Third Party Risk Management

ACP CT Chapter

March, 2019

pwc

Introductions – With you today

Jim Slavin

PwC Director
CS&P – Third Party Risk
Hartford, CT
Jim.slavin@pwc.com

Joe Krause

PwC Director
Cybersecurity & Privacy
Boston & Hartford
joseph.krause@pwc.com

Mike Isaac

PwC Manager
Cybersecurity & Privacy
Florham Park, NJ
michael.r.isaac@pwc.com

Agenda

Objective: Discuss current trends in identifying, mitigating, and managing risks presented by third parties- using cyber and business continuity risks as examples

- Overview of the Third Party Risk Management Framework
- Managing Third Party Cybersecurity and Privacy Risks
- Managing Third Party Business Continuity/Disaster Recovery Risk
    - FFIEC Appendix J as a Guide
- Questions and Comments (Welcome Throughout)

1

Introduction to third party risk management

What is third party risk management?

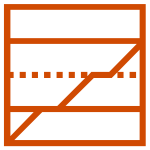
Third party risk management helps organizations answer a few seemingly simple yet critical questions:

1 **With whom am I doing business?**

2 **What risks do they pose?**

3 **How do I successfully manage those risks?**

Current Trends in TPRM



New regulations and increasing expectations (OCC, GDPR, NYDFS, CA Privacy, FFIEC etc.)

Borderless supplier marketplaces

Increasing concentration risk concern

Disruptive new technologies such as IoT and migration to Cloud

Movement away from point in time assessments

Executive focus on TPRM risk

Use of risk data, predictive modeling, statistics and visualization to generate insights

Increased focus on fourth, fifth and nth party risk

Movement away from manual processes and spreadsheets

Advent of consortiums and industry alliances

What is third party risk management?

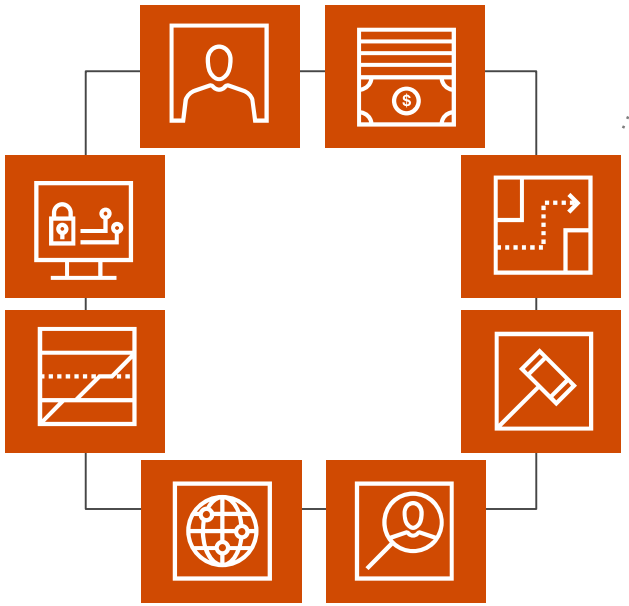
There are numerous risks that organizations using third parties need to consider, including:

Reputational

Financial

Cyber and Privacy

Risk that an organization's data is lost or security is compromised due to deficiencies in the cybersecurity and privacy controls of the third party



Continuity & Resiliency

Risk of third-party failure on the continuation of business as usual for the organization

