VendorINSIGHT COMPLIANCE UPDATE

Spring 2015

VendorINSIGHT® is the industry-leading solution for financial institutions offering the most features and capabilities for vendor risk monitoring.

Business Resilience Management: Transforming the Landscape for Vendor Management

Vendor Management Programs Impacted by New FFIEC Updates to IT Examination Handbook for Business Continuity Planning and Disaster Recovery

On February 6, 2015, FFIEC issued a revised Business Continuity Planning booklet with a new appendix titled *Strengthening the Resilience of Outsourced Technology Services*. Much of the new appendix is dedicated to the importance of having a framework to identify, measure, monitor and mitigate the risks associated with outsourcing to third-party technology service providers (TSPs). The appendix further emphasizes the critical nature of fourth-party relationships (e.g, subcontractors utilized by a third party) and their importance in the overall risk management framework.

This new emphasis and new guidance comes as no surprise. Early last year, a number of bank examiners and regulators present at industry conferences were citing facts and figures that highlighted the importance and criticality of reliable, tested recovery plans and the essential need to better manage third and fourth party relationships through vendor management programs. Regulators noted that more than one half of investigated third party failures stemmed from failures at the fourth party level and were related to inadequate BCP/DR resiliency preparedness.

VendorINSIGHT® has reviewed the guidance and has included several suggestions and commentary related to the new guidance in the sidebar to the original text below.

NEW!
BCP-INSIGHT™ software offers integrated business risk management capabilities with VendorINSIGHT®

BCP-INSIGHT™, a cost-effective and full-featured system for Business Continuity and Planning and Disaster Recovery, is now fully-integrated with VendorINSIGHT®!

In January 2015, VendorINSIGHT® announced full integration and compatibility to BCP-INSIGHT™, our patent-pending solution that helps financial institutions analyze third party vendor risk and business process recovery risk side-by-side. The system includes:

- Recovery document storage and maintenance;
- Business process recovery risk ratings; and
- Threat scenario definitions

Please contact your Program Administrator for more information. We expect this topic to continue to evolve over the coming year and we are likely to see new guidance updated in Federal Reserve, FDIC, OCC and CFPB documents in the months ahead.

VendorINSIGHT®
2645 Erie Ave.
Suite 51
Cincinnati, OH 45208

1-877-997-2674

www.vendorinsight.com

VendorInsight

VendorINSIGHT COMPLIANCE UPDATE

Message in a Bottle?

In order to help you understand the new guidance, we open the bottle, read what the FFIEC is saying and point you to the features in VendorINSIGHT® and BCP-INSIGHT™ that can help you achieve 100% compliance.

Look for new terms such as *Business Resilience* and learn why all financial institutions must critique the BCP planning, testing and results of their third party technology service providers.

Visit http://www.vendorinsight.com or http://www.bcpinsight.com for more information.

FFIEC Business Continuity Planning Handbook Update
Appendix J: Strengthening the Resilience of Outsourced Technology Services

Background and Purpose
Many financial institutions depend on third-party service providers to perform or support critical operations. These financial institutions should recognize that using such providers does not relieve the financial institution of its responsibility to ensure that outsourced activities are conducted in a safe and sound manner. The responsibility for properly overseeing outsourced relationships lies with the financial institution's board of directors and senior management. An effective third-party management program should provide the framework for management to identify, measure, monitor, and mitigate the risks associated with outsourcing.[1]

When a financial institution relies upon third parties to provide operational services, they also **rely on those service providers to have sufficient recovery capabilities for the specific services they perform** on behalf of the financial institution. In addition to providing systems and processing, technology service providers (TSPs) may also be retained by a financial institution to provide information technology (IT) recovery capabilities for the financial institution's internal systems. Effective business continuity planning (BCP) and testing demonstrate the financial institution's ability not only to recover IT systems, but also to **return critical business functions to normal operations within established recovery time objectives (RTOs)**. A financial institution should be able to demonstrate the ability to recover critical IT systems and resume normal business operations **regardless of whether the process is supported in-house or at a TSP for all types of adverse events (e.g., natural disaster, infrastructure failure, technology failure, availability of staff, or cyber attack[2]).**

This appendix discusses four key elements of BCP that a financial institution should address to ensure they are contracting with TSPs that are strengthening the resilience of technology services:

- Third-party management addresses a financial institution management's responsibility to control the business continuity risks associated with its TSPs and their subcontractors.
- Third-party capacity addresses the potential impact of a significant disruption on a third-party servicer's ability to restore services to multiple clients.
- Testing with third-party TSPs addresses the importance of validating business continuity plans with TSPs and considerations for a robust third-party testing program.
- Cyber resilience covers aspects of BCP unique to disruptions caused by cyber events.

VendorINSIGHT® leads the industry in automation, features and 100% compliance with all existing regulatory guidance from Federal Reserve, FFIEC, FDIC, OCC, CFPB, GLBA, and NCUA.

Key features are highlighted below that help VendorINSIGHT® customers meet the prescribed requirements.

The Vendor Relationship Profile (VRP) in VendorINSIGHT® helps identify third parties that are critical to essential business operations.

The VRP profile is automatically linked to a proprietary matrix of Due Diligence requirements. A review of BCP/DR preparedness, testing and outcomes is an essential component of the due diligence framework.

The Policy Compliance Module (PCM) ensures that the appropriate BCP/DR review is completed and documented in the system.

When coupled with the BCP-INSIGHT™ system, management is able to link key technology vendors with processes and the probabilistic events that might adversely affect business continuity. An integrated view of risk is essential for compliance with this new guidance.

Third-Party Management
Establishing a well-defined relationship with TSPs is essential to business resilience. A financial institution's third-party management program should be risk-focused and **provide oversight and controls commensurate with the level of risk presented by the outsourcing arrangement.** To ensure business resilience, the program should include outsourced activities that are critical to the financial institution's ongoing operations. Attention to due diligence, contract management, and ongoing monitoring of TSPs is important to maintaining business resilience. The FFIEC IT Examination Handbook's "Outsourcing Technology Services Booklet" addresses expectations for managing third-party relationships. This section of the appendix focuses on business-resiliency aspects of third-party management.

Due Diligence
A financial institution should evaluate and perform thorough due diligence before engaging a TSP. A financial institution should consider the maturity of new technologies and gain an understanding of the benefits and risks of engaging TSPs using such technologies during the due diligence process. Improvements in technologies have the potential to strengthen business resilience, but may introduce new and different risks (e.g., shared access to data, virtual exploits, and authentication weaknesses). **As part of its due diligence, a financial institution should assess the effectiveness of a TSP's business continuity program, with particular emphasis on recovery capabilities and capacity.[3] In addition, an institution should understand the due diligence process the TSP uses for its subcontractors and service providers. Furthermore, the financial institution should review the TSP's BCP program and its alignment with the financial institution's own program, including an evaluation of the TSP's BCP testing strategy and results** to ensure they meet the financial institution's requirements and promote resilience.

Contracts
The terms of service should be defined in written contracts[4] that have been reviewed by a financial institution's legal counsel and subject matter experts before execution. **Contract terms that can impact the financial institution's ability to ensure effective business resilience** include the following:

- Right to audit: Agreements should provide for the right of the financial institution or its representatives to audit the TSP and/or to have access to audit reports. A financial institution should review available audit reports addressing TSPs' resiliency capabilities and interdependencies (e.g., subcontractors), BCP testing, and remediation efforts, and assess the impact, if any, on the financial institution's BCP.
- Establishing and monitoring performance standards: **Contracts should define measurable service level agreements (SLAs) for the services being provided.** For business continuity expectations, clear recovery time objectives and recovery point objectives (RPOs) should be addressed.
- Default and termination: Contracts should define events that constitute contractual default (e.g., the inability to meet BCP provisions, SLAs, and/or RTOs) and provide a list of acceptable remedies and opportunities for curing a default.
- Subcontracting: If agreements allow for subcontracting, the TSP's contractual provisions should also apply to the subcontractor. Contract provisions should clearly state that the primary TSP has overall accountability for all services that the TSP and its subcontractors provide, including business continuity capabilities.

The Vendor Relationship Profile (VRP) in VendorINSIGHT® ensures that business resiliency and BCP/DR is a required part of the due diligence and contracting framework for outsourced activities that are critical to operations.

The VRP and the more formal Vendor Risk Assessment (VRA) templates in VendorINSIGHT® provide a best-in-class framework for evaluating the alignment and effectiveness of a third party's BCP program.

VendorINSIGHT® customers can subscribe to BCP/DR review assessment reports for their key vendors. These reports are prepared and published by VendorINSIGHT® as a part of a complete menu of Vendor Evaluation Services available with the VendorINSIGHT® program.

A complete contract checklist is available in the VendorINSIGHT® system that already includes ALL of these recommended checklist items.

Contractual SLAs with vendors can be systematically linked into all performance reviews in the VendorINSIGHT® system.

In the VendorINSIGHT® system this contract checklist can be directly associated to a financial institution's policy requirement to address these items and demonstrate that the financial institution properly considered each BCP/DR element for business resiliency with its third party service providers.

Agreements should define the services that may be subcontracted, the TSP's due diligence process for engaging and monitoring subcontractors, and the notification requirements regarding changes to the TSP's subcontractors. The contractual provisions should also address the right to audit and BCP testing requirements for subcontractors. Additionally, agreements should include the TSP's process for assessing the subcontractor's financial condition.

- Foreign-based service providers: A financial institution should review data security controls of foreign-based TSPs or foreign-based subcontractors that back up and/or store data offshore. Because information security and data privacy standards may be different in foreign jurisdictions, the contract should clearly address the need for data security and confidentiality to, at a minimum, adhere to U.S. regulatory standards.

- BCP testing: Contracts should address the financial institution's BCP testing requirements[5] for the TSPs. The contract should define testing frequency and the availability of test results. The contract should also include the financial institution's ability to participate in the TSP's BCP testing on a periodic basis.[6]

- Data governance: Contracts should clearly define data ownership and handling expectations during the relationship and following the conclusion of the contract. This may include data classification, integrity, availability, transport methods, and backup requirements. In addition, expectations for data volume and growth should be addressed.

- TSP updates: Contracts should empower a financial institution to request information from its service provider(s) describing the TSP's response to relevant regulations, supervisory guidance, or other notices published by any of the federal banking agencies.

- Security issues: Contracts should clearly state the responsibility of the TSP to address security issues associated with services and, where appropriate, to communicate the issue(s) and solution(s) to its financial institution clients. Additionally, responsibilities for incident response should be incorporated. The contract should include notification responsibilities for situations where breaches in security result in unauthorized intrusions to the TSP that may materially affect the financial institution clients.

Noted as above, a complete contract checklist is available in the VendorINSIGHT® system that already includes ALL of these recommended checklist items.

Using VendorINSIGHT® this contract checklist can be linked to the financial institution's policy requirement to address these items and serves to demonstrate that the financial institution properly considered each BCP/DR element for business resiliency with its third party service providers.

Ongoing Monitoring

Management should effectively monitor TSP performance throughout the life of the contract. Effective ongoing monitoring assists the financial institution in ensuring the resilience of outsourced technology services. **The financial institution should perform periodic in-depth assessments of the TSP's control environment, including BCP,** through the review of service provider business continuity plan testing activities, independent and/or third party assessments[7], and management information systems (MIS) reports[8] to assess the potential impact on the financial institution's business resilience. The financial institution should ensure that results of such reviews are documented and reported by the TSP to the appropriate management oversight committee or the board of directors and used to determine any necessary changes to the financial institution's BCP and, if warranted, the service provider contract.

BCP reviews are already an integral part of the due diligence and review framework in VendorINSIGHT®.

Strategic Considerations - Third-Party Management
Financial institution management should ensure business resilience considerations are **embedded within their third-party risk management life cycle. This includes addressing business continuity elements within the due diligence process, contract negotiations, ongoing monitoring processes, and processes for termination of the contract. This should also include considerations relative to service providers' use of subcontractors.** Finally, the oversight and controls on outsourced activities should be commensurate with the level of risk presented by these arrangements.

The financial institution should ensure that each TSP has a robust third-party management program that includes a review of each subcontractor's business continuity plan. The failure of a subcontractor could result in the failure of the TSP's ability to provide contracted services.

Third-Party Capacity
An increasing concentration risk corresponds to financial institutions' increased use of third-party service providers. That, in conjunction with industry consolidation, has resulted in fewer, more specialized TSPs providing services to larger numbers of financial institutions. This trend increases the potential impact of a scenario in which a TSP is required to support recovery services to large numbers of financial institutions due to a widespread disaster. In addition, a business disruption at a single TSP may affect critical services provided to a large number of institutions dependent on those services. **In both scenarios, it is critical that the TSP have sufficient capacity to meet RTOs and RPOs needed by the financial institution clients.**

As reliance on technology increases, a financial institution is less able to withstand the absence of a critical serviced function. Outsourcing diminishes the IT self-sufficiency of financial institution staff because of the increased dependence on the TSP for technical support. The increased reliance on technology for all daily processes means it is no longer feasible for a financial institution to operate manually for an extended length of time. Additionally, because TSPs operate many critical processes, it is difficult for a serviced client to quickly move these processes internally or to another TSP.

Significant TSP Continuity Scenarios
The significant size and client concentration of larger TSPs increases the potential impact of service disruptions across major segments of the financial industry, increasing the importance of resilience for these organizations. Natural disasters, physical threats, and cyber attacks could have a significant effect on servicer capabilities. Beyond physical and cyber threats, financial pressures can lead service providers to make decisions not to invest fully in appropriate security controls or resilience measures that would facilitate continuity of operations. In cases of extreme financial distress, it may not be financially viable for a servicer to continue making necessary product updates, or even to continue operations. Without advance notice or awareness of deterioration in a TSP's financial condition, the financial institution clients might not have appropriate time to make alternate processing arrangements.

BCP reviews are already an integral part of the due diligence and review framework in VendorINSIGHT® for customers using the automated VRP and PCM modules, or for those subscribed to the Vendor Evaluation Reports for BCP/DR.

In early 2013, VendorINSIGHT® updated its template standards to include the identification, management, notification and monitoring of subcontractors (4th parties) in third party vendor relationships. These remain a part of the automated vendor assessment.

Enhancements to the scoring template and question set in the VRA (Vendor Risk Assessment) were recently made to address the concept of a large-scale recovery effort that might fully utilize the recovery capacity of a third party service provider. The concept of "recovery capacity" is a new concept introduced with this guidance.

TSP Alternatives
It is incumbent on financial institutions and third-party service providers to i**dentify and prepare for potentially-significant disruptive events, including those that may have a low probability of occurring but would have a high impact on the institution.** In spite of such planning, there may be circumstances that cause a service to be unavailable for longer than a committed and tested RTO. In these situations, a financial institution and its TSPs should assess the impact on their respective customers and take the necessary steps to minimize the impact of the event. In extreme scenarios, where a TSP can no longer effectively perform its responsibilities, a new TSP may have to assume operations. Depending upon the specific circumstances, a new TSP may convert the financial institution to its systems and move them to its data center. Alternatively, the new TSP could assume control of the existing data center running the existing systems. If no alternate TSP is available, the financial institution may have to move the operations in-house. The latter is generally not a valid option, as the reasons to outsource include a lack of expertise or financial resources to run services in-house and, therefore, moving them with little or no notice would exacerbate these limitations.

If operations at a TSP cease, for most applications, the length of time required to convert a financial institution to an alternate system would greatly exceed any reasonable RTO for an application that abruptly ceased. There are three possible solutions in the event of a TSP failure. The first is for the financial institution clients of a failed service provider to assume the operation of the service either by contracting with an alternate TSP or performing the services themselves at the existing site. This would require a steep learning curve for the new TSP or the financial institution clients taking over the application. Second, the financial institution clients could convert to an alternate TSP's application. There would still be a delay, however, as they would need to prepare infrastructure at the new site, convert data if necessary, and perform functional testing before resuming the service. The third solution would be to move the existing critical infrastructure to an alternate TSP that could successfully and securely take over and run the application or service at its site. This assumes that the alternate TSP would not be affected by the situation that prevented the original TSP from fulfilling its servicing responsibilities and that the alternate TSP would have the necessary expertise to provide the service.[9] Regardless of the option selected, the ability of an alternate TSP or the financial institution clients to take over processing responsibilities assumes the following items. The problem TSP's data center has workable backup systems or infrastructure that would facilitate transition to an alternate TSP. The alternate TSP (or the financial institution clients) has sufficient capacity in space, systems, and personnel to deliver the service effectively.

A financial institution should have contingency plans in place to address alternatives for the resilience of services supporting critical operations if the current TSP cannot continue to provide the service. These plans should identify alternate TSPs or in-house arrangements and preparations required for such a conversion to the extent possible.

Strategic Considerations - Third-Party Capacity
A critical failure at a service provider potentially could have large-scale consequences. A financial institution should ensure that its TSPs have adequate planning and testing strategies that address severe events in order to identify single points of failure that would cause wide-scale disruption. Given the increased concentration of providers in the TSP industry, a financial institution should ensure that it has identified, and potentially prearranged, a comprehensive set of alternative resources to provide full resilience of operations in such scenarios.

There are certain steps a financial institution can take with their TSPs to

The BCP-INSIGHT™ and VendorINSIGHT® systems enable scenario-based probabilities to be assigned to various types of business process disruptions.

The BCP-INSIGHT™ system evaluates each business process against a multi-factor scoring matrix that includes RTO (MAD proxy) and IMPACT. Additionally, recovery complexity is assessed as a part of the Process Vulnerability Rating established for the business process.

Through the linkages to VendorINSIGHT®, a financial institution can determine which third party service providers are associated with resilient or non-resilient business processes.

Recovery complexity is assessed as a part of the Process Vulnerability Rating established for each business process in BCP-INSIGHT™.

The current VRA framework in VendorINSIGHT® already encompasses the identification of third party provided services that are replicable either with another provider or that could be brought in house. These assessments and classifications alter the risk score for each vendor and direct management to additional due diligence steps.

plan for the possible failure of critical services. First, the parties can discuss scenarios of significant disruptions that may necessitate transitioning critical services to alternate TSPs. Second, the parties can assess their immediate or short-term space, systems, and personnel capacity to absorb, assume, or transfer failed operations. Last, the parties can identify the most plausible range of recovery options and develop business continuity plans that address restoration of key services. FFIEC member agencies encourage larger, more complex financial institutions and TSPs to consider industry-wide recovery scenarios that strengthen the resilience of the financial services sector. Institutions of all sizes should consider methods to participate through user groups or industry initiatives to test recovery scenarios.

Testing With Third-Party TSPs

Testing is a critical step in the cyclical BCP process and should be sufficient in scope and rigor to demonstrate the ability to meet recovery objectives, regardless of whether a service is performed in-house or is outsourced. **Third parties provide important services to many financial institutions and as such should be included within the financial institution's enterprise-wide business continuity testing program. The testing program should be based on a financial institution's established risk prioritization and evaluation of the criticality of the functions involved.** Testing with third parties should disclose the adequacy of both organizations' ability to recover, restore, resume, and maintain operations after disruptions, consistent with business and contractual requirements.

This booklet discusses expectations, governance, and other attributes of an effective BCP testing program and includes an appendix dedicated to governance and attributes of a testing program.[10] In addition, the FFIEC IT Examination Handbook's "Outsourcing Technology Services Booklet" addresses third-party testing considerations. Financial institutions and third parties should apply the concepts from both booklets to their programs for BCP testing with third parties.

Third-party TSPs typically provide services to more than one financial institution, and the largest providers may service hundreds of institutions. When the volume of clients is large, a TSP may not be able to test with all clients in a set period (e.g., annually). A financial institution, however, should be proactive in managing its third-party relationships, including addressing its testing expectations. A financial institution should ensure it is an active participant in its TSPs' testing programs and that these providers have a testing strategy that includes testing plausible significant disruptive events. Because a provider may not be able to test with all clients on a regular basis, financial institutions should register on any waiting list with the TSP. In the interim, financial institutions should obtain documentation on the scope, execution, and results of testing activity conducted for the services they receive. Any test results that impact the financial institution are to be provided to the board. A financial institution should ensure that it understands its TSP's testing process to ensure that the testing is adequate to meet its continuity expectations.

