DATCON '24 Kansas City NEXT

Are You Risk Aware?

Third-Party Risk Management

Dr. Erika Voss, PhD

VP Information Security
DAT Freight & Analytics

Vanessa Sukolics

Head of Risk and Controls
DAT Freight & Analytics

What is Third-Party Risk Management?

The process whereby companies monitor and manage interactions with all external parties with which it has a relationship.

This may include both contractual and non-contractual parties.

Key words:

“External”

“Monitor”

“Manage”

"Due Diligence"

Caring is sharing

Know your vendor's security posture

- It is key to impacting or damaging yours

Protect your business financial health

- Anticipate the before
- The “What If” game matters

Comply with regulations

- PCI, HIPAA, NYDFS, CCPA, GDPR

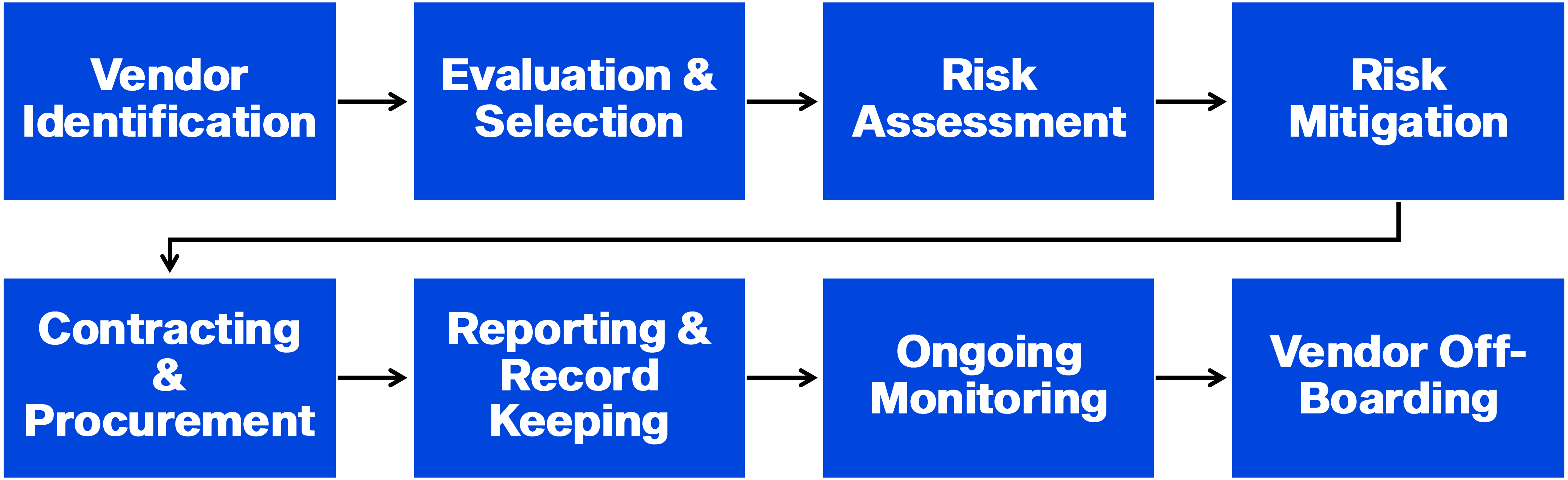
Protect your company's reputation

- Stock price
- Customers

Knowledge

Scope and get	Scope and get leadership buy-in for your TPRM program
Identify and understand	Identify and understand types of third-party risk
Implement	Implement TPRM across your organization
Maintain and monitor	Maintain and monitor your TPRM program

Third-Party Risk Management Lifecycle



Vendor Identification

Evaluation & Selection

Risk Assessment

Risk Mitigation

Contracting & Procurement

Reporting & Record Keeping

Ongoing Monitoring

Vendor Off-Boarding

Building a Third-Party Risk Management Program?

Identify, assess, and control the risks and interactions with your company

Think procurement

Think offboarding

Comply with regulations

Protect confidential information (PII, PHI, PCI)

Strengthen your supply chain – the first or second tiers

Handle disruptions – exercise the plan

Identify the types of third-party risks

- Cybersecurity risk
- Operational risk
- Compliance risk
- Reputational risk
- Financial risk
- Strategic risk
- Geopolitical risk
- Supply chain risk - NEW

Alignment

Align with your Executives on your organization’s risk appetite and establish a shared definition of third-party risk.

Why is it important to them?

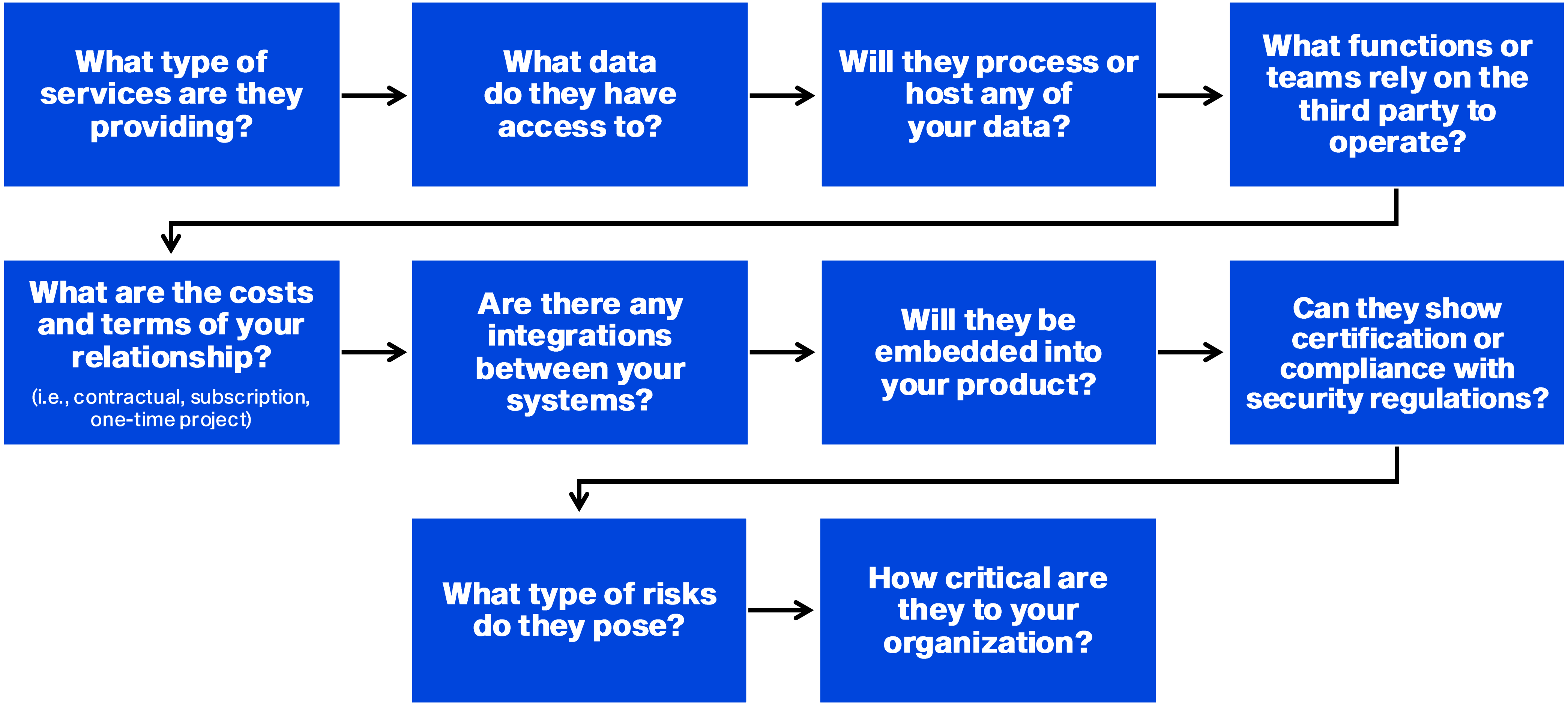
Correlate your third-party risks to broader enterprise risks:

- Reputational loss
- Regulatory fines
- Brand damage

Accuracy Matters

- What are the goals of your TPRM program?
- Do you have specific compliance requirements or deliverables (i.e. for publicly traded companies or regulated industries)?
- What risk domains should be managed (i.e. InfoSec, privacy, financial, reputational)?
- What is the organization’s appetite for risk?

Create effective, efficient assessment processes



What type of services are they providing?

What data do they have access to?

Will they process or host any of your data?

What functions or teams rely on the third party to operate?

What are the costs and terms of your relationship?

(i.e., contractual, subscription, one-time project)

Are there any integrations between your systems?

Will they be embedded into your product?

Can they show certification or compliance with security regulations?

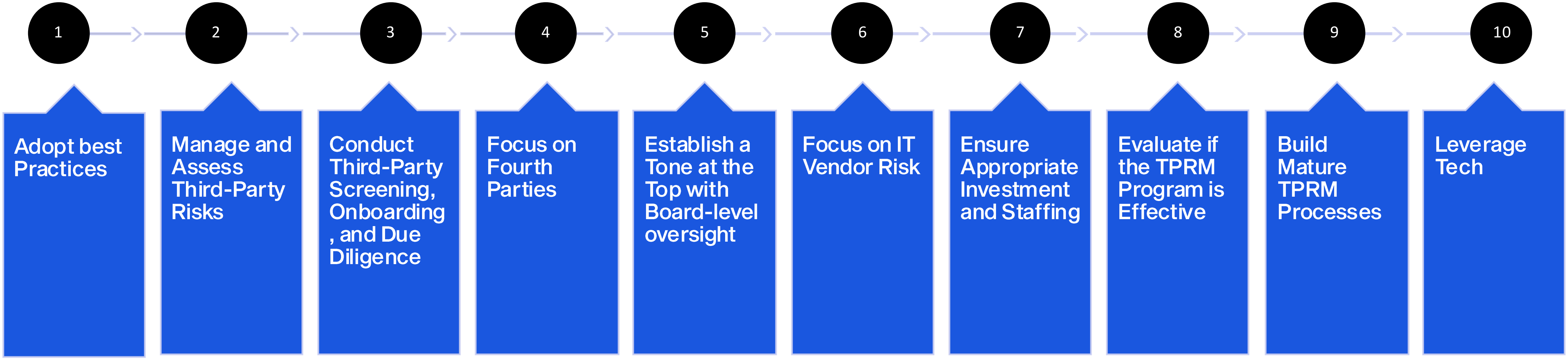
What type of risks do they pose?

How critical are they to your organization?

Exercise, exercise, exercise

- Table-top exercises matter
- Discuss with both your business partners and your executive leadership team
- Continuous monitoring
- Go deep into your supply chain; it matters
- Capture the risks
- Account for third-party risks in your GRC program

Now what?



1. Adopt best Practices
2. Manage and Assess Third-Party Risks
3. Conduct Third-Party Screening, Onboarding , and Due Diligence
4. Focus on Fourth Parties
5. Establish a Tone at the Top with Board-level oversight
6. Focus on IT Vendor Risk
7. Ensure Appropriate Investment and Staffing
8. Evaluate if the TPRM Program is Effective
9. Build Mature TPRM Processes
10. Leverage Tech

Key takeaways

73% of organizations have moderate to high level dependency on service providers

800 companies were surveyed across the US; 37% responded with their programs for TPRM aren't established or consistent

Only 54% of companies across the globe make TPRM a part of their broader Cyber Risk Management Program

Be better?

Automating response to third-party incidents

Too many organizations report using manual processes and a complex array of tools to understand and resolve vendor breaches.

Building a single source of truth

More teams are getting involved in third-party risk management, but the use of multiple overlapping tools presents a foggy picture of risk.

Giving up spreadsheets once and for all

Nearly half of companies still use spreadsheets to assess their third parties – and many are not confident in the results!

Remediating third-party risks

The point of a TPRM program is to reduce risk. However, research shows a disparity between the frequency of risk assessments and effective risk remediation.

DATCON '24 Kansas City NEXT

Thank You