Third-Party Risk Management

Ankura Financial Services Advisory

Jon Berry
Jordan Kuperschmid
Peter Pearlman
Ope Odebiyi

April 2025

Thank You - Premier Partner Members

cefli

Thank You – CEFLI Affiliate Members

cefli

Deloitte.

faegre drinker

ankura

berwyngroup

Evadata

Guidehouse
outwit complexity

MAYNARDNEXSEN

mtb

troutman pepper locke

Wolters Kluwer

CEFLI Reminders

The Presentation Deck

- The presentation deck is available now, on this page: **https://cefli.org/webinars/**

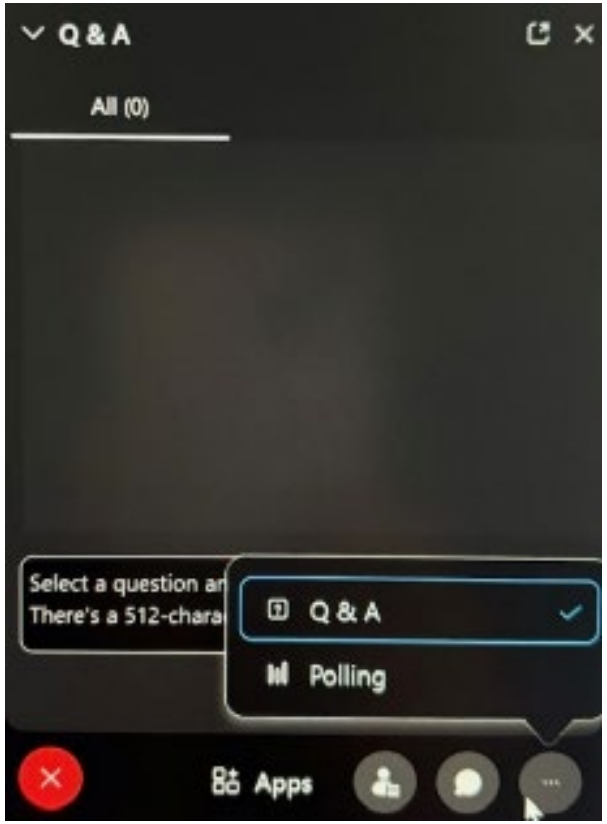
Post-Event Communication

We will email the following information to you in the next few days:

- A link to the recording
- A copy of the slides
- A Certificate of Attendance template (to those who attended the live event)

Questions Welcomed!

- Please use the **Q&A Function** (not the Chat function).
- Type your questions into the Q&A area at any time. We'll save some time at the end to cover questions at that time.



Today's Speakers

Jon Berry

Senior Managing Director, Financial Services Advisory

Jordan Kuperschmid

Senior Managing Director, Financial Services Advisory

Pete Pearlman

Managing Director, Financial Services Advisory

Ope Odebiyi

Managing Director, Technology and Cyber Risk Advisory

Third-Party Risk Management

Ankura Financial Services Advisory

Jon Berry
Jordan Kuperschmid
Peter Pearlman
Ope Odebiyi

April 2025

Background

In today's interconnected landscape, effective management of third-party risks is critical for Insurers to mitigate customer, brand and financial risk.

In today's dynamic business environment, financial institutions increasingly leverage **third-parties to drive innovation and operational efficiency**. This reliance **introduces risks that must be proactively managed**. As organizations entrust core operations, IT infrastructure, and sensitive data to external providers, they become **vulnerable to potential disruptions and other risks**.

Building a **robust Third-Party Risk Management (TPRM) program** is not merely a defensive measure; it is a **strategic imperative**. An effective **program ensures regulatory compliance, safeguards sensitive information**, and fosters **strong, resilient partnerships.** By **proactively addressing third-party risks**, financial institutions can **enhance operational resilience, protect their reputation**, and cultivate **long-term, trusted relationships** with their vendors and customers alike.

Recent Events

Data Breach

- A large insurer's third-party software provider was subject to a ransomware attack, leading to the compromising of sensitive customer data for over a million individuals.
- The insurer faced legal and class action lawsuits, suffering financial and reputational damage in the process.

Failed IT Migration

- A financial institution had outsourced the migration of customer data to a new system. Following the migration, customers were unable to access their accounts.
- The institution suffered regulatory fines and increased scrutiny following the incident.

Operational Resilience

- A financial institution’s cloud provider experienced a major outage, leading to the disruption of their online trading platform.
- Both the organization and their customers were unable to execute trades during this time, leading to reputational damage.

