Third-Party Assurance: Why and How?

Ook verkrijgbaar in het Nederlands

www.isaca.org/currentissue

Outsourcing IT services to the cloud offers many benefits for organizations. The concerns regarding maintaining and securing IT services become the responsibility of the supplier. The organization is supported and risk is transferred with a contract.

However, outsourcing IT services does not guarantee the IT environment will have no concerns; even services from Microsoft, Amazon and Google can experience hiccups. Contracted services can be subject to disturbances that impact day-to-day operations. How can an organization handle the IT risk and reputational risk that comes with it? And what controls can IT auditors expect an organization has implemented to mitigate risk? To answer these questions, it is important to first understand the risk and vulnerabilities of an organization to determine an appropriate framework.

The Risk

There are several studies regarding supplier disturbances and their impact that can help determine whether supplier disturbances need to be considered a significant risk.

Research by the Business Continuity Institute (BCI) indicates that enterprises have suffered millions of dollars' worth of financial damage due to experiencing one or more supplier disruptions.[1]

The risk of continuity of cloud service is highlighted by research by Uptime Institute. This study, investigating outages that have been publicly reported, shows that there have been increasing reports of outages in cloud services over the past three years.[2] It is possible that the number of publicly reported outages increased due to legal obligations to report outages. Nevertheless, the numbers demonstrate that outages are still present. Therefore, risk that causes disturbances, such as the risk of network failure or power outage, should be taken into account.

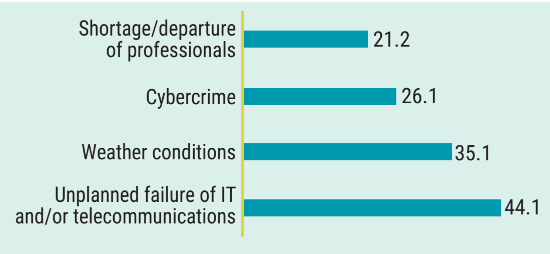
In addition, a survey on cloud security incidents conducted by (ISC)^2 indicates that 28 percent of the organizations surveyed were specifically affected by cloud security incidents.[3]

Disturbances from suppliers are nothing new and can be expected to occur. Major cloud providers such as Microsoft,[4] Google[5] and Amazon[6] are transparent about the need to handle disturbances regularly. It is more important to understand the impact of the risk on the organization.

Causes of Disturbances

Various studies reveal several factors that cause disturbances. BCI's report (**figure 1**) shows that 44.1 percent of the disturbances are due to the unplanned failure of IT and/or telecommunications. Furthermore, weather conditions (35.1 percent), cybercrime (26.1 percent) and the shortage/departure of professionals (21.2 percent) are important factors that affect supplier services. The factors that cause disturbances are a combination of technical failure, external factors and human actions.[7]

Figure 1—BCI Causes of Disruption

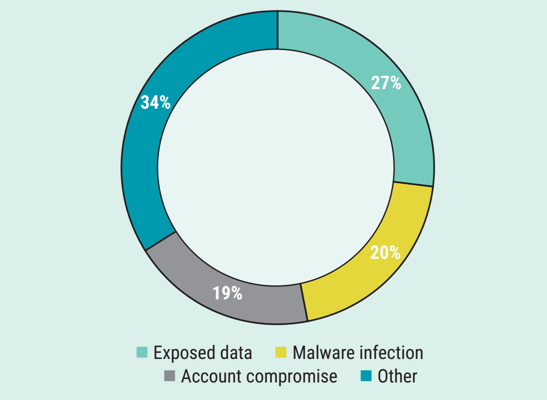


Source: Adapted from Business Continuity Institute (BCI), *BCI Supply Chain Resilience Report 2019*, United Kingdom, 5 November 2019, *https://www.thebci.org/resource/bci-supply-chain-resilience-report-2019.html*

The (ISC)^2 research (**figure 2**) also indicates external factors and human action that caused public cloud-related security incidents. In more than

Jouke Albeda,
CISA, CISSP, RE
Is an experienced IT auditor at Contrisity, where he supports enterprises within the fields of audit, risk and compliance and is associated with 3angles, audit risk and compliance. Previously, he worked as a risk and compliance manager at Datacenter.com and worked for Binder Dijker Otte (BDO) and Ernst & Young (EY) within the external IT audit practice. He has published articles in The Institute of Internal Auditors' (IIA) *Audit Magazine* and the Dutch professional organization for IT auditors, NOREA's magazine *de IT-Auditor*.