If a third party provides critical services, the financial institution should conduct periodic BCP testing with reasonable frequency. As noted in the FFIEC IT Examination Handbook's "Outsourcing Technology Services Booklet," critical services require annual or more frequent tests of the contingency plan. **As with all BCP testing, the frequency should be driven by the financial institution's risk assessment, risk rating, and any significant changes to the operating environment.** To the extent that a test is unsuccessful, any issues identified should be tracked and resolved in a timely manner, according to the severity of the issues. The scope of BCP testing with third parties should be commensurate with the level and criticality of services provided and, in some cases, requires an end-to-end exercise. Finally, the right to perform or participate in BCP testing with third parties should be described within the contract governing the third-party relationship.

The BCP-INSIGHT™ system allows third parties to participate in the online tabletop tests run by a financial institution.

The BCP-INSIGHT™ system provides a template to evaluate each business process against a multi-factor scoring matrix that includes RTO (MAD proxy) and IMPACT. This provides prioritization for the financial institution.

Recovery complexity is assessed as a part of the Process Vulnerability Rating established for each business process in BCP-INSIGHT™.

All BCP testing and review requirements in VendorINSIGHT® are systematically linked to the risk rating ensuring that this compliance requirement is met.

Testing Scenarios

A financial institution should develop plausible and realistic scenarios of threats that may potentially disrupt business processes and the financial institution's ability to meet both business requirements and customers' expectations. These scenarios should include those threats that may affect services provided by third parties to test the incident response plan and crisis management, including communication processes with third-party providers and other applicable stakeholders. Testing should demonstrate not only the ability to failover to a secondary site but also the ability to restore normal operations. **In addition, the financial institution should develop appropriate scenarios to test their response in the event of a significant event or crisis at the TSP. Scenarios to consider include:**

- TSP outage or disruption, resulting in activation of the third party's alternative recovery arrangements. In this scenario, the third party is demonstrating recovery from an outage while the client financial institution has not been directly affected, but the TSP may require some response from the client if auto-failover is not used (e.g., changing telecommunication lines or providers).
- Financial institution outage or disruption. In this scenario, the TSP has not been directly affected but has to react to address the client's recovery activities and needs.
- Cyber events demonstrating the financial institution's and third-party provider's ability to respond quickly and efficiently to such an event. For example, a financial institution's ability to recover from a disruption of critical functions because of a distributed denial of service (DDoS) attack or the ability to recover from a data corruption event should be subject to testing. A financial institution may consider working with an outside party, such as other financial institutions or an industry group, to test these types of events.
- Simultaneous attack affecting both the institution and its provider.

Testing Complexity

A financial institution should develop testing strategies that demonstrate its ability to support connectivity, functionality, volume, and capacity using alternate facilities. The testing strategies should encompass internal and external dependencies, including activities outsourced to domestic and foreign-based TSPs. **Lessons learned from natural disasters and other events highlight that simple testing of network connectivity with a third party is not adequate. For critical business functions, test strategies and plans should be extended beyond third-party network connectivity and include transaction processing and functionality testing to assess infrastructure, capacity, and data integrity. Documenting transaction flows, as well as developing formal process diagrams or charts, may help ensure that testing effectively identifies interdependencies and end-to-end processes.**

In striving to increase the effectiveness of test scenarios over time, the financial institution should, as appropriate, consider the following:

- Performing integrated tests or exercises that incorporate more than one system or application, as well as external dependencies, to gauge the effectiveness of continuity plans for a business line or major function.
- Testing interdependencies where two or more departments, business lines, processes, functions, and/or third parties support one another.
- Conducting end-to-end exercises to demonstrate the ability of the financial institution to recover a business process from initiation (e.g., customer contact) through process finalization (e.g., transaction closure), including functions provided by a TSP.
- Conducting full-scale exercises that involve recovery of systems and applications in an interactive manner in a recovery environment, including all critical functions and modules provided by a TSP.
- Performing exercises that include the financial institution's third-party provider's subcontractors, vendors, or servicers.

A review of a third party's BCP/DR testing and test results should give consideration to the comprehensiveness and appropriateness, which embodies these variations listed at the left.

VendorINSIGHT's Vendor Evaluation Reports provide the analysis and detail needed to understand whether the vendor is sufficiently testing its recovery capabilities at the various points of failure that could occur.

The BCP-INSIGHT™ system enables easy identification of process interdependencies to facilitate BCP/DR test planning and execution.

The availability and proprietary indexing of recovery documentation and technology reference material in the BCP-INSIGHT™ system provides easy access from any location during a test or real life recovery event to ensure a sustainable recovery and reliable business resiliency.

By increasing the scope and effectiveness of testing with TSPs over time, a financial institution should achieve a robust third-party testing program that includes the financial institution's recovery capabilities. Increasing test complexity helps identify weaknesses in the financial institution's business continuity plan. Financial institution management should ensure that any issues identified with either their recovery capabilities or those of their TSPs are documented with action plans and target dates for resolution.

Strategic Considerations - Testing With TSPs
Testing with third parties involves challenges because of the number of clients being serviced and the TSP's need to maintain daily operations. There are a number of strategic objectives, however, that a financial institution needs to address in an effective third-party BCP testing program.

A client financial institution needs assurance that its third-party service providers have the necessary capacity to restore critical services in the event of a widespread disruption or outage. This assurance includes adequate infrastructure and personnel to restore services to financial institution clients and support typical business volumes. Clients gain assurance through an effective BCP testing program.

Because not all clients can participate in every testing activity, TSPs should be transparent about testing activities and results and should provide information that facilitates third-party relationship monitoring. Service providers should share test results and reports, remediation action plans and status reports on their completion, and related analysis/modeling. In most instances, proxy testing[11] will not fully capture each financial institution's unique operational needs; therefore, each financial institution should participate in its TSP's BCP testing program when possible. Appropriate testing for the most likely significant disruptive scenarios provides assurances that financial institutions and service providers will be better prepared to recover from these events.

VendorINSIGHT® Vendor Evaluation Reports provide the analysis and detail needed to understand whether the vendor is sufficiently testing its recovery capabilities at the various points of failure that could occur.

Following testing, the financial institution should evaluate the results and understand any gaps that may exist between the service provider and the institution. A plan should be developed to ensure these gaps are addressed as appropriate.

Cyber Resilience
The increasing sophistication and volume of cyber threats and their ability to disrupt operations or corrupt data can affect the business resilience of financial institutions and TSPs. **Financial institutions, and their TSPs, need to incorporate the potential impact of a cyber event into their BCP process and ensure appropriate resilience capabilities are in place.** The changing cyber threat landscape may include the following risks that must be managed to achieve resilience.

Enhancements to the scoring template and question set in the VRA (Vendor Risk Assessment) in VendorINSIGHT® were recently made to address validation of third party dialogue and planning for Cyber Resilience. The concept of "Cyber Resilience" is a new concept introduced with this guidance.

Risks-
Malware
Malware represents a serious and growing threat to financial institutions and TSPs as it is focused on achieving high-impact objectives, such as data corruption and unauthorized financial transactions. Anti-malware vendors are continually challenged to keep pace with rapidly proliferating malware threats. For example, "zero-day"[12] exploits can result in significant damage. To strengthen resilience against malware threats, financial institutions and TSPs should use a layered anti-malware strategy, including integrity checks, anomaly detection, system behavior monitoring, and employee security awareness training, in addition to traditional signature-based anti-malware systems. Resilience also calls for the more common controls, such as strong passwords, appropriately controlled mobile devices, controls over access to social networks, hardened[13] software and operating systems, and controlled and monitored Internet access.

Insider Threats
Cyber threats can be launched from within a financial institution or TSP by a disgruntled employee or a person placed in the financial institution deliberately to carry out a cyber attack. The financial institution should consider the possibility that a knowledgeable insider may cause a disruptive event and the potential impact of the event on business resilience. Employee screening, dual controls, and segregation of duties are some examples of controls that can help to mitigate the risks of an insider attack.

Data or Systems Destruction and Corruption
A cyber attack may simultaneously target production data and online backups for destruction or corruption. It may also target the destruction of hardware. Data destruction occurs when data are erased or rendered unusable. Data corruption occurs when data are altered without authorization. Either can occur inadvertently or through malicious intent. In some cases of data corruption, data may appear usable but produce unexpected and undesirable results. A financial institution or TSP may not become aware that data has been corrupted for some period of time after an event, and may find it difficult to determine the extent of the problem. Thus, data corruption may have a greater impact on the financial institution and require a different recovery response than cases of data destruction.

Data replication can be an effective strategy for rapid recovery in the event of data destruction or data corruption. Data replication, however, may also be susceptible to simultaneous cyber attacks, and using this replication strategy may inadvertently result in backup or replicated data being destroyed or corrupted along with the production data. For effective business resilience, the financial institution and TSP should take steps to ensure that replicated backup data cannot be destroyed or corrupted in an attack on production data. If data are replicated in near real time, the financial institution and service provider should consider the vulnerability of their backup systems to an attack that impacts both simultaneously. Management at the financial institution and the TSP should ensure appropriate redundancy controls and segregation of replicated backup data files to provide for sufficient recovery capabilities against these threats.

Another control for consideration is an "air-gap," a security measure in which a computer, system, or network is physically separated from other computers, systems, or networks. An air-gapped data backup architecture limits exposure to a cyber attack and allows for restoration of data to a point in time before the attack began. Alternatively, a periodic read-only data backup entails the transmission of data to a physically and logically separate read-only backup location. These and other emerging data backup techniques address cyber attacks and mitigate the risk of corrupt data being replicated.