Third-Party Risk Management Leading Practices

To navigate today's complex risk landscape and drive strategic value, Insurers should embrace a balanced risk-based approach with data-driven oversight to ensure resilient ecosystems.

TPRM Governance:
Establish a well-defined governance model, along with clear frameworks, policies and procedures that outline explicit roles and responsibilities for all stakeholders.

Risk-Based Approach:
Implement a tiered approach to due diligence, ongoing monitoring, and governance, with increasing scrutiny based on the risk-tier of each vendor.

Continuous Monitoring & Assessment:
Perform ongoing monitoring of third-party risk profiles, including financial, operational, regulatory, projects mix changes.

Data Privacy & Cybersecurity:
Conduct comprehensive assessments of third-party cybersecurity/data practices and robust controls to ensure compliance with regulations (e.g., GDPR, CCPA, NYDFS).

Contractual Risk Mitigation:
Ensure contracts clearly define performance / delivery expectations, risk ownership, security requirements, and audit rights and all are properly operationalized.

Centralized Data Repository:
Establish a single source of truth for data, a centralized repository for all TPRM data, to support informed risk decisions.

Incident Response & Business Continuity Planning:
Develop and test third-party incident response and business continuity plans.

Risk Reporting & Analytics:
Utilize data analytics and reporting to identify and track third-party risks and trends.

Third-Party Risk Landscape

When choosing a third-party, one should consider the risks below, with a focus on inherent and residual risk. Third-parties should be tiered based upon their risk profile, along with the criticality of services they provide.

Regulatory / Compliance Risks

- Regulatory Fines or Penalties for Non-Compliance
- Contractual/Legal Risks
- Privacy Violations (e.g., GDPR, CCPA, etc.)
- Governing Body Frameworks (e.g., DORA)
- Regulatory Reporting Errors
- Remediation

Information / Cybersecurity Risks

- Cyberattacks (Ransomware, Malware, Phishing)
- Data Loss/Data Breaches
- Intellectual Property Theft
- Access Control Failures
- Technology Vulnerabilities
- Data Integrity Issues
- Data Retention Issues

Operational / Business Continuity Risks

- Performance Risk
- Concentration Risk
- Resiliency Failures
- Technology Failures
- People and Process Risk
- Transaction Errors
- Natural Disasters

Financial Risks

- Financial Viability Issues
- Credit Risk
- Counterparty Risk
- Fraudulent Activity
- Liquidity Risk
- Market Risk /Derivatives Risks

Reputational / Customer Risks

- Reputation/Brand Damage
- Revenue/Customer Impact
- Customer Dissatisfaction
- Environmental and Sustainability Concerns
- Geopolitical Risks

Emerging Risk

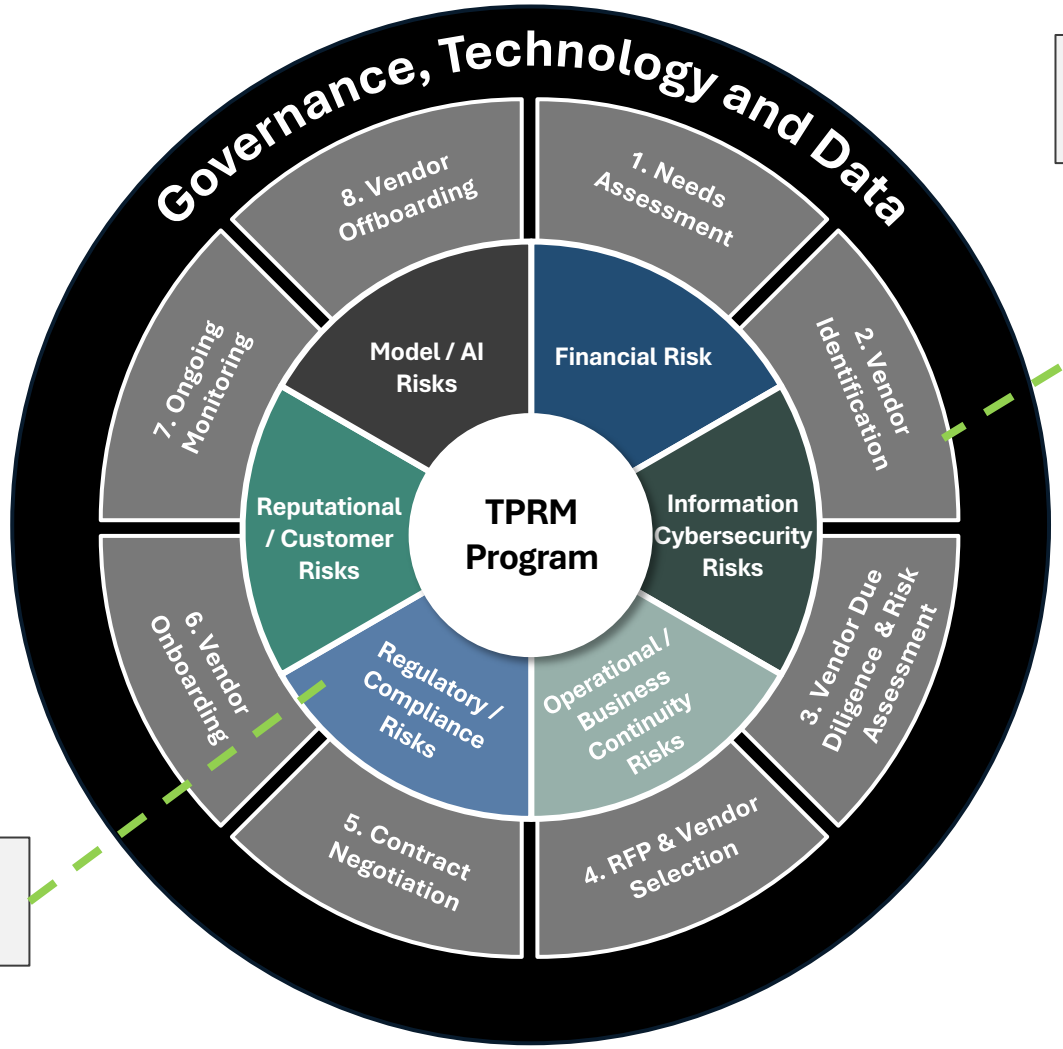
Model / AI Risks

- AI Governance
- Model Bias Risks
- Model Drift Risks
- Lack of Transparency and Explainability
- Data Integrity Risks
- Intellectual Property Risks

Third-Party Risk Management Program Foundations

Third-Party Risk Management mitigates key risk, follows a structured lifecycle, and is enabled by technology.

A comprehensive TPRM framework seeks to ***identify, assess, and mitigate a wide spectrum of risks*** *within the vendor lifecycle activities, which is* ***supported and enabled by governance, technology and data****.*