Figure 2—(ISC)² Public Cloud-Related Security Incidents

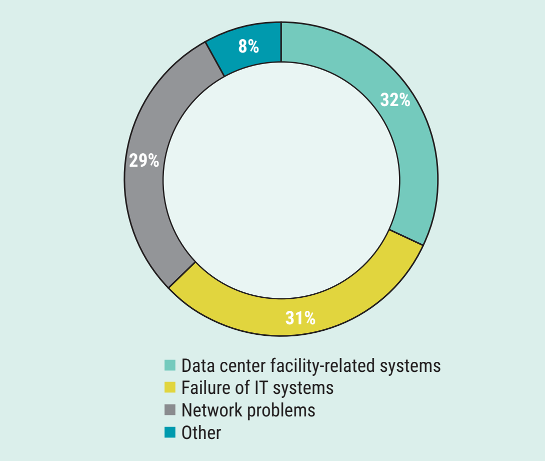


Source: Adapted from (ISC)², *2019 Cloud Security Report*, USA, August 2019, *https://www.cybersecurity-insiders.com/portfolio/2019-cloud-security-report-isc2/*

a quarter of cases (27 percent), data were exposed. Furthermore, in 20 percent of cases, there is maliciously infected software, and in 19 percent of cases, there is theft of an account.[8]

The Uptime Institute report (**figure 3**) indicates that data center facility-related systems are the biggest reason for outages (32 percent), followed by the failure of IT systems (31 percent) and network problems (29 percent). The report does not easily distinguish between technical issues, human actions and external factors.[9]

Figure 3—Uptime Institute Reasons for Outages



Source: Adapted from Uptime Institute, *Publicly Reported Outages 2018-19*, USA, March 2019, *https://uptimeinstitute.com/publicly-reported-outages-2018-19*

In examining these causes, a combination of controls should be implemented that addresses technical risk, risk within operational processes and risk caused by human action. The existing knowledge about the design and use of technology (e.g., the COBIT® framework, International Organization for Standardization [ISO] standards, Trust Service Principles) should be used to prevent unnecessary weaknesses in the system. Using best practices can prevent common mistakes from being made. Best practices and frameworks published by recognized professional practice organizations such as ISACA®, ISO, the Payment Card Industry (PCI), and the US National Institute of Standards and Technology (NIST) are available for addressing the human factors and other external and technical factors.

Measuring the Risk

Disturbances do not always have a major impact on the customer of the service. For instance, the failure of a test system for an hour often does not have a significant effect on productivity for the end user. However, not having an operational trading system for a stockbroker for 15 minutes has a considerable impact. Even when it comes to data leakage, the impact on a test database can be very different from a database of personal data.

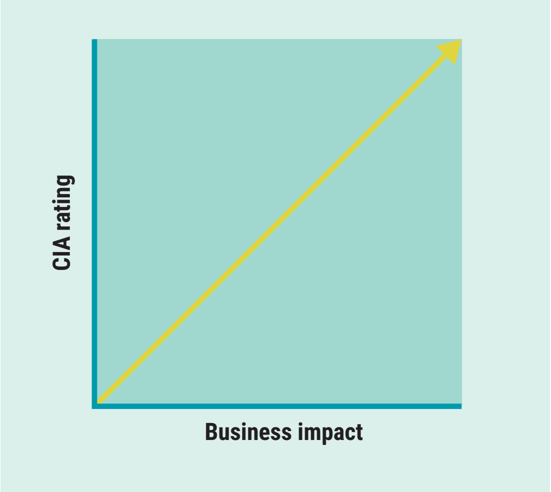
The impact of a disturbance may be related to the confidentiality, integrity and availability (CIA) model of information security:

- **Availability**—Availability is mostly affected when a disturbance occurs. This includes failures that indicate (unplanned) system failure, preventing them from being used.
- **Confidentiality**—In addition to availability, the theft of or unauthorized access to data is a common incident with a negative impact on the customer of the service.
- **Integrity**—Data can be manipulated. There is no clear distinction in the aforementioned investigations into incidents where data are/have been manipulated in the cloud; however, this is certainly a risk.

When incidents occur at a service provider, it does not automatically impact all its customers to the same extent. This could be the reason why BCI's research shows that in half of the cases, the damage is less than €50,000 while the other half has losses of more than €500 million.[10]

To assess the impact, the value of the service taken must be rated. For this purpose, NIST has issued the Special Publication (SP) standard SP 800-30.[11] This standard appoints an impact analysis based on the CIA rating. The risk of an incident having a (significantly) negative impact on an organization increases simultaneously alongside the CIA rating (**figure 4**).

Figure 4—Relation of CIA Rating on Business Impact



To determine the necessary measures to address the risk, an impact analysis must be made first. If an incident does not have a significant disrupting impact on individuals or (critical) business processes, mitigating measures may not be needed.

Getting Back Control of the Service Organization

There are several ways to test organizations on maturity in managing risk. Common assessments include requesting third-party statements and having a self-assessment carried out. Several organizations have designed vendor review frameworks, such as the Cloud Security Alliance (CSA) and ISACA. CSA has CSA START Level and Scheme Requirements,[12] where a distinction is made between the levels of assurance. The lowest level of assurance is realized by performing self-assessments. The second level of assurance is realized by third-party statements and the third level of assurance is realized by continuous auditing.

> “WHEN INCIDENTS OCCUR AT A SERVICE PROVIDER, IT DOES NOT AUTOMATICALLY IMPACT ALL ITS CUSTOMERS TO THE SAME EXTENT.”

An *ISACA® Journal* article “Vendor Risk Management Demystified”[13] mentions a framework with three levels ranked by degree of assurance. The lowest level of assurance is realized by vendor self-assessments. The second level consists of a desktop review and infrastructure assessments and provides more assurance. The highest level, an onsite review and an infrastructure and application assessment, provides the most assurance.

There are several measures that can be used to assess a suppliers’ environment:

- Certification of global standards and frameworks such as ISO 27001, Uptime TIER, TIA-942, and the Payment Card Industry Data Security Standard (PCI DSS)
- Self-assessment questionnaires for the supplier, based on standards and frameworks such as ISO 27001, Trust Service Principles and CSA
- Type II third-party reports that test the operation of measures periodically using robust standards or frameworks such as ISAE 3402/SSAE16 and SOC reports
- Continuous monitoring of measures where there is continuous insight into the functioning of an organization’s control environment and security measures

All of these measures can overlap. It cannot be taken for granted that a third-party statement Type 2 is better than a certification. On the one hand, an SOC 2 Type 2 (Type 2 third-party) report regarding availability often takes general measures in helicopter view into account. On the other hand, a certification such as Uptime TIER III will investigate more thoroughly the technical aspects. When looking at a data center, the advantage of the Uptime Tier Facility certification is that a more thorough audit is conducted on the technical aspects that ensure the technical availability, while the advantage of a SOC 2 Type 2 report is that it assures the operational effectiveness of the organization’s implemented controls. A combination of both provides assurance over a

period of time and ensures that independent professionals have taken an in-depth review and conducted multiple tests that ensure that the technical infrastructure provides the availability.

Besides the depth of investigation, the independence of the audit company and the auditors must be considered when determining a level of trust in their report. An independent firm with professionals who are compliant with professional practice regulations provides a higher level of assurance than an audit by the internal audit department of a supplier.

Best Practices for Supplier Assurance

As the impact of risk increases, more assurance over the maturity of the control environment of a supplier is desired. As the CIA rating increases (the more important the availability, integrity and confidentiality of the service for the operation of the business processes), more assurance is needed.

CIA Rating

The CIA rating consists of three factors (availability, integrity and confidentiality) that can be classified as low, moderate and high. When dealing with risk, which shows the impact on the organization, an average of the three factors cannot be used as a classification metric for said risk. For instance, a service that supports business processes where availability is extremely important but where the data that are processed are reasonably confidential and impact on integrity is fairly important would reach an average of a mid-rating; however, the impact on business processes can be the same as a service where two of three factors are scaled up to high. Hence, the highest classified factor should be used as an overall general CIA qualification.

Certifications

Based on the ratings of the separate CIA components, specific certifications might be desired. For availability, an Uptime TIER, TIA-942 or TSI certification could be recommended. For integrity and confidentiality, an ISO 27001 or PCI certification could be recommended.

Besides the framework used, it is possible to define additional requirements for certification. For example, is the certification provided by an independent contractor that just started or by an experienced audit company? The scope of the certificate (which processes and departments are audited) and levels of certification (such as multiple levels of TIERs for Uptime and different PCI standards) should also be taken into consideration.

Self-Assessments, Type 2 Third-Party Reports and Continuous Monitoring

Self-assessments, Type 2 third-party reports (i.e., SOC, ISAE3402, SSAE16) and continuous monitoring often provide overarching insight into the extent to which an organization is in control, but they can also be focused on the applicability of the demands and requirements of the customer. The reliability of the information of an assessment is often related to the frequency of an assessment and the independence of the executive body. For example, an annual self-assessment provides less assurance as to how well an organization is in control than a third-party statement provided every six months.

Conclusion

The audit of suppliers is necessary if (critical) business processes are outsourced. Disturbances within the provisioning of cloud services can occur, including the system not being available for a period of time, and cybercrime is also common. Depending on the type of service and applicability of the organization, these disturbances can have a large (financial) impact. For significant processes, the internal and external auditors should ensure that a proper monitoring process is implemented and conducted regarding third-party services.

Figure 5—Third-Party Assessment Framework

		Type of Certification per CIA		
		Confidentiality	Integrity	Availability
Low	Self-assessment	Certifications become more important as CIA qualification increases. Specific certifications depend on the service.		
Moderate	Type II third-party report			
High	Continuous monitoring and type II third-party reports			

To maintain appropriate control over suppliers, it is important to test suppliers. The more that is done to mitigate risk, the less likely risk will arise. As the CIA rating increases, more attention must be paid. A combination of assessments and certifications can be used to evaluate suppliers. The framework illustrated in **figure 5** demonstrates how the different kinds of assessments and certifications relate to the CIA rating.

The type of certification will differ based on the service. When processing payment card transactions, PCI DSS can be required if confidentiality and integrity risk regarding the transactions is deemed to be moderate or high. When selecting a data center for critical services availability, risk may be deemed to be high, and an Uptime Institute Tier IV certification can be demanded.

This framework can also be extended when there is a need to comply with regulations like the EU General Data Protection Regulation (GDPR) or the US State of California Consumer Privacy Act (CCPA). An additional column for personal identifiable information (PII) can be added and specific certifications or contractual obligations can be demanded.

Endnotes

1 Business Continuity Institute (BCI), *BCI Supply Chain Resilience Report 2019*, United Kingdom, 5 November 2019, *https://www.thebci.org/resource/bci-supply-chain-resilience-report-2019.html*

2 Uptime Institute, *Publicly Reported Outages 2018-19*, USA, March 2019, *https://uptimeinstitute.com/publicly-reported-outages-2018-19*

3 (ISC)², *2019 Cloud Security Report*, USA, August 2019, *https://www.cybersecurity-insiders.com/portfolio/2019-cloud-security-report-isc2/*

4 Microsoft Azure, "Azure Status History," *https://status.azure.com/en-us/status/history/*

5 Google Cloud, "Google Cloud Status Dashboard," *https://status.cloud.google.com/summary*

6 Amazon Web Services (AWS), "AWS Post-Event Summaries," *https://aws.amazon.com/premiumsupport/technology/pes/*

7 *Op cit* BCI

8 *Op cit* (ISC)²

9 *Op cit* Uptime Institute

10 *Op cit* BCI

11 National Institute of Standards and Technologies (NIST), NIST Special Publication (SP) 800-30, *Guide for Conducting Risk Assessments*, USA, February 2012, *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf*

12 Cloud Security Alliance (CSA), STAR Level and Scheme Requirements, 4 September 2019, *https://cloudsecurityalliance.org/artifacts/star-level-and-scheme-requirements/*

13 Patel, D.; "Vendor Risk Management Demystified," *ISACA® Journal*, vol. 4, 2015, *https://www.isaca.org/archives*