BerryDunn

EMPOWER 2025

Annual Not-For-Profit Summit

Trust but Verify: Strengthening Vendor Oversight for Financial and Security Resilience

BerryDunn

June 25, 2025

Presenters

Tina Bode

CISA, COBIT, CRISC, Prosci®
CCP, ITIL (F), Lean Six Sigma
Green Belt Certified

Senior Manager | Berry, Dunn, McNeil & Parker, LLC

Agenda

1 Learning objectives

2 Vendor risk management

3 Security and monitoring controls

4 AI thoughts

5 Questions

Learning objectives

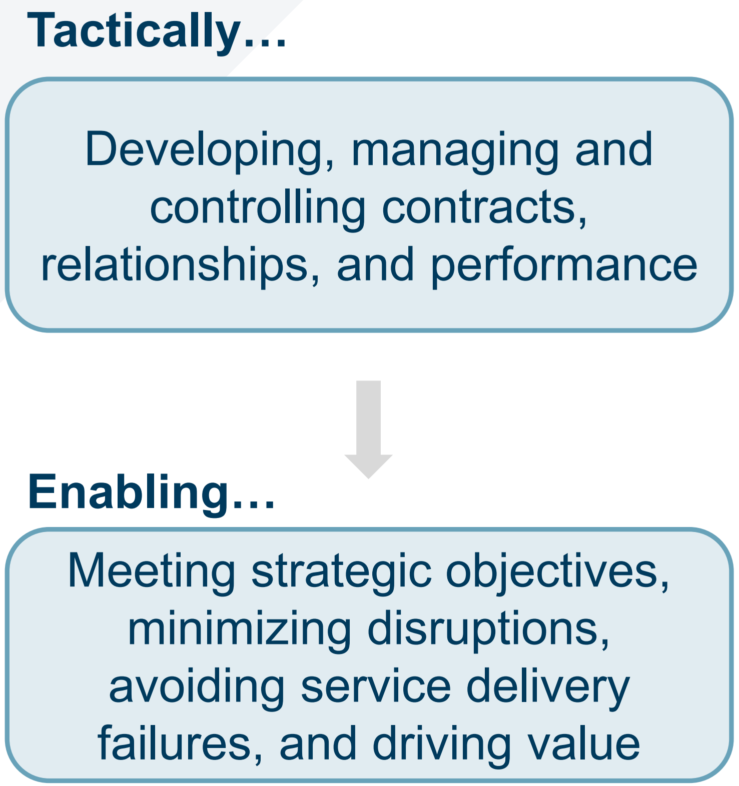
- Understand proper vendor risk management related to financial reporting
- Learn best practices for your own security and monitoring controls

BerryDunn
EMPOWER 2025
Annual Not-For-Profit Summit

Section 1

Vendor risk management

Why is vendor management important?



Tactically…

Developing, managing and controlling contracts, relationships, and performance

Enabling…

Meeting strategic objectives, minimizing disruptions, avoiding service delivery failures, and driving value

Organizations are changing how they operate.

- Increasing focus on internal operations and leveraging third parties for expertise and cost efficiencies
- Growth of Cloud, SaaS, IaaS, MSP, and other technology vendors

Vendor risks

Downtime risk

You're without that service

Perception risk

Your customers may not know it's a third-party service (branded as yours)

Financial risk

What if they go out of business? How do they impact your bottom line?

Compliance risk

How do their actions affect you?

Recovery and backup risk

Will you be able to access the data they host?

Your Reputation at Stake

Outsourcing services, not responsibility

MOVEit Transfer Exploit Hits Hundreds
GoAnywhere MFT Breach Exposes Data
NCR POS Outage Disrupts Restaurants
Healthcare Sector Hit by Vendor Vulnerabilities
Latitude Financial Data Breach
Education Sector Breach Impacts Thousands
Third-Party Law Firm Leak Exposes Client Data

Vendor risk management responsibilities

- Organizational-wide effort
- “Owners” of each vendor
- Vendor management coordinator
- Board oversight
- Vendor management happens twice:
    1. Initial vetting
    2. Ongoing

Polling question #1

Where to start

Vendor management BEGINS when a contract is signed.

Ongoing process, not one and done.

1. **Identify**
   Work with all departments in the organization and develop an inventory of third parties used
2. **Risk rank**
   Identify the risk and impact of each vendor to your organization
3. **Monitor**
   Conduct initial and annual due diligence based on the level of risk
4. **Report**
   Report on results of monitoring to the Board annually

1

Identify

Create a vendor inventory:

- Vendor’s name
- Contact information of primary contact
- Services/goods provided
- Your organization’s vendor “owner”
- Department the vendor contracts with
- Contract terms (length of contract, pricing)
- Any special requirements

If IT vendor or provider:

- Name and version of software or hardware used/purchased
- Is product hosted or on-prem?
- What customizations may exist?
- What support is being provided?
- Are upgrades included? How often?

2

Risk rank

- Risk ranking vendors allows you to establish an understanding of the vendor’s importance in your organization.
- Risk rankings also establish a standard and consistent expectation for due diligence procedures.

Critical or high risk

- Vendor provides a critical service (you couldn’t operate without them)
- Vendor has direct access to facilities or systems
- Vendor hosts confidential or personal information

Moderate risk

- Vendor provides an important service (you could operate without them, but would cause stress)
- Vendor has limited access to facilities or systems
- Vendor does not host or have access to confidential or PII information

Low risk

- Vendor provides a non-critical service (you could operate without them with minimal impact)
- Vendor has no access to facilities or systems
- Vendor has no access to data

High Effort ←→ Limited Effort

3

Monitor

Critical/High Risk Vendor:
Full vetting upon hire. Annual due diligence review.

Moderate Risk Vendor:
Full vetting upon hire. Biannual due diligence review.

Low Risk Vendor:
Some vetting upon hire. Due diligence review upon contract renewal.

Monitor

Monitoring activities should include:

Legal/Compliance

- Contract language
- Service level agreements
- Insurance
- Reference checks
- Background checks
- “Right to audit” clause
- Data ownership
- Responsibilities of each party
- Fourth parties

Financial Review

- Financial statements and footnotes
- Going concern risk
- Key accounting ratios (liquidity, profitability, asset turnover, financial leverage)
- SOC 1 Report

Security Review

- Understand data
- IT questionnaire/review
- SOC 2 report review
- Information security policy
- Disaster recovery and/or business continuity plans
- Incident response plan
- Security breach and/or lawsuit notifications
- User access review
- Data backup testing

A note on SOC exams

What to check

- Opinion
- Type 1 or Type 2
- SOC 1 or SOC 2
- Control objectives
- User control considerations
- Subservice control considerations

If a SOC exam is not available

Request the vendor complete a questionnaire or provide documentation

4

Report

- Contract and SLA performance
- Risk assessment
- Documentation requested/reviewed
- Documented concerns or issues
- Areas needing Board and executive input

Monitor

Shifting board responsibilities

- SEC requirements
- Disclosure of cybersecurity risks and incidents
- Oversight of cybersecurity and risk
- Cybersecurity and vendor management often go together
- Changes may require additional cybersecurity expertise on Boards

Polling question #2

BerryDunn

EMPOWER 2025

Annual Not-For-Profit Summit

Section 2

Security and monitoring controls

Security and monitoring controls

Minimum controls

- Annual user access reviews
- Testing data integrity before and/or after major software changes
- Identifying and documenting your responsibilities
- Data backup testing
- Failover testing results
- Fourth-party data hosting and controls

BerryDunn

EMPOWER 2025

Annual Not-For-Profit Summit

Section 3

AI thoughts

AI thoughts

Vendor use

- Ask your vendors how they use AI
- Include this as part of your annual due diligence review

Polling question #3

AI thoughts

Internal use: appropriate use cases and cautions

- Potentially lower risk vs. medium to high reward
  - Microsoft Copilot and ChatGPT
  - Workflow automation tools
- Deliberate balance of risk vs. reward
  - Generative AI

Questions?

BerryDunn

EMPOWER 2025

Annual Not-For-Profit Summit

Tina Bode

Senior Manager | Berry, Dunn, McNeil & Parker, LLC

207.541.2253
tbode@berrydunn.com

BerryDunn is the brand name under which Berry, Dunn, McNeil & Parker, LLC and BDMP Assurance, LLP, independently owned entities, provide services. Berry, Dunn, McNeil & Parker, LLC provides tax, advisory, and consulting services. BDMP Assurance, LLP, a licensed CPA firm, provides attest services.