Business continuity beyond company walls

When a crisis hits, will your vendors’ resiliency match your own?

May 2014
Reliance on third parties is substantial and continues to gain momentum. Companies are becoming increasingly comfortable migrating core and strategic functions to external providers with the objectives of improving efficiency, accelerating growth, and enabling operational transformation.

Do strategy execution discussions include the need to gain insight into your critical vendors’ resiliency and recovery capabilities?

If not, are strategic goals at risk of being derailed by an unfortunate combination of unprepared vendors and insufficient internal resiliency and contingency planning?

**Consider this scenario**

A global weather forecast predicts that a major early-August typhoon has a 30% chance of impacting an overseas location that’s home to your most important manufacturing, logistics, and supplier operations. Within 48 hours, that possibility has become a certainty, with impacts likely much stronger than had been predicted earlier. To make matters worse, the storm also has the potential to impact a nearby outsourced customer contact centre that supports 75% of your call volume. The centre was recently expanded to provide nearly all of the finance functions for your domestic and global manufacturing locations.

Adding to these clear dangers is the country’s tenuous political situation: In recent national elections, the longtime ruling party was voted out of office, and most government functions are still in the midst of leadership transitions. In this atmosphere, your risk management team is concerned about the country’s ability to manage an effective emergency response and, long-term, about its overall political stability.

What are your options, given these variables? Will you try to ride out the storm and run the risk of watching your global growth strategy collapse before yielding its promised benefits? Or, have you forearmed your organisation against such business interruption risks by instituting a business continuity management programme that encompasses vendor risk by incorporating increased resiliency and rapid recovery?

With the increasing frequency of extreme climate and weather events combining with an unsettled political and economic landscape in many parts of the world, the type of scenario described above is all too realistic and all too possible. To some degree, organisations with global supply and service chains and outsourced business processes live constantly in the crosshairs, with a near guarantee of major impacts from a natural or manmade disaster – if not today, then soon.

**Is your organisation ready?**
Critical vendors, cascading impacts

All too often, organisations take a siloed and cursory view of their resiliency and recoverability needs around business interruption risk. The more exposed and constantly evolving functions within the organisation, such as IT and supply chain management, may have performed a limited analysis and taken a few well-meaning preventative measures, but these rarely take into account the internal and external process and technology interdependencies necessary to significantly reduce the operational and financial impacts associated with interruption events.

Meanwhile, functions such as human resources, finance, customer care, and operations, with their well-established processes and less dynamic operating environment, often make only the most cursory dive into ‘what if’ scenarios for unplanned operational interruptions, contenting themselves with ad-hoc and unconfirmed recovery plans. Further, the totality of an organisation’s resiliency and recoverability needs are often only vaguely defined, with no structures or mechanisms to allow for integrated testing and validation. As a result, leadership often has a poor understanding of the organisation’s real business interruption needs and capabilities. This lack of clarity is amplified even further when we move beyond company walls and begin examining interruption risk among the vendors who provide support for the organisation’s critical functions. Even when a vendor provides a summary of its business continuity programme, companies are rarely able to understand how the vendor’s continuity programme aligns with their own resiliency and recovery needs.

After an organisation has reached a mature level of operational resiliency and recoverability by developing its own business continuity management (BCM) processes and mechanisms, it is imperative for it go beyond basic vendor risk management by developing detailed procedures for understanding critical vendors’ interruption resiliency and recovery capabilities. We’ve seen numerous instances where an interruption at a critical third party (such as a component supplier, logistics provider, financial services intermediary, business process outsourcer, or technology vendor) impacts even the most internally prepared organisation. The ripple effect of downtime can be huge, both economically and in terms of your brand. Finding out after an interruption event that your vendor is prioritising restoring service to other, more ‘major’ customers ahead of you can be as damaging to your market share, brand, and reputation as if the disaster had struck your operations directly. Unfortunately, the limited value of cursory annual business continuity vendor questionnaires only becomes apparent after an interruption occurs. A more robust process is a necessity.
Step 1: Map your vendor risk landscape

The journey to an integrated, responsive, and proactive business continuity management programme that extends beyond company walls begins with a thorough business impact analysis (BIA). The BIA provides a detailed, foundational view of how interruption events (e.g., loss of technology, reduction in personnel, loss of facilities, loss of third parties) can impact the organisation. In addition to highlighting critical technology, personnel needs, and key workspace needs, the BIA also provides the first piece of the vendor resiliency and recoverability puzzle.

A key output of the BIA is a set of impact and resiliency strategy details about the organisation’s critical vendors that can significantly improve the vendor risk management programme and help reduce interruption risk created or exacerbated by vendor outages. The impact and resiliency strategy details include a mapping of business processes to specific critical vendors, impacts over time if those vendors’ services are unavailable, an analysis of whether alternate vendors exist, and, if so, their ability to substitute for the primary vendor (e.g., in terms of performance, capacity, ramp-up/lead time, quality, etc.).

A companion process to the BIA is the interruption risk assessment (RA), which identifies and evaluates areas in which the company is exposed to natural and manmade interruption events and which processes would be impacted. A subsequent, high-level vendor interruption risk assessment (VIRA) is performed once the company’s critical vendors have been identified. The VIRA is often performed with the assistance of the vendor management function, as vendor attribute data such as key locations, contractual obligations, service level agreements, rights to audit, amount of leverage the organisation has over the vendor, and other company goods and services provided by the vendor are necessary to obtain a complete risk assessment perspective. One of the more important VIRA results is the identification of correlated risks – i.e., specific interruption risks that can affect a critical vendor (or group of vendors) and the company simultaneously.

From here, the next phase of business continuity programme implementation can begin: the identification of a recovery strategy. As the owners of critical processes document their recovery strategies, they’ll also describe how critical vendors figure into those strategies. Crisis communication linkages to critical vendors will also be documented to enable the efficient and effective flow of information during a crisis.

At the conclusion of the full BIA and RA process, the company will have the answers to two important questions:

1. Which vendors will have the most impact on my organisation if they suffer an interruption, and how quickly will the impact materialise?
2. How does my recovery strategy involve my critical vendors?

And if the company has completed its VIRA, a third important question will have been answered:

3. What are the more probable interruption events that could threaten my critical vendors?

Once the organisation has performed all the key activities necessary to identify its critical vendors, predict their likely interruption risks, and determine how they will be used in a crisis, it is time to move to the next component of the vendor resiliency and recovery analysis programme: vendor resiliency stratification.
Step 2: Distinguish among different shades of red

Not all critical vendors are equally important to the organisation, and not all customers are equally important to those vendors. Given abundant time, resources, and funding, you’d want to evaluate all your critical vendors’ resiliency and recovery capabilities. However, corporate realities dictate taking a risk-informed approach in order to obtain the greatest amount of comfort for a reasonable amount of effort and funding. Within the BIA and RA documentation is the foundation for developing a risk-informed approach that enables vendor resiliency and recovery assessment stratification. That foundation can be distilled to nine critical risk variables:

1. Revenue and inventory impact from loss
2. Proximity of the vendor and logistics
3. Capacity utilisation (performance and capacity of the vendor)
4. Service level agreements and right to audit
5. Potential impact on service/product quality if vendor change is performed rapidly
6. Labour, country, and geopolitical risks
7. Level of vendor integration with your technology
8. Correlated risk (natural and man-made hazards, geographic concentration, availability, and reliability)
9. Regulatory issues and crossborder issues

Determining the weighting of the various critical vendor attributes from the BIA and RA is a collaborative process best overseen by the same cross-functional steering committee shepherding the business continuity programme.

The amount of resiliency and recovery analysis performed for each critical vendor will vary based upon their position in the vendor interruption management stratification. Vendors within the top tier will need more frequent and rigorous inspection and analysis while those in lower tiers will require less. Linking vendor interruption risk management activities with the broader vendor risk management programme will help ensure a coordinated approach to understanding the totality of the organisation’s vendor risk portfolio. (See Figure 1.) This could possibly mean document reviews and site visits for due diligence on financial health, reputational brand, IT/physical security, technology risk, operational risk, and fourth-party risk. (See Figure 2.)