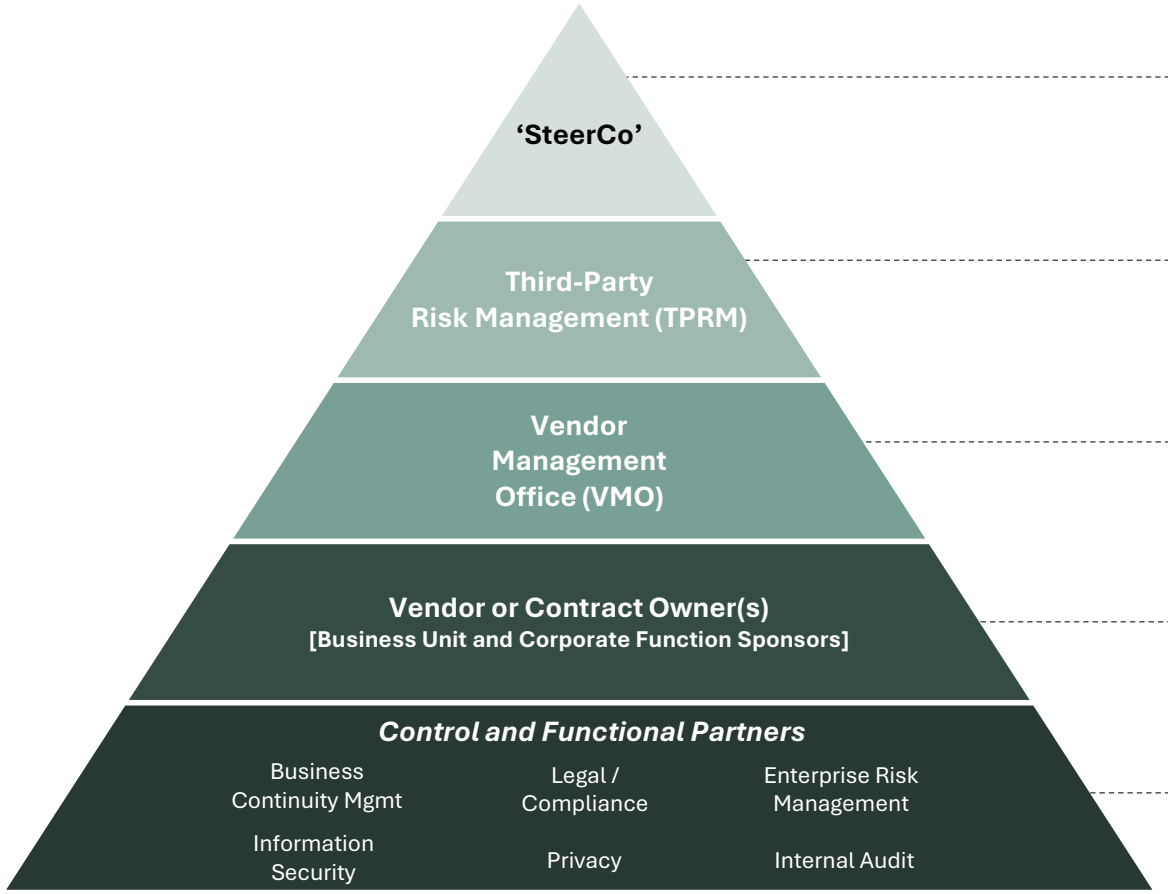
Vendor Lifecycle Activities

Vendor Risk Landscape

Example Third-Party Risk Management Governance Structure

Robust TPRM governance requires a clear structure and orchestration amongst many stakeholders, tailored to your risks. There are many ways to design your specific structure.

Example Governance Structure



Purpose: Function and/or Committee for strategic direction, approves major vendor decisions, oversees TPRM.
Responsibilities Include:
- Approves vendor management policies and procedures.
- Reviews and approves high-risk vendor relationships.
- Sets the risk tolerance for vendor relationships.

Purpose: Identifies, assesses, and mitigates risks associated with external vendors, suppliers, and partners.
Responsibilities Include:
- Evaluating potential risks associated with engaging third-parties, including financial, operational, regulatory, and reputational risks.
- Continuously monitoring the performance and activities of third-parties.

Purpose: Manages the day-to-day operations of the vendor management program and acts as the central hub for all vendor related activities.
Responsibilities Include:
- Acts as central hub for all vendor-related activities (e.g., due diligence, onboarding, monitoring).
- Responsible for developing vendor management policies, procedures, and standards.

Purpose: Primary point of contact and is accountable for specific vendor relationships and or engagement, ensuring alignment between vendor performance and business objectives, and facilitating effective day-to-day management.
Responsibilities Include:
- Acts as the primary liaison between the organization and the assigned vendor.
- Monitors day-to-day vendor performance, ensuring adherence to contractual obligations and SLAs.

Purpose: Provides specialized expertise and operational execution throughout the vendor management lifecycle, supporting TPRM and ensuring effective vendor relationships.
Responsibilities Include:
- Provides specialized expertise and input throughout the vendor lifecycle.
- Executes operational tasks and provides support to the VMO in vendor-related activities.

Example TPRM Governance, Components, and Architecture

A sound TPRM architecture ensures standardized processes, and clear reporting, enabling proactive risk mitigation and regulatory alignment across all third-party relationships.





Centralized Intake and Prioritization

- Defines a process for initiating new or modifying existing third-party relationships.
- Establishes clear evaluation and prioritization criteria based on risk, strategic alignment and regulatory requirements.
- Maintains a centralized vendor inventory and risk profile repository.
- Streamlines effort for third-parties and internal personnel.

Dedicated Third-Party Risk Coordinating Body

- Serves as the central hub for all TPRM activities/interaction and monitors for best practices.
- Establishes and maintains standardized processes and tools.
- Facilitates comprehensive risk assessments.
- Provides clear issue resolution pathways.
- Owns and delivers consolidated reporting.

Collaborative Risk Domain Integration

- Enables close partnership with control partners across relevant risk domains (cybersecurity, compliance, privacy, resilience, legal, anti-fraud, records).
- Ensures alignment with evolving regulatory requirements and industry best practices.
- Monitors and adapts to the changing risk landscape.
- Creates an optimized risk-based approach to diligence, contracting, and monitoring.

Dynamic Risk Intelligence

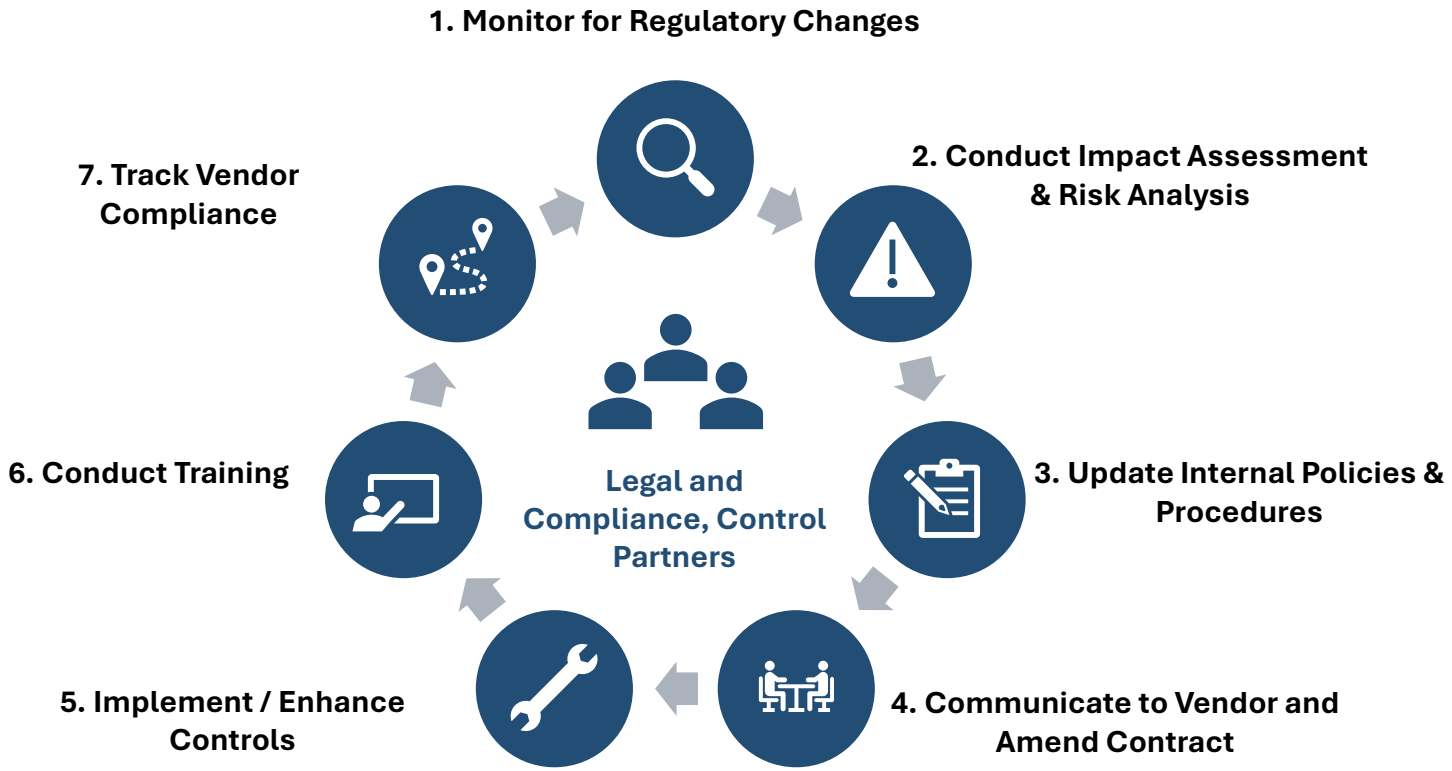
- Facilitates continuous assessment of internal and external factors influencing third-party risk:
  - Drivers for third-party service utilization.
  - Feedback and performance data (complaints, successes).
  - Historical risk events and triggers.
  - Policy and regulatory updates.

Contract and Lifecycle Management

- Manages contract lifecycle (negotiation, execution, termination).
- Ensures audit rights and vendor control assurance.
- Provides training and awareness to employees and vendors.
- Includes a documented process for the safe and secure termination of third-party relationships.

Regulatory Change Management

Effective regulatory change management processes integrated with the TPRM program helps to ensure compliance and mitigates potential impacts through proactive monitoring, assessment, and adaptation.



