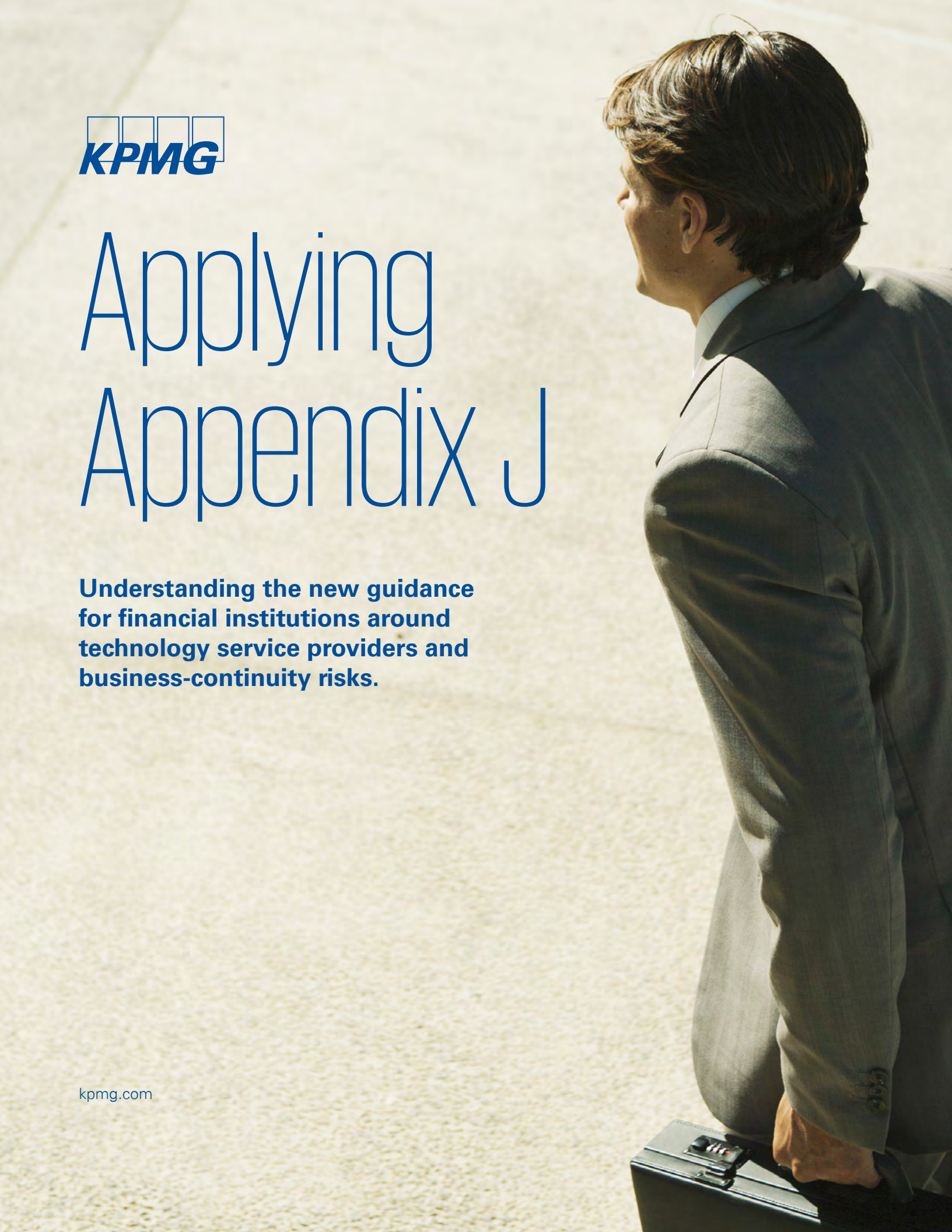

Applying Appendix J

Understanding the new guidance for financial institutions around technology service providers and business-continuity risks.

kpmg.com

The Federal Financial Institutions Examination Council (FFIEC) has issued guidance to help financial institutions (FIs) ensure their technology service providers (TSPs) have business-continuity procedures in place so that outsourced operations are secure and recoverable. The guidance, known as "Appendix J: Strengthening the Resilience of Outsourced Technology Services," highlights the following four elements:

— Adequate third-party risk management (TPRM) over the business continuity risks associated with any of the TSPs' subcontractors (i.e., fourth parties)

— Business continuity planning (BCP) that addresses the scenario of a significant disruption of a TSP (impacting services to multiple clients), including impact assessment and plans

— Validating business continuity plans through testing with the TSP to ensure strong TPRM

— BCP addressing cyber-events scenarios, including impact assessment and plans.

Because there has been an increased concentration of use of TSPs by multiple FIs or by multiple businesses within an FI, FIs should evaluate how a TSP's plans, from an infrastructure and resource perspective, account for a widespread disruption or outage.

Considerations about resiliency throughout the TPRM lifecycle for TSPs:

Planning: FIs evaluating new opportunities for technology outsourcing should review the risks related to the maturity of the new technologies they are considering. These include the risks and benefits around shared access to data, or the commingling of data with those of other FIs that may be vulnerable to hacking or to virtual-machine exploits or authentication risks, for example.

Due Diligence: Risk assessments and evaluations should include a review of the TSP's BCP program, along with its capabilities to support the FI's BCP needs (in other words, alignment to the FI's BCP program).

— If a TSP further subcontracts technology support and/or services, the TSP should perform a risk-based assessment and due diligence of the fourth party. The FI may also want to perform its own assessment and due diligence of the fourth party and consider making such fourth-party reviews part of its own TPRM program. Fourth-party access to data and environments should be a core component of the TSP's fourth-party oversight, especially when engaging foreign-based providers. In addition, the FI and TSP should pay greater attention to a fourth party's controls, which, if failed, would adversely affect the FI's or TSP's operations.

— The FI must understand and assess the TSP's testing strategy, which would include a review of prior testing results. This assessment would evaluate controls, including periodic management reporting (also assessing the level of reporting/escalation for adequacy).

— The FI should have a methodology to evaluate how well the TSP could support the FI's resilience objectives if the TSP's other clients were to be affected by a widespread disruption.

— The FI should review the TSP's financial viability to support the FI's strategic use of outsourced products or services.

— The FI should establish an exit strategy or termination plan according to various scenarios.

Contracting: Contractual requirements between the FI and the TSP should reflect the results of the planning and due diligence activities and any identified risks and control-performance expectations such as:

— Requirements related to the FI's BCP expectations, including defined recovery time/point objective, requirements for engagement/involvement in testing (including frequency of testing engagement), right to audit BCP strategy and execution, data governance, termination protocols, and minimum data security and confidentiality standards especially with foreign-based TSPs.

— Terms that define the actions or outcomes if BCP's expectations are not met.

— Clauses that clearly define responsibilities and accountabilities among the FI, TSP, and any fourth parties.

Ongoing Monitoring: A component of the TPRM program should include periodic assessment of the following activities:

— BCP controls, including reperformance of the due diligence activities (inclusive of financial viability review)

— The FI's validation of the BCP testing activities

— A review of independent assessments (internal/external) and management reporting (required by contract or otherwise) related to BCP performance and results

Any new risks to the FI should be evaluated and incorporated into future ongoing monitoring and contracts.

Termination: Considerations established during planning, due diligence, and contracting should enable effective termination. Beyond specific TSP termination requirements, the FI's TPRM and BCP programs should also include a standard process to follow when terminating TSPs.

Integration of the FI's TPRM and BCP Programs

A service or activity that is outsourced to a third party doesn't exempt that service or activity from an organization's BCP program.

FIs should align their risk-rating methodologies among their TPRM and BCP programs. That alignment will be beneficial for demonstrating a comprehensive risk-based approach to TSP involvement in the BCP activities.

The testing of BCP activity should be defined based on a risk-based methodology. At the higher risk levels, FIs should require that TSPs support FI participation in the TSP's BCP testing activities. Furthermore, FIs should evaluate the TSP's BCP program design and effectiveness to meet the FI's BCP requirements.

To ensure effective testing of TSPs, the BCP scenarios should be TSP specific and should demonstrate the ability for systems failover to restore normal operational activities. The scenarios FIs should consider include:

— Failure and recovery of one or both of FI/TSP, including when the TSP is unable to recover

— Cyber event occurrence and response/recovery (planning and consideration of the increasing cyber risks should be a core aspect of an integrated BCP–Cyber–TPRM program)

— Failover to any back-up third-party providers not engaged during normal production

— Dependencies among systems, processes, departments, or third parties.

When conflicts with the TSP's schedule prevent an FI from testing as frequently as required according to its BCP or TPRM program risk-rating methodology, the FI should require (contractually) that the TSP provide documentation related to their ongoing BCP testing activities, including coverage and results of tests. The FI should evaluate those results and determine if any adverse results warrant escalation according to its BCP or TPRM program requirements.

Whether deficiencies are identified through review of TSP, BCP results or through participation in testing activities by the FI or by the TSP, action plans should be defined and tracked to completion with defined approval and escalation protocols outlined in the BCP and TPRM programs.

Conclusion:

In addition to FIs being responsible for ensuring their own business continuity plans and testing protocols to address operational failure and recovery scenarios, they must also:

— Assess the effectiveness of its TSPs business continuity program focusing on their ability to meet the FI's RTOs, RPOs and capacity;

— Define terms of service in written contracts which are reviewed by the FI's legal counsel and subject-matter professionals; and

— Effectively monitor TSP performance throughout the life of the contract, including the termination of the contract as well as the use of subcontractors.

The above requirements are in addition to the typical BCP fundamentals of alternate TSPs and comprehensive testing. In conclusion, when engaging TSPs to provide systems, software, or processes in the conduct of normal business, FIs must ensure TSPs adequately provide resiliency for the FI's processes. FIs must align their BCP and TPRM programs to ensure they provide adequate, risk-based coverage of higher risk processes and third parties.

Note: Appendix J added cyber attacks to the traditional adverse events as natural disasters, infrastructure failure, technology failure, and availability of staff. FIs and TSPs are to include this potential impact and ensure appropriate resilience capabilities are established and implemented. Solutions can include reviewing policies and procedures to minimize insider threats, using multi-layered anti-malware strategies, addressing any gaps with data and/or online backups architectures and technology, as well as identifying and correcting any single points of failure with communication providers. cyber attacks have become a constant and growing threat to most organizations, and as a result Incident Response Teams have been established to prepare for and respond to cyber events.

Contact

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

Tony Buffomante
Principal, KPMG Cyber Security Services
T: 312-665-1748
E: abuffomante@kpmg.com

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

kpmg.com/socialmedia