Figure 1: The spectrum of vendor risk
Figure 2: Vendor management governance and organisation model

**Governance and organisation**

<table>
<thead>
<tr>
<th>Accountability and oversight</th>
<th>Documentation and reporting</th>
<th>Organisational coverage</th>
<th>Risk management</th>
<th>Independent reviews</th>
</tr>
</thead>
</table>

**Board approved programme**

- Programme support
- Tactical reporting
- Tracking
- Training
- Tools and technology
- Continuous improvement

**Policy and procedures**

- **Planning**
  - Inherent risks
  - Strategic objectives
  - Complexity assessment
  - Cost/benefit
  - Other initiatives
  - Dual employee
  - Customer impact
  - Information security
  - Contingency plans
  - Laws and regulations
  - Diversity
  - Selection and contract monitoring
  - Critical activities

- **Due diligence**
  - Strategies and goals
  - Legal and regulatory
  - Financial risk
  - Experience and reputation
  - Fees and incentives
  - Qualification, background, reputation
  - Risk management
  - Information security
  - Management information systems
  - Resilience
  - Incident reporting and management
  - Physical security
  - HR
  - Subcontractors
  - Insurance coverage
  - Conflicting arrangements
  - Country risk
  - Reputational risk
  - Operational competency
  - Fraud
  - Model risk
  - FCPA
  - BSA/AML
  - PCI-DSS

- **Contract negotiation**
  - Nature and scope
  - Performance
  - Information handling
  - Right to audit
  - Compliance
  - Cost and compensation
  - Ownership and license
  - Confidentiality and integrity
  - Contingency
  - Indemnification
  - Insurance
  - Dispute resolution
  - Limits on liability
  - Default and termination
  - Customer complaints
  - Subcontracting
  - Foreign based 3rd parties
  - OCC-CFPB supervision
  - Diversity
  - Records management
  - Amendments

- **On-going monitoring**
  - Conflicting interests
  - Compliance
  - Financial condition
  - Insurance
  - Key personnel
  - Manage risk proactively
  - Adaptable process
  - Technology
  - Contingency plans
  - 4th parties
  - Confidentiality
  - Customer complaints
  - Issues management
  - Credentials and certifications
  - Problem management
  - Monitoring plan
  - Testing

- **Termination**
  - Contingency planning
  - Transition
  - Data
  - Joint intellectual property
  - Reputational risk
  - Written exit plan
  - Identification of alternate sources
  - Customer impact
Step 3: Be specific

The days of check-the-box vendor risk management are over. You can’t just request a copy of the vendor’s business continuity programme description and call it good, and you can’t just rely on lengthy but generic business continuity questionnaires or the results of recent recovery exercises.

In today’s business climate, with both internal and external stakeholders hyper-aware of risk, companies must dig deeper to obtain true and verifiable comfort. For vendor BCM, the best comfort comes from assessing the quality of the vendor’s resiliency and recovery capabilities in areas that are integral to your organisation’s operational resilience. This information is documented within the organisation’s BIA and RA and should include, at a minimum:

• A list of the goods and services provided by the vendor
• A list of the processes within your organisation that consume the vendor’s outputs, or rely on a vendor to complete the service/product delivery cycle
• A description of where the vendor’s activities are geographically performed
• A determination of the point at which a vendor interruption crosses the threshold of criticality
• A description of possible regulatory impacts from a vendor’s lack of resiliency
• A description of the vendor’s role during an interruption that affects the organisation

Some of the overarching vendor resiliency questions could be summarised as follows:

1. Does the vendor’s resiliency and continuity programme cover the goods and services used by our organisation?
2. Does the vendor’s recovery prioritisation and timeline for these goods and services align with our organisation’s recovery needs?
3. How detailed is the vendor’s resiliency analysis for their own critical vendor that are linked to the goods and services consumed by your organisation (e.g., 4th party risk)?
4. Are assumptions accurate regarding your current and planned volume of goods and services consumed?
5. What do the vendor’s BIA and RA show for the goods and services consumed by your organisation and the locations from which they are provided?
6. Do the threats, risks, and potential impacts identified by the vendor match those in your own vendor analysis?
7. Could your organisation be affected by the same risk events that threaten your vendors?
8. If the vendor received a business continuity-related ‘certification’, did the scope of the certification cover all the critical goods and services consumed by your organisation?
9. Does the vendor’s crisis management plan include timely customer notification to allow the customer time to effectively respond to a potential interruption of goods and services?
10. Does the vendor perform integrated technology and operational recovery exercises for those operations involved in providing goods and services to your organisation?

What’s your leverage?

You know which of your vendors are critical to your operations, but do you know where you rank in importance among your critical vendor’s other customers?

When a vendor’s operations are functioning normally, it will strive to fully meet all of its customers’ needs. But what happens when a crisis event occurs? Rational vendors would seek to avoid the negative publicity and potential legal damages that come from not meeting contractual requirements. Future revenue and legal exposure would significantly inform their customer prioritisation process that determines who will get priority access to its restored pipeline of goods and services.

Prioritisation algorithms likely have total customer spend as one of the highest criteria to determine which customers receive support and which do not. As part of its assessment of a vendor’s resiliency posture, a company should always seek to determine its own place in the vendor’s customer hierarchy. The clarity this affords can help you make informed strategic decisions on vendor diversity, inventory management, and the probability of receiving detailed resiliency information from the vendor.

If there is any question about your prioritisation with the vendor, whether you are allowed to inspect the vendor’s crisis management and customer support criteria within their business continuity plans should provide clarity. This is once again where the adage ‘trust, but verify’ is relevant.
Step 4: Trust but verify

Once critical vendors have been slotted into risk-ranked tiers and vendor resiliency questions have been developed, the process of obtaining and validating an enumeration of the vendor’s resiliency and recovery capabilities begins.

The following are six best practices that will aid your vendor resiliency interaction and analysis:

1. Ensure that the majority of your resiliency inquiry communications with the vendor originate from the individual who owns the vendor relationship. Most likely, this individual has an important stake in the vendor’s reliability and is involved in business continuity activities related to the vendor’s goods and services. The higher this individual is within your organisation structure, the more importance the vendor will likely ascribe to the communication.

2. Your point person should speak directly with the individual responsible for maintaining the vendor’s resiliency and continuity programme. Discussions with this individual can yield interesting insights into the vendor’s overall BCM programme, framework, and standards, as well as the competency of the people who have developed and operated the programme. If the vendor’s resiliency and continuity contact is continuously unavailable, or the position remains unfilled/undefined for a protracted period, consider reevaluating your vendor relationship.

3. Enlist the vendor as a resiliency partner, since interruption events at either end of the relationship continuum will affect both parties. Being transparent about the organisation’s resiliency goals will give the vendor comfort that there is no ulterior motive for requesting detailed operational resiliency information.

4. Obtain relevant portions of the vendor’s BIA and RA. Even if summarised, they’ll give you insight into whether the resiliency programme is built on a solid foundation.

5. Use a tailored version of international business continuity standards as a basis for vendor inquiries. Ask the vendor to provide supporting documentation for the more impactful questions.

6. Have the vendor describe its response to a prior potential or actual crisis event. Ask for relevant post-mortems or documents describing lessons learned. Ask the vendor directly for the framework it uses for identifying, escalating, and responding to crisis events. Ask for the impact thresholds where they would contact customers in advance of, or immediately after, a crisis event. Confirm that your organisation would react quickly to these communications.
Regulators get tough on recoverability


Three major points stand out in regard to vendor risk management:

1. The bulletin specifies that consideration of a third party’s resilience would henceforth be considered a required part of due diligence.
2. It introduces the concept of third-party relationships that involve ‘critical activities’ and sets an expectation that banks will exercise more comprehensive and rigorous due diligence, management, and oversight of such relationships.
3. It establishes an overarching standard that institutions under the OCC’s regulatory umbrella should adopt risk-management processes commensurate with the level of risk and complexity in its third-party relationships.

These three elements signal that, at least in these sectors of the banking industry, companies need to get serious about mapping their vendor risk landscape, determining the criticality of each vendor relationship, and adopting robust analytical processes to identify, measure, monitor, and control recoverability risks and other risks associated with third-party relationships, particularly for their most critical vendors.
Collating, analysing, and reacting to vendor responses is the final phase of implementing your vendor resiliency risk management programme. This is where expectation meets reality. You’ll likely discover that many of your critical vendors have minimal formal resiliency or business continuity management programmes, often focusing solely on IT disaster recovery and life safety emergency management. Those vendors that do have more mature business continuity programmes may not have the level of customer focus needed by your organisation. Just because you operate within a regulated industry doesn’t mean that your critical vendors have the same sensitivity or depth of knowledge on regulatory resiliency requirements.

So it often comes down to how much vendor resiliency risk you are willing to accept. The stratification process from Step 2 will help leadership come to a consensus on which actions to take for critical vendors that turn out to lack adequate resiliency and recoverability. Knowledge provides clarity and the ability to make informed decisions. Sometimes deciding on a course of action is easy, as when a critical vendor imbedded within a regulated process lacks necessary resiliency and recovery capabilities – in which case, switching or diversifying vendors is obligatory.

In other situations, where the regulatory component is not in play, management response has more flexibility. For instance, management may decide to continue a relationship with a resiliency-deficient vendor due to irresistible pricing or lack of suitable alternate vendors. In these situations, management is aware and informed, and has decided to informally self-insure against the risk. Organisations may want to reduce the interruption risk associated with these vendors through a combination of strategies, such as:

- Maintaining higher inventory levels for at-risk items
- Collaborating with the vendor to improve its resiliency
- Creating limited ‘backup’ vendor relationships
- Implementing more robust business continuity practices for the affected business processes

Sometimes, the expected cost of vendor resiliency contingency planning can lead management to conclude that replacing the less resilient vendor is a less risky and costly alternative.
Performing a resiliency and recoverability analysis before finalising a relationship with a critical vendor will often give you more leverage to obtain the needed information in a timely manner, and increases the likelihood that resiliency and recoverability improvements will be made. Codifying in the vendor contract your expectations regarding availability of goods and services will often provide more transparency to the vendor’s cost of providing the necessary resiliency. And if a high level of vendor availability is critical to a strategic growth goal or to fulfilling a regulatory requirement, resiliency levels should never be negotiable.

The governance model in Figure 4 lays out the type of organisational framework under which vendor risk management activities around resiliency and recoverability should be conducted. The organisation will need to define vendor risk management reporting structures, roles, and responsibilities within the structure; create the polices, procedures, and guidelines to govern its assessments (such as risk assessment methodology); and establish the organisation’s risk tolerance levels.

Figure 4: Vendor risk management governance model

<table>
<thead>
<tr>
<th>Internal audit</th>
<th>3rd line of defence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance</td>
<td>Critical Vendor Oversight Committee</td>
</tr>
<tr>
<td>Legal and compliance</td>
<td></td>
</tr>
<tr>
<td>Management and oversight</td>
<td></td>
</tr>
<tr>
<td>Sourcing</td>
<td>Operational Risk Oversight</td>
</tr>
<tr>
<td>Subject matter specialists</td>
<td></td>
</tr>
<tr>
<td>Business unit</td>
<td></td>
</tr>
<tr>
<td>Vendors</td>
<td></td>
</tr>
</tbody>
</table>

Step 5: React (continued)
Conclusion

In a vendor relationship, just as in any other relationship, you need to know you can count on the other party when crisis strikes. You need to know they’ll be there for you. To achieve comfort around vendor resiliency and recoverability, it’s all about transparency, asking the right questions and pushing the right levers to determine whether your vendors will be able to weather a serious business interruption and quickly resume delivery of the goods and services you need.

The more foreknowledge you have – about your own needs, the capabilities of your vendors, and the robustness of your resiliency plans – the more comfort you’ll have about staying on track toward your long-term strategic and operational goals, even when faced with a crisis event.
About PwC’s Business Continuity Management Services

PwC’s Business Continuity Management services help clients understand the impact of crisis events on operational performance and strategic goals. We also create integrated, optimised, and forward-looking Governance, Risk, and Compliance environments that help management determine the best approach for developing an effective BCM programme. Whether it’s minor adjustments to an existing BCM programme or a wholesale redesign, let us show you how to get more value and confidence from BCM. Isn’t it time to realise the strategic value locked within your BCM programme?

For more information about PwC’s Business Continuity Management and Vendor Risk Management Services, please visit pwc.com/riskassurance.

To have a deeper discussion around vendor resiliency and other organisational challenges you may be facing, please contact:

Marco Amitrano
Global Assurance Markets Leader
+44 (0) 1895 522386
marco.amitrano@uk.pwc.com

Dean Simone
US Risk Assurance Leader
+1 267 330 2070
dean.c.simone@us.pwc.com

Jim Woods
Hong Kong, China Risk Assurance Leader
+852 2289 2316
jim.woods@hk.pwc.com