Example Regulations/ Guidance

Data Privacy

- General Data Protection Regulation (GDPR)
- Gramm-Leach-Bliley Act (GLBA)
- Payment Card Industry Data Security Standard (PCI DSS)
- California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA)

Financial Regulations

- Sarbanes-Oxley Act (SOX)
- Office of Foreign Assets Control (OFAC) Regulations
- Bank Secrecy Act (BSA)
- Foreign Corrupt Practices Act (FCPA)
- Dodd-Frank Wall Street Reform and Consumer Protection Act

Frameworks / Guidance:

- Digital Operational Resilience Act (DORA)
- AI: NAIC Model Bulletin and State Guidance and Regulations
- OCC Bulletin 2013-29
- NIST Cybersecurity Framework
- FFIEC Guidance (Federal Financial Institutions Examination Council)
- Federal Reserve Board (FRB) SR 23-4

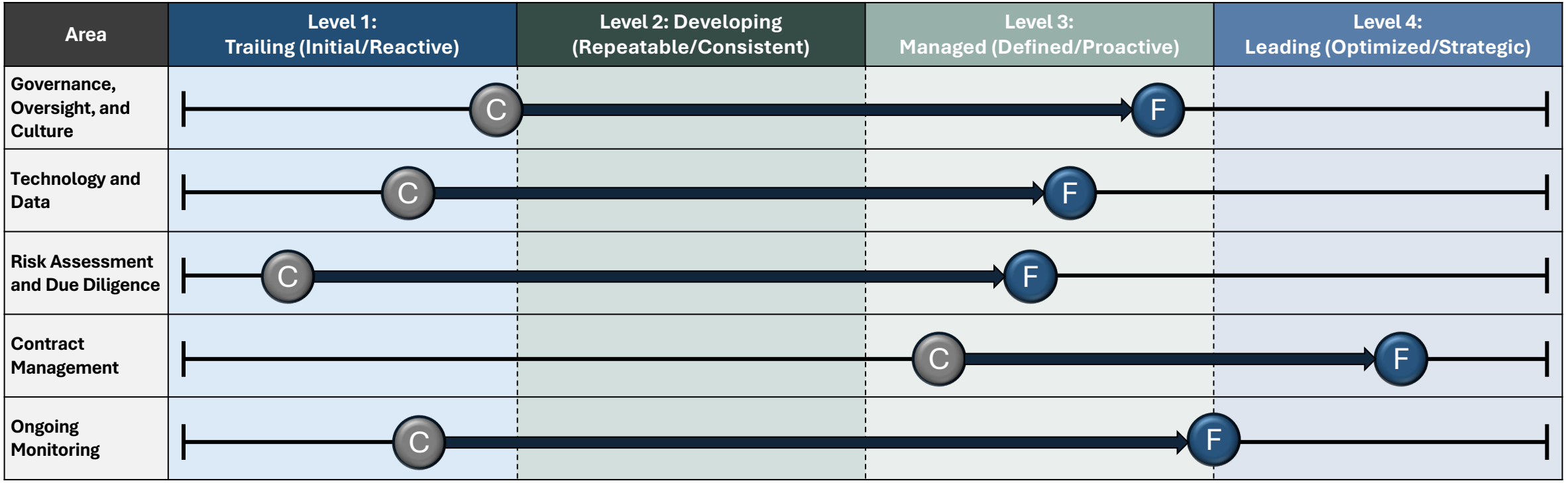
Considerations for a Third-Party Risk Management Program

To achieve a robust TPRM program, Insurers should evaluate their operating model across a wide variety of considerations, ranging from upfront controls to downstream reporting

Category	Considerations / Questions
Roles, Responsibilities, and Interaction Model	• Are roles and responsibilities clearly defined for all parties involved in third-party risk management? • Is there a documented interaction model and explicit escalation procedures? • Is there segregation of duties between those who assess risk and those who manage/utilize the vendor?
Risk Assessment and Risk-Based Approach	• Is there a documented, comprehensive risk-based assessment process? • Are specific risk factors (e.g., criticality of service, data sensitivity, financial stability) considered and risk ratings clearly defined? • Does the risk assessment process address relevant regulatory guidance?
Use of Technology	• Are there technology solutions that effectively automates task assignments, approvals, and escalations to ensure adherence to defined interaction models? • Does the technology enable each of the relevant roles/stakeholders to conduct their work efficiently and collaboratively? • Does the technology facilitate the collection of centralized program records and knowledge management?
Scope of Third-Party Relationships	• Does the scope include all material third-party relationships, including cloud providers, software vendors, and counterparties? • Is there a clear definition of what constitutes a "material" third-party and an appropriately sized process for each vendor type/risk category? • Does the scope of the program consider fourth-party risk?
Upfront and Ongoing Procedures and Controls	• Are there sufficient due diligence procedures for vendor selection and contracting? And are any findings incorporated into the monitoring efforts? • Are there clearly defined and measurable service level agreements (SLAs) that promote/incent the desired behaviors from the third-party? • Are analytical tools and data feeds utilized to continuously monitor vendor performance, identify anomalies, and trigger alerts based on risk thresholds?
Reporting and Data Capabilities	• Is there a comprehensive, actionable program reporting capability, including risk dashboards at the desired frequency? • Does reporting include key risk indicators (KRIs) and key performance indicators (KPIs)? • Are data/reports used to drive decision making and actions?
Incident Response and Action Planning	• Does the program have a documented incident response plan specifically for third-party related risks? • Are there clearly defined escalation paths and communication protocols for various risk triggers (e.g., data breach, financial viability issues, continuity breaks)? • Are regular testing and simulation exercises conducted to ensure the effectiveness of the incident response plan and the readiness of relevant stakeholders?

Third-Party Risk Management Maturity Matrix

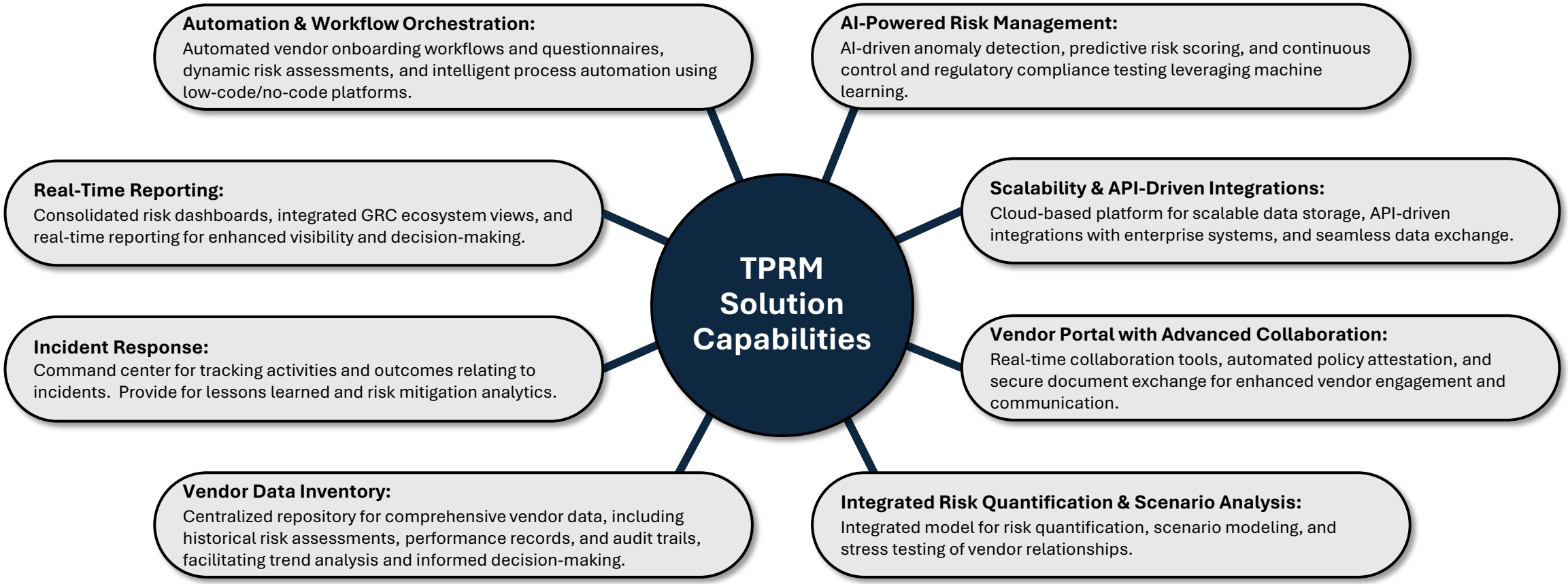
A maturity matrix can be leveraged to assess a company's current state ('C') and desired future state ('F') to illuminate the activities and related roadmap related to achieve the future state.



Illustrative: Detailed assessment is tailored to each company's industry, geography, risk profile

Technology Enabled Capabilities

To optimize your Third-Party Risk Management Program, select technology solution(s) that deliver the capabilities to support and integrate the elements of your TPRM program.



Questions & Answers

Jon Berry – Senior Managing Director, Financial Services Advisory jon.berry@ankura.com **610.745.0849**

Jordan Kuperschmid – Senior Managing Director, Financial Services Advisory jordan.kuperschmid@ankura.com **908.347.5610**

Pete Pearlman – Managing Director, Financial Services Advisory peter.pearlman@ankura.com **908.892.3898**

Ope Odebiyi – Managing Director, Technology and Cyber Risk Advisory ope.odebiyi@ankura.com **312.972.6261**

CEFLI Reminders

1. Please complete our **1-minute post event survey** when you receive the email shortly after we say good-bye today
2. The **presentation deck, a link to the recorded event and a Certificate of Attendance** template will be emailed to those who attended the live session
3. CEFLI's materials are not filed for CLE or CE with any State Bar or other organizations. In the event you plan to self-submit for CE or CLE with the organizations you are involved with, the following slide may be helpful.

CE & CLE Insights

While CEFLI does not file its materials with any State Bar Associations, if you plan to self-submit for potential CLE consideration with a State Bar Association, the following may be helpful:

- CEFLI is the sponsor of its in-person and Educational Webinar event
- CEFLI provides a Certificate of Attendance form only to individuals who attended a live webinar or an in-person event
- CEFLI does not have a way of knowing how many attorneys attend a CEFLI webinar or event
- CEFLI webinars (which are one hour in duration) do not have a timed agenda
- Participants may ask questions of the speakers during webinar events by clicking on the Q&A feature in the Webex
- CEFLI is not a marketing organization – it is a compliance and ethics organization whose mission is to support professionals by providing educational opportunities that address current compliance matters

Thank You Jon, Jordan, Pete and Ope!

Ankura Financial Services has extensive experience assisting a wide variety of financial services clients assess and enhance their Third-Party Risk Management Programs.

Jon Berry – Senior Managing Director, Financial Services Advisory jon.berry@ankura.com 610.745.0849

Jon Berry is a Senior Managing Director, based in Boston, MA. with over 25 years of experience in the financial services industry. Jon has worked extensively with banks, insurers, and asset management companies, focusing on third-party risk management, complex business and technology transformation, and regulatory compliance. He is known for leading large-scale programs that enhance organizational effectiveness, manage risk, and improve customer experience through digital and technological enablement. Jon has successfully guided teams in assessing, designing, and implementing strategies that lower costs, increase controls, and drive positive change, ensuring clients navigate the intricate economic and regulatory landscapes effectively.

Jordan Kuperschmid – Senior Managing Director, Financial Services Advisory jordan.kuperschmid@ankura.com 908.347.5610

Jordan Kuperschmid is a Senior Managing Director, based in New York with over 35 years of experience in the financial services industry. He has worked extensively with insurance and reinsurance companies. Jordan specializes in remediation and transformation, focusing on operations, risk management, and data. His expertise includes mitigating third-party risks and addressing issues related to intentional or unintentional disruptions that impact customers. Jordan has also contributed to the transformation of risk and compliance operating models, enhancing control and process efficiencies. Jordan's work has been pivotal in supporting negotiations and settlements with regulatory bodies by analyzing complex transactional data and implementing ongoing monitoring tools.

Pete Pearlman – Managing Director, Financial Services Advisory peter.pearlman@ankura.com 908.892.3898

Pete Pearlman is a Managing Director, based in New York with over 35 years of experience in the financial services industry. He has worked extensively with insurance companies, banks, and their service providers. He has extensive experience designing third-party risk management strategies, implementing those strategies at the corporate level and in the businesses, and engaging third-parties to assist his clients across the insurance operational lifecycle and sourcing work to third-party service providers.

Ope Odebiyi – Managing Director, Technology and Cyber Risk Advisory ope.odebiyi@ankura.com 312.972.6261

Ope Odebiyi is a Managing Director based in Chicago, IL. with 20 years of experience and background in IT Operations and Infrastructure. Over the years, he has managed cybersecurity risk assessments, third-party risk management, target operating model implementation for some of the largest global organizations across North America, Europe, and Asia. His client engagements span healthcare, life sciences / pharmaceutical, manufacturing, financial services, and insurance industries.

www.Ankura.com