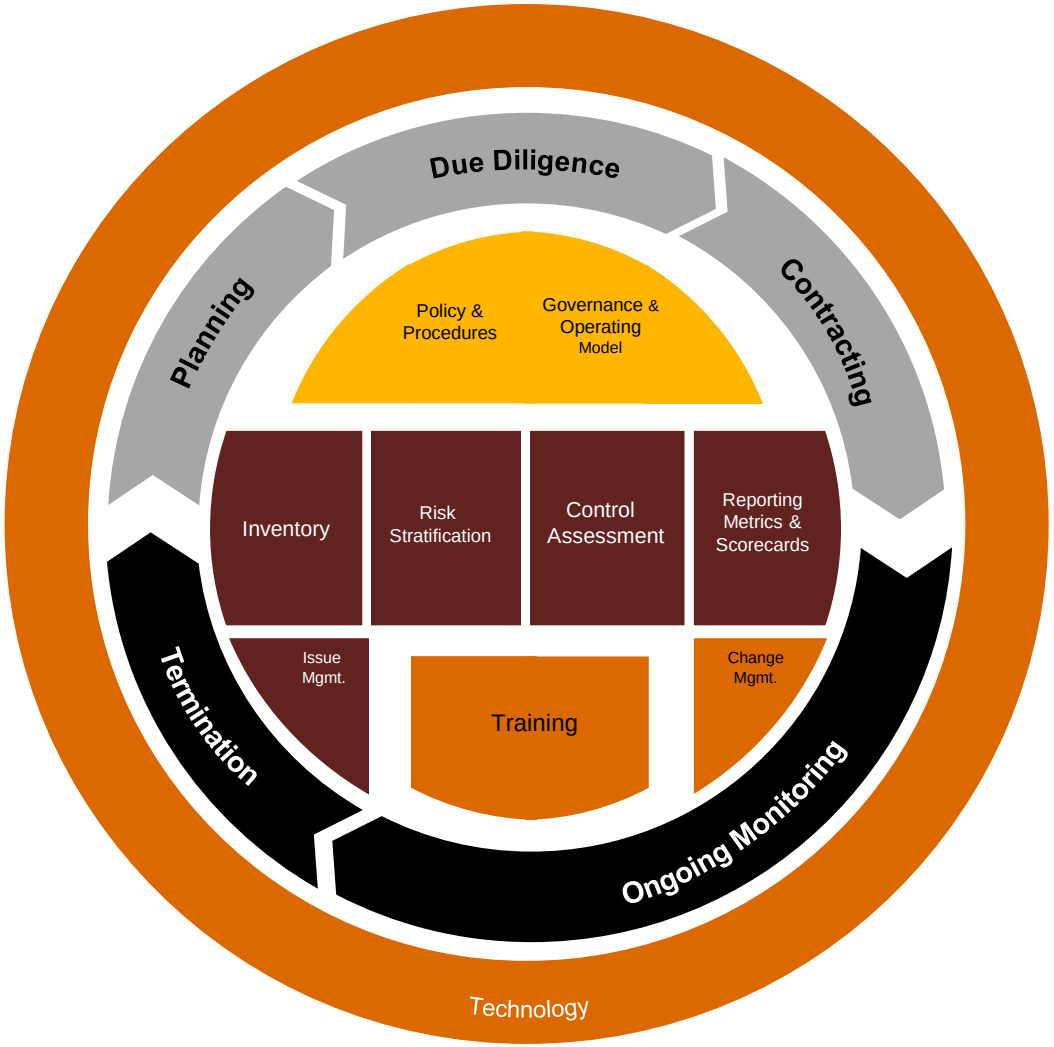
Operational Risk

Regulatory Compliance

Geopolitical

Environment and Social Accountability

The TPRM Lifecycle



- Planning
- Due Diligence
- Contracting
- Ongoing Monitoring
- Termination

- Governance & Oversight
- Technology

2

Cybersecurity Considerations

Objectives of TPRM: Understand the cyber program at your provider

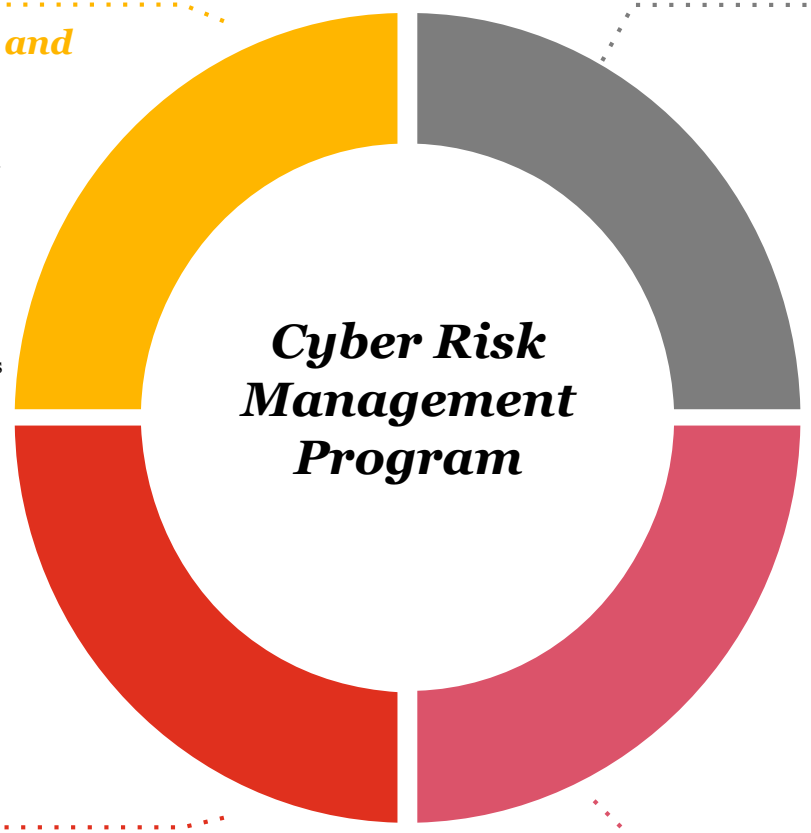
With the increasing frequency and sophistication of cyber incidents and heightened regulatory and investor scrutiny, many organizations are establishing new Cyber Risk Management programs – primarily focused on improving risk governance structures and setting up a credible second line of defense.

Establishing an effective Cyber Risk Management program based on a defined framework and operating model enables organizations to consistently identify, assess, respond to, monitor, and report on existing and emerging cyber risks

Cyber Risk Governance, Strategy and Operating Model

The foundation of the Cyber Risk Management Program is defined and aligned to the enterprise risk appetite and strategy. Some of the key activities include:

- Defining the operating model
- Setting cyber risk appetite for the enterprise or lines of business
- Establishing risk committees
- Defining Cyber Risk Management Policies & Standards for Second Line of Defense
- Designing a centralized library of risks, threats and controls



Cyber Risk Identification and Assessment

Cyber risks and threats that could potentially impact the enterprise are identified, as well as the controls that are in place to mitigate them. Some of the key activities include:

- Risk identification and threat profiling
- Determining inherent risk, identifying and evaluating controls and residual risk estimation

Cyber Risk Monitoring and Reporting

A formal and repeatable process is established to monitor key performance indicators and report their evolution to the board of directors or appropriate risk committees. Some of the key activities include:

- Design a cyber risk dashboard and reporting platform
- Define second line of defense key performance indicators and establish a mapping to the enterprise key risk indicators

Cyber Risk Response

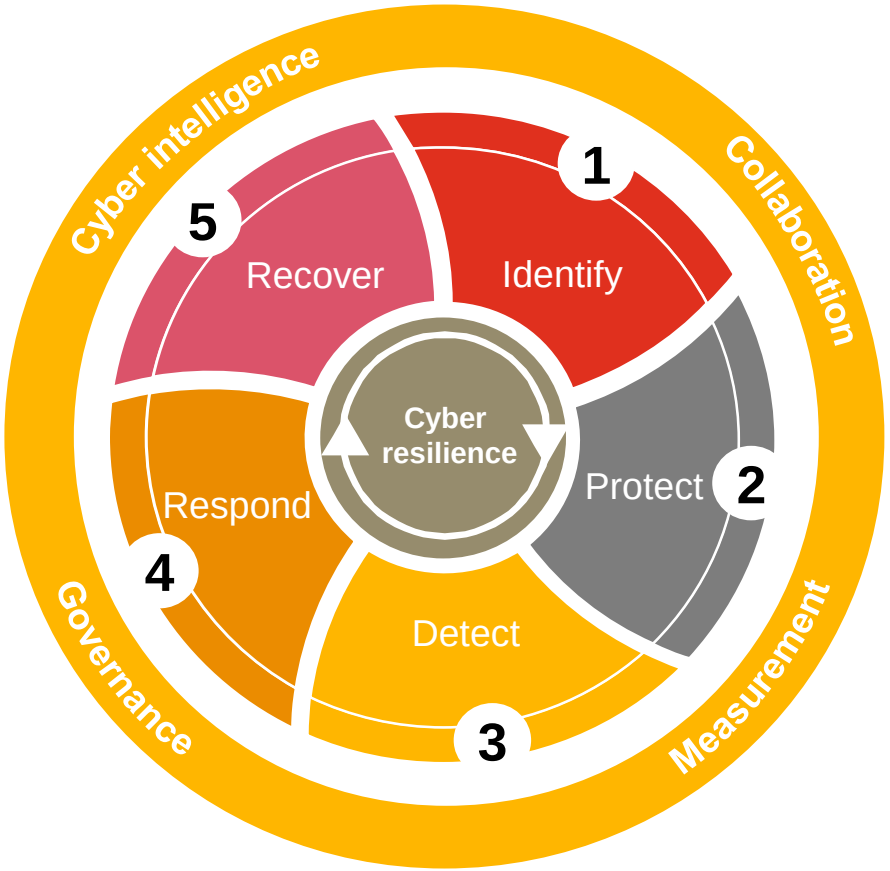
A plan is defined to treat risk and manage risk exposure. Some of the key activities include:

- Analyze risk appetite vs current risk exposure to determine the appropriate risk treatment decision (i.e. treat, terminate, transfer, tolerate)
- Identify mitigation actions and implement according to determined plan

Measuring the third party for cyber resilience

When these 5 functions are working well, the organization will be more capable of withstanding and recovering from incidents – cyber attacks or otherwise.

Identify	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities
Protect	Develop and implement the appropriate safeguards
Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event
Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event
Recover	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event



Role of the third party assessor in the process

Identify

Review the results of management's efforts to:

- **Inventory information assets** and understand the business impact of their technology landscape;
- **Risk rank assets** based on business criticality, data sensitivity, and technology risk (i.e., **identify crown jewels**);
- **Assess cybersecurity program maturity**, factoring in people, processes, and technology supporting cyber risk management functions;
- **Understand obligations** to customers, regulators, auditors, and government bodies;
- **Review third-party and business partner connections** into and out of their IT environment;
- **Collaborate with peer organizations** and trusted advisors to explore the emerging threat landscape, incorporating observations into incident readiness processes where feasible.

Role of the third party assessor in the process

Prioritize & govern

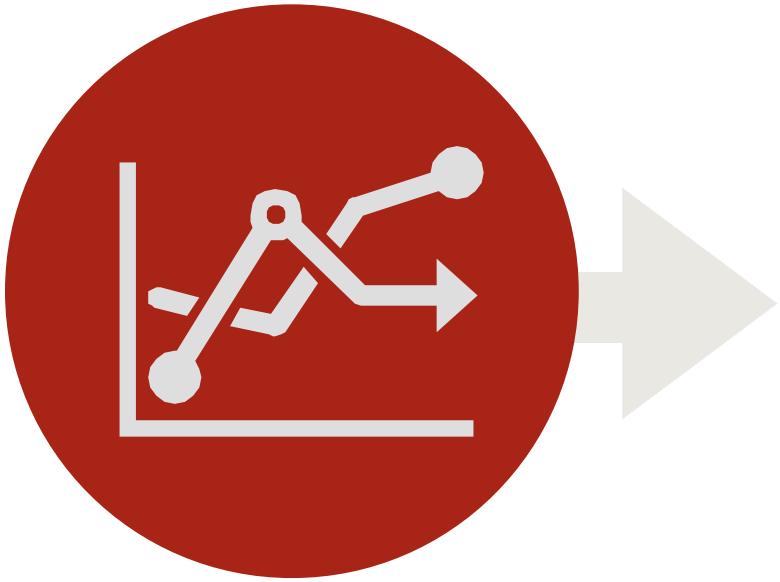
Review the results of management's efforts to:

- Perform and **interpret the results of risk assessments**, with a particular emphasis on strategically important risks;
- Highlight risk areas **where decisions were made to accept the risk**;
- **Develop program remediation plan** (e.g., heat map, roadmap) designed to tackle quick wins, high-impact opportunities, and multi-year initiatives first;
- Engage business and technology stakeholders to **develop future-state program** and **risk management** operating model;
- **Allocate resources**, budgeting for both CapEx and OpEx, to effectively implement and operate next-generation capabilities;
- **Establish governance model** and organizational structure to provide oversight, steer program, and coordinate efforts.

Role of the third party assessor in the process

Monitor

Review the results of management's efforts to:



- Develop program **key performance indicators and metrics** and feed data back into governance for **continuous improvement;**
- **Report** on indicators of compromise, key risk indicators and key performance indicators;
- Report on cyber risk program maturity **assessment results** and progress toward **maturity improvements**;
- **Monitor peer organizations'** activity for potential growth opportunities and business risks.

3

BCM Considerations

How prepared are you if you lose a critical third party?

- When it comes to business continuity and third party service providers, it is common for companies to think about their own potential crisis event and how their critical third party service providers / vendors will support them during a business disruption.
- *However, companies rarely develop and document recovery strategies and plans addressing how they will continue business if one of their critical third party service providers suffers a business disruption that results in them either being unavailable for an extended period of time or possibly is lost completely.*
- We've seen numerous instances where a business disruption at a critical third party impacts even the most internally prepared organizations. And the ripple effect of downtime can be huge both economically and in terms of your brand.

The message here is: "Don't let your service provider's crisis become your crisis!"

Do you know your third parties? Do they know you?

- It is extremely important for you to know how critical you are to your third party service providers. The companies that provide third party products and/or services to your company also provide products and services to other companies. And just like you, they too must assess the criticality of their business functions, dependencies, resource requirements, and the needs of their customers and stakeholders and prioritize accordingly.
- *While a particular third party service provider may be critical to you and to your company's ability to continue business, your company may not be as critical to that third party service provider. That's not to say your business isn't important to them and that you won't be supported in some capacity at some point in time, but there may be many other companies that could be prioritized ahead of your company.*

The message here is: "Know how important you are to your service provider! Don't find out after a business disruption to your third party, that their recovery prioritization does not align with your expectations!"

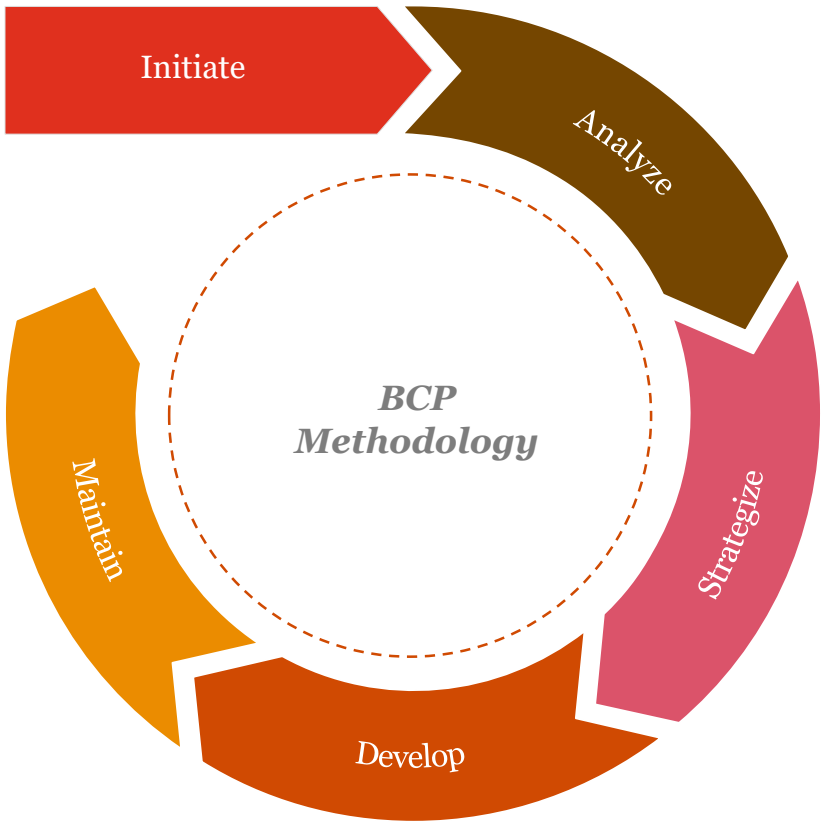
Understand the risks and have a plan!

- If your company is like most, you have a service level agreement with your critical third party service providers, but little to nothing in the way of documented strategies addressing how your company will be supported should the third party service provider experience a business disruption.
- *Unfortunately, service level agreements provide limited protection if your third party service provider experiences a crisis event, as they'll likely fall back to the contract's "Force Majeure" clause where they'll exercise "best efforts" during the event.*

The message here is: "Don't rely on SLAs during a business disruption to your third party. Have a plan. Develop a strategy!"

Analyze third party providers as you would your own business functions leveraging the BCM Lifecycle.

- Policy & Governance (including Board & Senior Management oversight)
- Risk Assessment/Business Impact Analysis
- Technology and Business Strategies
- Plan Development & Documentation (including detailed recovery procedures for addressing business functions, technology, security, people life safety and pandemic issues, outsourced activities, and crisis communications)
- Testing, Sustainability/Maintenance (including Training & Awareness programs and Periodic Review processes)



Key Activities within each phase of the BCP lifecycle

1 Initiate

Project governance, planning and kick-off

- Understanding historical BCM program and leadership goals and objectives
- Defining risk impact categories and individual impact threshold ranges
- Coordinating with key stakeholders from IT DR, Supply Chain, Risk Management, and Emergency Response to ensure interdependencies are well coordinated

2 Analyze

Business impact analysis

- Defining Recovery Time Objectives (RTOs) and impacts for critical business function downtime
- Identifying minimum resources required to continue to operate with a focus on applications, equipment, materials, facilities, staffing, vital records, key personnel and critical vendors
- Identifying RTOs for all application systems and technology used by the critical functions and their associated recovery point objectives (RPO)

3 Strategize

Gap & strategy selection

- Performing a gap analysis of recovery needs against what is currently in-place
- Conducting recovery strategy sessions for a loss of site (e.g., transfer workload, work from home, shift production), systems (e.g., manual workarounds), people (e.g., transfer workload, temporary staffing), and third parties (e.g., alternate vendors)
- Discussing potential risks, issues, and investment needs associated with recovery strategies

4 Develop

Plan development

- Aligning the recovery approach across the organization
- Identifying recovery teams, roles and responsibilities
- Documenting the recovery plans and procedures for each critical process

5 Maintain

Validation, training and awareness

- Validating the recovery procedures
- Familiarizing personnel with their roles and responsibilities
- Conducting table top walkthroughs of the BCPs

BCM activities to strengthen third party resiliency

Business Impact Analysis & Risk Assessment

- Identify and validate your third party service providers as part of your annual BIA process. Risk rank each of them and prioritize them based on criticality. Determine the impact to the company should the service provider be unavailable for an extended period of time or be lost completely.

Strategy Development / Selection

- Identify your recovery options and develop strategies to address the scenario including the implementation of work around procedures if applicable.
- Establish a relationship with your key service providers and understand their recovery priorities and where your company falls within their prioritization.
- Understand what the third party providers' "best efforts" entails, and how that aligns with your recovery requirements and the expectations of your customers and stakeholders.

Testing & Exercise

- Exercise scenarios for full and partial loss.

Appendix J

Appendix J is contained within the Federal Financial Institutions Examination Council's (FFIEC's) Business Continuity Handbook and includes themes and requirements set forth by the Office of the Comptroller of the Currency (OCC) guiding financial services institution's due diligence of their third-party technology service providers. But is leading practice for companies in all industries, not just financial services. Appendix J covers the following four elements:

Third party risk management

Validation of resiliency capabilities at each stage of the relationship management lifecycle

Third party capacity

Third parties' ability to deliver essential services under adverse scenarios, in addition to possible alternatives in the event of third party failure

Testing with third parties TSPs

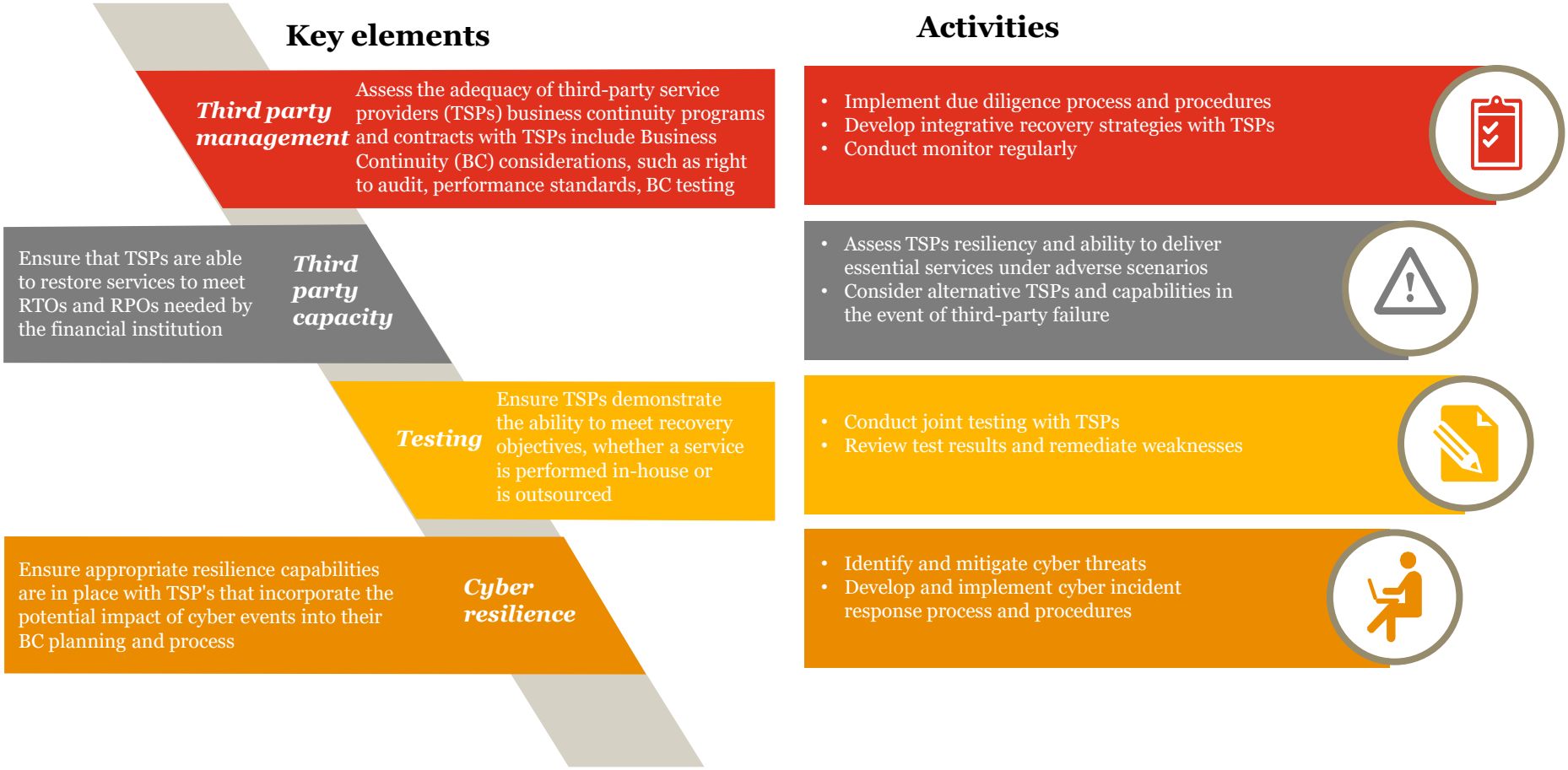
Testing business continuity resilience between financial institutions and TSPs, in addition to the review of test results and remediation of any observed weaknesses

Cyber resilience

Identification and mitigation of cyber threats to data and operational infrastructure, as well as effective incident response procedures to cyber attacks

Appendix J – Key Elements & Activities

The following graphic describes the key elements and identifies activities to address each of them.



Thank you

pwc.com