KPMG

Does your third-party risk program extend far enough?

Financial institutions must make managing "fourth-party" risk a priority

kpmg.com

Financial institutions need to address "fourth parties"

— Has your third–party risk management (TPRM) program adequately addressed the risk of your third parties' use of downstream suppliers, vendors, and subcontractors (that is, fourth parties)?

— Do you know how far your data is traveling outside your company's direct oversight?

— Which of your critical services are dependent on fourth parties?

— Is your data adequately managed to ensure confidentiality is maintained, that customer and consumer rights are protected, and that your company's reputation is not exposed to greater risk?

If you are unsure of the answers, read on for a discussion of some practices your company should consider implementing within your TPRM program to address these fourth-party risks.

Fourth-party oversight is vital

Financial institutions have been working diligently to establish TPRM programs to fulfill recent regulatory guidance, such as Office of the Comptroller of the Currency (OCC) Bulletin 2013-29 and Federal Reserve Board (FRB) Supervisory Letter 13-19. Given the significance of these directives, financial institutions have had to decide where to focus their primary activities.

In reality, fourth-party risk management requires even greater consideration given you have no legal contract with them. Consider: Third parties engaged by financial institutions often enlist the help of subcontractors, suppliers, vendors, or other organizations. However, third parties may fail to manage these fourth parties with the same rigor that the financial institution would have applied if it had engaged the fourth party directly. Regulators expect financial institutions to manage third parties—and by extension, fourth parties—in the same way they manage an internal function or division.

In light of this regulatory expectation, oversight of fourth parties is a key component of a FS institutions third party risk management program and should be a priority focus area as financial institutions work to ensure the sufficiency and sustainability of their TPRM programs.

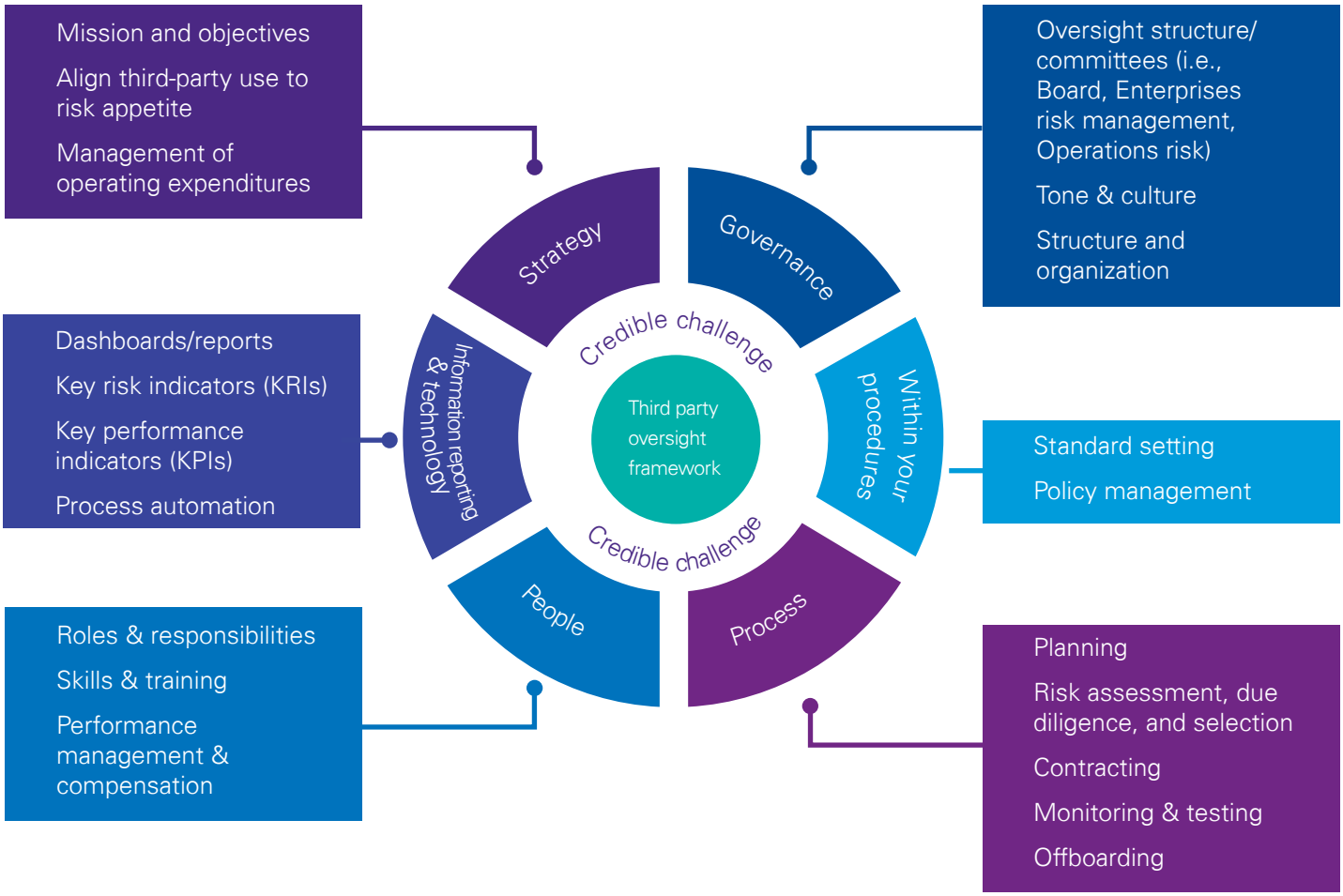
Call to action

Within your TPRM program you have to have the ability to identify fourth parties and demonstrate how you have assessed your third parties oversight and management of them. The result of this assessment should provide you with the information you need to make a decision whether to engage a third party to provide a service that is dependent on fourth parties. You should be able to inventory services dependent on fourth parties and explain how you assess their ongoing delivery of the services and your mitigation plans in the event that there is a break down in the delivery of the service.

KPMG

KPMG's TPRM framework

KPMG's TPRM framework aligns the requirements from regulatory guidance into six framework elements as depicted below:



Below, we present **KPMG's TPRM framework** elements aligned to specific fourth-party risk management considerations defining key aspects for considering when establishing a fourth-party risk program.

Program requirements	Key considerations when establishing a program
 **Strategy**	— Define when it is appropriate for your third parties to engage fourth parties. — Define risk appetite of fourth-party usage (consider concentration, type of service provided, etc.)
 **Governance**	— Establish a fourth-party risk assessment to identify when fourth parties are used and whether your third party has an adequate Third Party Risk Management Program in place to manage them in line with your expectations. — Define governance responsibilities for third parties, business areas engaging third parties that use fourth parties, as well as enterprise governance considering concentration of fourth-party use.
 **Policy & Procedures**	— Establish, within policy, which fourth parties are important for assessing and monitoring (in scope) and define criteria for risk assessing which fourth parties present greater risk. — Define roles and responsibilities considering governance and people factors. — Establish fourth-party center of excellence/risk program due diligence and ongoing monitoring protocols to include: – Details for determining critical fourth parties, as well as a risk rating of in-scope fourth parties – For higher-risk fourth parties, definitions of specific due diligence and risk assessment activities necessary – Methods and criteria for assessing the third parties oversight program of fourth parties
 **People**	— Engage dedicated, knowledgeable, and trained resources to the fourth-party center of excellence/risk program who understand general third-party risk concerns to adequately assess third parties' oversight of fourth parties, including risk-based assessment of certain fourth parties. — Ensure other risk subject matter experts are accountable when engaged to assess specific risk concerns with the fourth-party program, (e.g. information security, business continuity, compliance, etc.).
 **Information Tech & Reporting**	— Enable capture of fourth-party risk assessments as well as inventory (of significant fourth parties) to allow for adequate governance and oversight. Document and understand data flows across key fourth parties and how your data is stored and backed up once it enters the fourth parties environment.

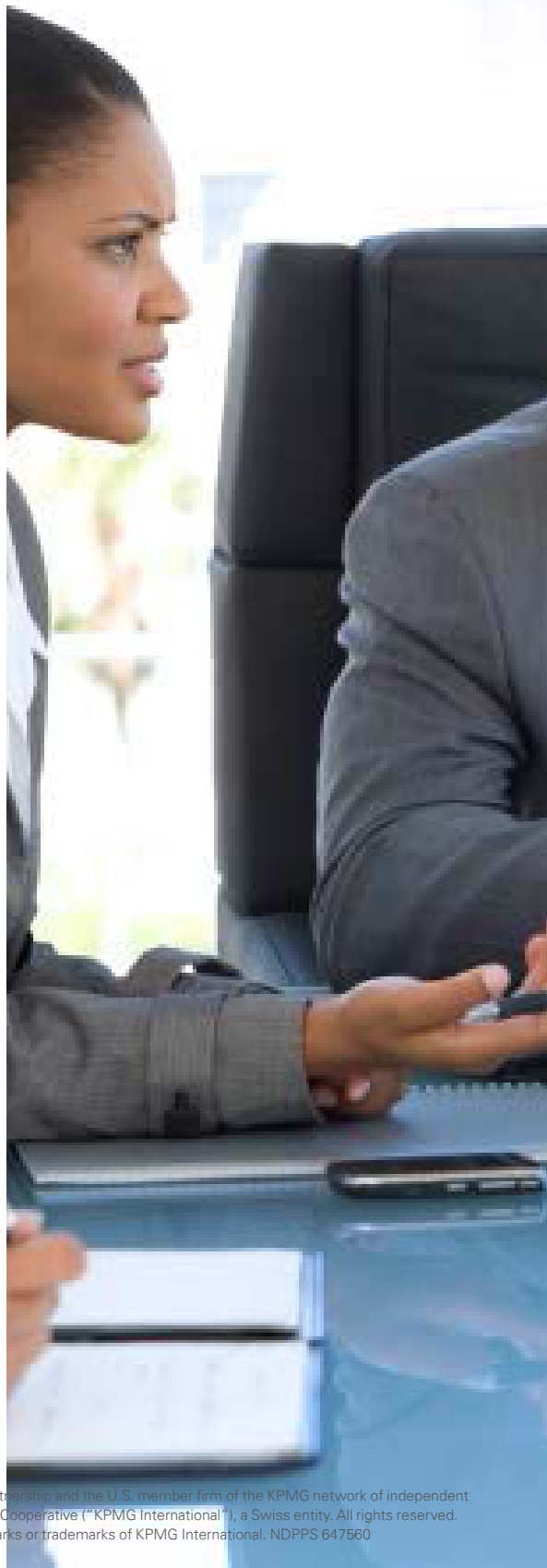
KPMG

Program requirements	Key considerations when establishing a program
 **Life cycle – Planning**	— Identify if the third party-relationship product/services align with the fourth-party strategy for allowing use of fourth party. — Identify if the third party engages fourth parties.
 **Life cycle – Due Diligence**	— Engage the fourth-party risk center of excellence to perform due diligence and risk assessment including: – Identifying and capturing the inventory of significant fourth parties – Applying risk rating to the significant fourth parties in scope – Performing specific fourth-party due diligence and risk assessment activities – Evaluating and risk assessing the third party's oversight program of fourth parties — Define a termination plan that includes consideration of critical fourth parties.
 **Life cycle – Contracting**	— Define standard clauses for inclusion in contracts related to appropriate use of fourth parties and communication when engaging or terminating significant fourth parties. — Define standard clauses for precluding use of fourth parties when the product/services don not meet risk appetite or strategy for allowing use of fourth parties. — Trigger unique contract clauses if proceeding with the third-party relationship when certain risks are identified without adequate due diligence or risk assessment results showing remediation of the risks. — Consider whether contracting directly with the fourth party is warranted. — Define and obtain appropriate approvals when risks are not adequately remediated or contract clauses/terms are not in alignment with defined protocols.
 **Life cycle – Ongoing Monitoring**	— Include a risk-based approach for repeating due diligence phase activities based upon the risk associated with the fourth-party use by the third party — Perform periodic monitoring of the third party's use of fourth parties, including: – Requiring updates from the third party for changes in use of fourth parties (including preapproval for new fourth parties providing significant services) – Requiring periodic review of the third parties' oversight program materials with targeted focus on critical fourth parties
 **Life cycle – Termination**	— Perform termination oversight related to sensitive data, customer interaction, etc., when third parties terminate use of a fourth party that was deemed critical. — Execute termination activities inclusive of oversight of the fourth party when terminating a third party that utilizes critical fourth parties.

Conclusion

Financial Service Institutions need to have a clear understanding of how services are delivered by third parties and where fourth parties play a key role in the delivery of the service.

Given the high regulatory expectations surrounding third party risk management and the inherent challenge of managing a party where there is no direct contract, it is reasonable to expect that FS institutions will require their third parties to demonstrate that they manage the fourth parties in a similar manner to them.



Contact

Greg Matthews
Partner
KPMG Advisory
T: 201-621-1156
E: gmatthews1@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia