteria.
- There are multitudes of quantitative and qualitative methods to do this.
- Below is a simple rules based method. When defining your model, consider the most frequently asked questions by your examiner.
  1. *How do you define your risk thresholds (e.g., tier, risk levels)?*
  2. *How do you enforce them across the enterprise?*
  3. *How to you validate "that", which range from exception management to SOC report validation?*

Risk	Inherent Risk Criteria		Control Assignment Criteria
Information Security	High	Confidential data processed by vendor (Payroll)	High IS Risk • Assessment Medium IS Risk • Service Organization Report (SOC) Report High Operational Risk • Operational Assessment Vendor Processes Card Data • PCI DSS Certification Vendor Employee Relationships • NDA, Employee Background Check
	Medium	Proprietary data stored by vendor (Project Management SharePoint)	
	Low	Public data	

REDUCING YOUR BURDEN

- Effective programs utilize cost effective specialists to protect their assets. Third-party specialists provide a multitude of services, including:
  - RFP Reviews
  - Contract Reviews
  - Vendor Assessments
- Benefits
  - Provides scale & cost savings
    - On average, 5-10 hours per year are required to adequately assess a vendor
  - Provides a knowledge base to junior staff
  - Frees up your senior staff
    - Vendor chase-ups
    - Report writing
    - Assessment questionnaire administration (YOY updates)
  - More time to better understand your risk
    - Review critical and emerging risks
    - Remediate critical controls
    - Analyze systemic risk (e.g. data centers, susceptible to specific threats)

QUESTIONS

Jeff Rowley

ACA Aponix

(803) 207-6805

jrowley@acaaponix.com

www.acaaponix.com