The objective of these strategies is to allow financial institutions and TSPs to maintain relatively current data backups without the risk of an attack destroying or corrupting the backup data. Financial institutions and TSPs should develop specific procedures for the investigation and resolution of data corruption in response and recovery strategies. Also, financial institutions and TSPs should ensure that data integrity controls[14] are in place to detect possible corruption in production and backup data.
Some financial institutions have deployed cloud-based disaster recovery services[15] as part of their resilience program. These services have unique data integrity risks and, therefore, financial institution management should assess services before implementation and reassess them periodically after deployment, as the technology, capability, and threats change. Financial institutions should ensure that cloud-based disaster recovery services protect against data destruction or corruption with the same level of assurance as non-cloud-based disaster recovery solutions. Financial institutions and their TSPs should ensure that appropriate security is in place for virtualized[16] cloud recovery services.
In addition, financial institutions and TSPs should have plans and processes to reconstitute their operations after a destructive attack.

Communications Infrastructure Disruption
Cyber attacks, such as DDoS attacks, can be used to disrupt communications and may target underlying infrastructures directly. Financial institutions' business resilience strategies depend on functioning communication links between various entities, including TSPs. The following possible scenarios could jeopardize ongoing operations:

- Reliance on a single communications provider, potentially creating a single point of failure.
- Disruptions that affect multiple financial institutions due to TSP concentration.
- Simultaneous disruptions of telecommunications and electronic messaging due to the convergence of voice and data services in the same network.
- Disruption of data and voice communications between other entities and TSPs.

A financial institution should recognize these possible scenarios and plan for alternate communications infrastructure, if available. FFIEC member agencies recognize that it may be difficult to achieve complete data communications resilience through independent redundant infrastructure, but the financial institution should explore alternatives.

Simultaneous Attack on Financial Institutions and TSPs
Business continuity plans frequently rely on the fact that production and backup facilities are separated by geography, such that a disaster in one geographic area will not affect a backup facility located a sufficient distance away. Cyber attacks, however, are not limited by geography and can target facilities located anywhere in the world. For example, a cyber attack can be directed against a financial institution's production and backup facilities simultaneously, rendering both inoperable. Similarly, a cyber attack could target both a financial institution and its TSPs. Cyber attacks may also be executed in conjunction with disruptive physical events and may affect multiple critical infrastructure sectors (e.g., the telecommunications and energy sectors). Financial institutions and TSPs should consider their susceptibility to simultaneous attacks in their business resilience planning, recovery, and testing strategies.

Strategic Considerations - Cyber Resilience
The ability of financial institutions and TSPs to respond effectively to a cyber attack is critical to business resilience. The financial institution should consider the following mitigating controls:

- Data backup architectures and technology that minimize the potential for data destruction and corruption;
- Data integrity controls, such as check sums;
- Independent, redundant alternative communications providers;
- Layered anti-malware strategy;
- Enhanced disaster recovery planning to include the possibility of simultaneous attacks;
- Increased awareness of potential insider threats;
- Enhanced incident response plans reflecting the current threat landscape; and
- Prearranged third-party forensic and incident management services.

Financial institutions and **TSPs should consider the cyber risks and controls discussed above, incorporate them into their BCP, as appropriate, and periodically test their ability to resume normal operations after a cyber attack.**

Cyber threats will continue to challenge business continuity preparedness. Financial institutions and TSPs should remain aware of emerging cyber threats and scenarios and consider their potential impact to operational resilience. Because the impact of each type of cyber event will vary, preparedness is the key to preventing or mitigating the effects of such an event.

Enhancements to the scoring template and question set in the VRA (Vendor Risk Assessment) in VendorINSIGHT® were recently made to address validation of third party dialogue and planning for Cyber Resilience. The concept of "Cyber Resilience" is a new concept introduced with this guidance.

Incident Response
Financial institutions and their **service providers should anticipate potential cyber incidents and develop a framework to respond to these incidents. If a financial institution or its TSP is under attack, management should consider the potential impact of any decision to limit or suspend processing and any downstream implications to the financial institution's business partners, customers, or other TSPs. Incident response processes should also address concerns regarding availability, confidentiality, and integrity of data with different sensitivities.[17] Finally, the financial institution and its TSPs should periodically update and test their incident response plan to ensure that it functions as intended, given the rapidly changing threat landscape.**

A financial institution experiencing a cyber attack may need to simultaneously investigate an ongoing security incident and execute the financial institution's recovery strategies. As a result, the financial institution and TSP should consider identifying and making advance arrangements for third-party forensic and incident management services. Also, a financial institution relying on such third-party services should plan for potential limited availability during a large-scale cyber event.

Conclusion
When using third-party service providers, management should ensure adequate business resiliency through:

- Third-Party Management, which involves due diligence procedures, regular monitoring, and strategic, integrative considerations with third-party servicers;
- Third-Party Capacity, which considers third parties' abilities to deliver essential services under adverse scenarios, in addition to possible alternatives in the event of third-party failure;
- Testing with Third-Party TSPs, which involves testing the business continuity resilience among the financial institution and third-party service providers, in addition to the review of test results and remediation of any observed weaknesses; and
- Cyber Resilience, which involves identification and mitigation of cyber threats to data and operational infrastructure, as well as effective incident response procedures to cyber attacks.

As stated throughout this appendix, the key concept maintains that regardless of whether the systems and resilience capabilities are managed by the financial institution or TSP, the financial institution's management and board are responsible for the oversight and assurance of continuing operations in a timely manner.The New OCC Risk Management Life Cycle

The OCC expects a bank to have risk management processes that are commensurate with the level of risk and complexity of its third-party relationships and the bank's organizational structures. Therefore, the OCC expects more comprehensive and rigorous oversight and management of third-party relationships that involve critical activities—significant bank functions (e.g., payments, clearing, settlements, custody) or significant shared services (e.g., information technology), or other activities that

- could cause a bank to face significant risk if the third party fails to meet expectations.
- could have significant customer impacts.
- require significant investment in resources to implement the third-party relationship and manage the risk.
- could have a major impact on bank operations if the bank has to find an alternate third party or if the outsourced activity has to be brought in-house.

A formal Incident Response Plan is an essential component of a comprehensive BCP plan, and the Incident Response Plan, including the roles and participation of vendors, can be maintained within the BCP-INSIGHT™ application and be directly linked to a vendor's risk profile and documentation in VendorINSIGHT®.

An effective third-party risk management process follows a **continuous life cycle** for all relationships and incorporates the following phases:

Planning: Developing a plan to manage the relationship is often the first step in the third-party risk management process. This step is helpful for many situations but is necessary when a bank is considering contracts with third parties that involve critical activities.

Due diligence and third-party selection: Conducting a review of a potential third party before signing a contract helps ensure that the bank selects an appropriate third party and understands and controls the risks posed by the relationship, consistent with the bank's risk appetite.

Contract negotiation: Developing a contract that clearly defines expectations and responsibilities of the third party helps to ensure the contract's enforceability, limit the bank's liability, and mitigate disputes about performance.

Ongoing monitoring: Performing **ongoing monitoring of the third-party relationship** once the contract is in place is essential to the bank's ability to manage risk of the third-party relationship.

Termination: Developing a contingency plan to ensure that the bank can transition the activities to another third party, bring the activities in-house, or discontinue the activities when a contract expires, the terms of the contract have been satisfied, in response to contract default, or in response to changes to the bank's or third party's business strategy.

In addition, a bank should perform the following throughout the life cycle of the relationship as part of its risk management process:

Oversight and accountability: Assigning clear roles and responsibilities for managing third-party relationships and integrating the bank's third-party risk management process with its enterprise risk management framework enables continuous oversight and accountability.

Documentation and reporting: Proper documentation and reporting facilitates oversight, accountability, monitoring, and risk management associated with third-party relationships.

Independent reviews: Conducting periodic **independent reviews of the risk management process enables management to assess whether the process aligns with the bank's strategy and effectively manages risk posed by third-party relationships.**

REFERENCES

1 ^FFIEC IT Examination Handbook's "Outsourcing Technology Services Booklet", /ITBooklets/FFIEC_ITBooklet_OutsourcingTechnologyServices.pdf.

2 ^Refer to "Introduction" and "Business Continuity Planning Process" sections of this booklet.

3 ^See the "Third-Party Capacity" section below.

4 ^See the FFIEC IT Examination Handbook's "Outsourcing Technology Services Booklet, " /ITBooklets/FFIEC_ITBooklet_OutsourcingTechnologyServices.pdffor comprehensive information on contract provisions.

5 ^See the "Risk Monitoring and Testing" section of this booklet.

6 ^Refer to the "Testing With Third-Party TSPs" section below.

7 ^This includes internal and outsourced audit reports, reports issued by regulatory agencies, and other independent assessments, such as consulting reports, penetration tests, and vulnerability assessments.

8 ^MIS reports include, for example, compliance with SLAs, TSP risk mitigation capabilities, or mediation timeframes.

9 ^This concept is equally applicable to a situation where operations are moved to an alternate data center owned by the same service provider.

10 ^See Appendix H, "Testing Program - Governance and Attributes."

11 ^Proxy testing is a term used to refer to testing that is conducted on like systems and with like interfaces for the purpose of not having to repeat similar tests that should provide similar results. Proxy tests are conducted using the same hardware and operating software and are sometimes used as a replacement for actual tests.

12 ^A zero-day threat exploits previously undiscovered vulnerabilities for which a software patch or other mitigating control is not yet available.

13 ^Hardening software and operating systems is intended to eliminate security risks and includes activities such as configuration management, security patch management, and the removal of all unnecessary programs and utilities.

14 ^FFIEC IT Examination Handbook's "Information Security Booklet," /ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf.

15 ^Cloud-based disaster recovery services employ virtualization, disk backup, and data replication technologies to provide financial institutions and their service providers with low-latency, diversified, and cost-effective offsite backup, recovery, and restoration services. The term "cloud" refers to the fact that the internal architecture of these services is abstracted from the customer.

16 ^Virtualization technology involves one physical computer running virtualization software that may contain two or more "virtual machines" that process data independently. These virtual machines may be backed up on offline media or replicated between physical processing environments.

17 ^FFIEC IT Examination Handbook's "Information Security Booklet," /ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf