Ensuring Vendor Continuity

Samuel Shanthan , CISA, CIPM, MBCI, has more than 15 years of business continuity and information security-related experience at large multinationals, Big Four and Fortune 500 organisations. He has managed business continuity setups in Europe, Asia, Africa, the Middle East and Australia. Currently, he works as a consultant in the public sector and is running his consulting practice, Grace Risk Advisors.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal),* find the article and choose the Comments tab to share your thoughts.

Go directly to the article:

Nowadays, there is much talk about the risk associated with outsourcing, vendors and supply chains. However, many organisations still do not measure associated risk and take preventive actions. Over many years, the main priority with vendors has been service level agreements (SLAs) and most of them are satisfied with 99.9 percent availability or similar. Many vendors and suppliers depend on other vendors and suppliers to provide their services. Although service levels and penalty clauses may be in place in agreements, they are not adequate when it comes to mitigating impacts caused in the organisation due to a critical vendor service failure. Further, most agreements contain a *"force majeure"* clause that will generally cover them for their failure, partially or fully, due to a disaster or crisis.

Therefore, vendor continuity risk is to be recognised and managed within business continuity management (BCM). This is also referred to in the International Organization for Standardization (ISO) standard ISO 22301:2012, specifically in clauses 4.1 and 8.2-8.4, as well as ISO 27001:2013 within continuity A.17.

Statement on Auditing Standards (SAS) 70 was a good practice, but it was inadequate to cover the previously mentioned risk and was not widely used outside the US. SAS 70 was replaced by Statement on Standards for Attestation Engagements (SSAE) 16 in 2010, but it has not yet gained global prominence. In spite of the presence of various standards, each organisation has to develop its own due diligence to assess vendors on which the organisation is going to depend.

A vendor checklist for critical services should be considered during planning, request for proposal (RFP) and evaluation. This includes due diligence of critical products and services on which particular vendors rely (i.e., those impacting the supply chain of the vendor). The aim of this assessment is not to pass the responsibility of a failure to the vendor, but to adequately assess the risk and treat it within acceptable time frames and limits or avoid the vendor.

It is important that the organisational procedures, especially relating to procurement, contain documented and effective procedures to include checking continuity risk of vendors that support critical processes or services.

It is beneficial to educate vendors with ideas and suggestions gleaned from the experience of other organisations (subject to maintaining confidentiality) or even new products. Vendors need to be considered as partners in continuity planning, and organisations may support vendors with recommendations to other clients.

This article suggests a more practical way to ensure vendor continuity, based on consultancy and industry experience across the public and private sectors, with the objectives of:

- Identifying and measuring the continuity risk associated with vendors, suppliers, outsourced services and managed services
- Treating such risk through appropriate actions and plans

This is a fairly simple approach with a mathematical computation that can be modified by the organisation and used in an Excel tool. This approach is focussed on medium to small organisations. Large outsourcing projects may require further detailed studies, and some organisations may use external feeds and recommendations.

SERVICE RISK AND CONTINUITY SCORE

In **figure 1**, the service risk is assessed and is illustrated by a quantitative rating and weighting method as guidance. Each organisation should adopt a suitable method to align with its corporate rating methods.

Continuity score has to be evaluated for each service and due diligence needs to be exercised, as not all information can be obtained from the vendor. These questions are drafted in a manner to assess the business continuity readiness while not documenting the confidential information of the vendor (**figure 2**).

Figure 1—Service Risk

Criteria	Consideration in Assessment	Evaluation (1-5)	Weight
Criticality—Is this product/service considered essential to any business process that is classified as critical as per the business impact assessment (BIA)?	Identify the supporting processes and their criticality. Non-critical score: 1 Critical score: 5	1-5	30-50%
Alternative means—Are there backup procedures, manual procedures or alternative means if the vendor of this product/service fails?	Consider alternative processing or backup equipment, manual methods or services available. Availability of alternate process score: 1 No alternative available score: 5	1-5	20-30%
Alternative product/service—Are there alternatives in the marketplace that can be obtained for this product/service?	Consider alternatives and technical compatibility. Alternatives available score: 1 No alternative available score: 5	1-5	10-20%
Easiness to switch—How easy is it to switch from one particular vendor to another vendor for this product/service?	Consider switching cost, effort and time. In some cases, the product is supported by multiple vendors (dealers) and it is possible to switch vendors without switching the product. Easy to switch score: 1 Impossible to switch score: 5	1-5	10-20%
Weighted Average—Service Risk:			

Note 1: The weight range is a suggestion based on previous experience in evaluating vendors. Every organisation may use a different weighting.

Note 2: In the assessment, service impact is primarily considered and probability is deliberately excluded, but an organisation may use probability as well.

Scoring criteria:
1. Risk is nil or negligible.
2. Risk is low.
3. Risk is moderate.
4. Risk is major.
5. Risk is extreme.

Source: Samuel Shanthan. Reprinted with permission.

Figure 2—Continuity Score

Criteria (Questions) to Be Sent to Vendors	Considerations in Evaluating Responses	Evaluation (0-5)	Weight
1. Does the organisation have a continuity policy rolled out and risk management policies in place? Provide names of the policies.	Existence of policies shows the presence of good governance.		10%
2. Does the organisation have a documented business continuity plan? Request the table of contents (ToC) and updated date.	The ToC shows the coverage and the updated date shows the interest taken in business continuity/disaster recovery.		15%
3. Has the organisation tested the business continuity plan? When were the last three tests conducted?	Testing shows the organisation's willingness to evaluate the effectiveness of its plan regularly.		10%
4. Was the BCM test effective? What was the result? If the BCM test was ineffective, was it retested or are there plans to retest?	Test effectiveness includes retesting and documenting failures for further action, which should be considered positively.		10%
5. What is the recovery time objective for the organisation's five most critical processes?	Consider the vendor's recovery time alignment to the organisation's recovery time requirements.		10%
6. What were the five broad scenarios tested in the last two years?	Consider the scope and scenarios to evaluate the coverage and interest of the organisation in ensuring its continuity.		10%
7. Does the organisation have adequate separation to avoid the same disaster striking both the primary and backup data, as well as recovery sites?	Consider the same threats—such as floods, tsunamis, terrorism or earthquakes—affecting both sites. They should be radially quite apart and not in the same geographic location, including on fault zones or coastal areas or in the same city.		5%
8. Was there a general staff training conducted in the last two years for business continuity?	Consider culture, training coverage and other awareness at the organisation.		10%
9. Is the organisation certified to any relevant standard in business continuity or information security or service continuity? What was the scope?	This shows the extra step the organisation has taken to align to best practices, but excludes quality assurance certification. Check the scope in the context of the organisation.		10%
10. What is the status of the organisation's financial viability, including assets, profits and revenue? The financial viability of the organisation is important in ensuring that the organisation will be serviced continuously.	This information may not be easily available for private companies and needs to be requested, ideally in the RFP (audited financial statements). Due diligence needs to be exercised to evaluate this information.		10%
Weighted Average—Continuity Score:			

Note 1: The weight range is a suggestion based on previous experience. Every organisation may use different weighting.

Scoring criteria:
1. Nonexistent or very poor
2. Setup is less effective.
3. Setup has major defects.
4. Good practice is met with minor defects, that are acceptable
5. Excellent setup and practice, with full compliance to best practices/standards

Source: Samuel Shanthan. Reprinted with permission.

A weighted average continuity score close to 5 indicates an excellent vendor for the particular product or service offered. This should be considered in conjunction with the service risk of the product and/or service. Continuity score measures the control that will mitigate the service risk.

A lower continuity score disqualifies a vendor if the product/services have a higher service risk. In other words, for lower service risk, continuity scores will have less importance.

Figure 3 may be used as guidance. In all cases, judgement should be exercised.

Figure 3—Continuity Score and Service Risk Mapping

Service Risk	Accepted Continuity Score
1 - <3	Assessing continuity score is optional.
3 - 5	Continuity score needs to be assessed and actions taken accordingly.

Source: Samuel Shanthan. Reprinted with permission.

If the service risk is low (i.e., <3), assessing the continuity score is optional, as the impact of the service becoming unavailable is low.

If the service risk is high when the impact of the service being unavailable is high, then the continuity score has to be assessed. In other words, how the vendor will ensure continuity of service and whether the vendor has sufficient business continuity and resilience setups need to be assessed. The continuity score should be good, preferably above 3.

Among other criteria for selecting vendors, business continuity should also be included for all products and services that have a service risk of three and above. Vendor selection evaluation should mention the service risk and the continuity score (if applicable, based on service risk) and justify the reason for selecting the vendor.

RISK ASSESSMENT AND TREATMENT

Considering the number of outsourced and other vendor services in operation in an organisation, risk needs to be reassessed periodically to reflect operational changes in order to mitigate new or existing and unforeseen service risk.

In any industry, there may be some vendors that are very powerful and have a monopoly. In such instances, it is not possible to assess their continuity when no other option is available. In some countries, telecoms are monopolies and, generally, no other choice is available unless a very small aperture terminal (VSAT) or other satellite communications are used, but these have limitations and cost concerns.

As in the cases noted, if there is significant dependency on the vendor and no other action is possible, that dependency risk has to be documented in a risk register and accepted at a corporate level. Vendor or outsourced service or supply chain risk assessment should be considered part of the organisationwide risk assessment. As a guide, such a risk assessment may include:

- A list of all outsourced or vendor-dependent services
- Risk assessment of the vendor service if it were to be unavailable for a prolonged period of time. Consider the service risk and continuity score mentioned previously.
- For high-level service risk, existence of action plans (such as testing manual procedures or obtaining regular softcopy dumps) before a vendor fails (default)
- Development of an action plan to execute after a vendor fails (default), cross-referenced in the respective business continuity and/or disaster recovery plans

Figure 4 shows an example of an outsourced risk assessment.

OTHER RISK NOT COVERED

A typical vendor continuity assessment may not cover the following risk areas, which may need to be addressed separately:

- Supply chain for common consumables for which adequate stock (in-house) and alternatives are in place (e.g., printing paper, printer cartridges)

Figure 4—Example of an Outsourced Risk Assessment

Parameters	Vendor 1	Vendor 2
Service	IT hosting	Communication link
Responsible division	IT	IT
Criticality of service	Major infrastructure and applications	Main communication with data centre (DC)
Service risk	4	3
Continuity score	3	2
Residual risk*	Low	Medium
Action required now (pre-default)	No action is required or possible, except for establishing disaster recovery (DR) setup (offsite) for the critical applications. Wherever possible, create manual procedures for critical operations.	Create a backup link with another vendor that does not share the same infrastructure, preferably on a different geographic route.
Course of action during default	Move to DR systems (off-site). Enact manual procedures wherever possible.	Switch to backup link only if the service cannot be restored within an acceptable time frame.

*This covers only the continuity risk. Consider the service risk and continuity scores in determining the residual risk. This could be based on a mathematical calculation or judgement as shown.

Source: Samuel Shanthan. Reprinted with permission.

- *Ad hoc* activities such as those related to auditing, consulting and project management vendors as they will be temporary. This could be part of the project risk assessment.
- Other risk associated with outsourcing such as confidentiality, conflict of interest and compliance. These have to be addressed in other risk assessments.
- Information security, especially confidentiality and integrity. This should be covered separately or combined into one, depending on the organisational setup. Since information security and business continuity have overlaps, it is a good practice to combine the risk assessment if possible.
- Deliberate default or nonperformance by vendor

This risk may be addressed by escrow. An escrow agreement is an arrangement by which one party (usually a vendor) deposits an asset or software code with a third person (called an escrow agent), who will, in turn, make delivery to the other party (usually a client) if and when the specified conditions of the contract have been met (such as insolvency of the vendor or noncompliance with the contract).

In the event of a deliberate default or legal/regulatory action preventing vendor operation, an escrow agreement may be of use. Escrow is one way of treating the risk of continuity of the vendor, at least in the short term, especially with software. The need and usefulness of an escrow agreement should be explored for the concerned service with the vendor.

There are different levels of escrow and the appropriate level should be chosen, with the possibility of executing and using the escrow agreement for the organisation's purposes. However, depending on the cost and benefit, an organisation may choose not to have an escrow agreement.

CONCLUSION

It is of paramount importance to ensure the continuity of vendors, especially those that are providing and supporting the critical services and processes of the organisation.

The initial challenge is incorporating a requirement for business continuity in selecting vendors, as well as preparing the requirements for tender as part of procurement and project procedures or checklists.

The next challenges are understanding and measuring the business continuity readiness/effectiveness of the vendor, which requires exercising due diligence and obtaining completed questionaries.

Finally, based on a risk assessment, action plans should be available before and after a default/interruption occurs.