Commission de Surveillance du Secteur Financier

Version dated 4 December 2019

FAQs on the assessment of IT outsourcing materiality

Frequently Asked Questions on the assessment of IT outsourcing materiality

Disclaimer: The answers to the "Frequently Asked Questions" (hereafter "FAQs") solely intend to assist the supervised entities in assessing the materiality of their IT outsourcing projects. Based on this assessment, the supervised entities might be required to inform the CSSF or request for authorization, as specified in the circulars CSSF 12/552, 17/654, 17/656 and 18/698.

We remind the supervised institutions that whatever the materiality of an IT outsourcing, they always have to perform a due diligence and a risk analysis of their IT outsourcing project.

For clarity purpose, in this document "material IT outsourcing" refers to any "IT outsourcing that support material activities".

QUESTION 1: What does "IT outsourcing" mean?

Updated on 4 December 2019

IT outsourcing means an arrangement of any form between the institution and a service provider (including of the same group) by which that service provider performs an IT process, an IT service or an IT activity that would otherwise be undertaken by the institution itself.

QUESTION 2: What does "material activity" mean?

Date of publication: 27 March 2019

Any activity that, when it is not carried out in accordance with the rules, reduces the institution's ability to meet the regulatory requirements or to continue its operations as well as any activity necessary for sound and prudent risk management shall be deemed to be "material".

QUESTION 3: How to assess the materiality of an IT outsourcing?

Updated on 4 December 2019

An IT outsourcing is considered material if at least one of the following statements is met:

1. From a technical point of view, the outsourced IT operational functions, activities or services safeguard the security and continuity of critical parts of the IT infrastructure. A deficiency in these outsourced IT operational functions, activities or services may significantly disrupt the ability of the supervised entity to protect its IT infrastructure and, therefore, the ability of the supervised entity to operate its material activities in a controlled manner.

2. From a business point of view, the outsourced IT operational functions, activities or services support a material activity. In case of failure or dysfunction of the IT operational functions, activities or services, there is a major impact on the business activity. This major impact may be one of the following in nature[1]:
   - A **financial impact**, including (but not limited to) loss of funds or assets, potential customer compensation, legal and remediation costs, contractual damages, loss of revenue.
   - A **potential for business disruption**, considering (but not limited to) the criticality of the financial services affected; the number of customers and/or branches and employees potentially affected.
   - A **potential reputational impact** on the institution based on the criticality of the financial service or operational activity affected (e.g. theft of an important volume of customer data); the external profile/visibility of the IT systems and services affected (e.g. mobile or on-line banking systems, point of sale, ATMs or payment systems).
   - A **regulatory impact**, including the potential for public censure by the regulator, fines or even variation of permissions.
   - A **strategic impact** on the institution, for example if strategic product or business plans are compromised or stolen.

QUESTION 4: Can you provide examples of materiality assessment for IT outsourcing?

Date of publication: 27 March 2019

The following examples use the above mentioned definitions and rules to assess the materiality of an IT outsourcing.

Please note that the following examples only intend to help the supervised entities in their assessment of materiality, they cannot be generalized. Each entity should be challenge and adapt to its own case.

Example 1: Portfolio Valuation systems

Your institution intends to outsource the Portfolio Valuation systems. The business operations will remain at your institution.

You have assessed that this project is an “IT outsourcing” because an external provider will perform the IT operational functions (e.g. the hosting, change management, security and backup operations).

You have also assessed that the Portfolio Valuation systems support the “portfolio valuation” process of your institution. You have assessed that a failure of the outsourced IT systems would discontinue the portfolio valuation process and such a failure would have financial and reputation impacts.

As a consequence, you have concluded that the IT outsourcing that is foreseen by your institution would support material activities and is therefore a material IT outsourcing.

Example 2: Backup storage

Your institution intends to outsource the backup storage to a third party.

You have assessed that this project is an “IT outsourcing” because an external provider will perform IT operational functions (in this case, the backup storage of all your IT systems).

[1] Reference: EBA/GL/2017/05

In this example, we will use two different scenarios to evaluate the materiality of the IT outsourcing.

- Scenario A: Your institution also keeps a copy of the backups in a backup storage location and uses the external service provider as an additional continuity measure. In this scenario, you intend to mitigate the risk of a disaster that would impact both your IT production environment and the location where your backups are stored. You have assessed that a failure of the external IT service provider would not impact the continuity of your IT and business services, as it is very unlikely that the three different sites fail at the same time (your IT production environment, your backup storage location and the service provider's location). Also, the backups are stored encrypted and your institution keeps the encryption key, hence you have assessed that a data leak would not impact the reputation of your institution. Therefore, you have concluded that this IT outsourcing is not material.
- Scenario B: Your institution solely relies on the external provider for the storage of the backup. In this scenario, the outsourced IT systems safeguards the continuity of critical parts of your IT infrastructure and also the business activities. Therefore, you have concluded that this IT outsourcing is material.

Example 3: Ticketing system

Your institution intends to outsource the hosting of the ticketing system supporting your "help desk" function and the related IT operations (change management of the ticketing system, backup of the ticketing system, etc.).

You have assessed that this project is an "IT outsourcing" because an external provider will perform IT operational functions.

In case of failure of the ticketing system that is hosted by the external provider, your institution has implemented an alternate procedure, enabling the help desk function to continue its activities. Also, your institution keeps a regular copy of the data in the ticketing system and would be able to deploy the ticketing system internally or to another external service provider. In addition, you have assessed that no sensitive data will be stored in the ticketing system, hence a data leakage would not significantly impact the reputation of your institution. Finally, you have assessed that no material activity would be impacted by a failure of the ticketing system. Therefore, you have concluded that this IT outsourcing is not material.

Example 4: Internet banking application

Your institution intends to outsource the hosting of the internet banking application and the related IT operations (change management of the internet banking application, backup of the internet banking application, etc.).

You have assessed that this project is an "IT outsourcing" because an external provider will perform IT operational functions.

In this example, we will use three different scenarios to evaluate the materiality of the IT outsourcing.

- Scenario A: Your internet banking application is a consultative web site, your clients can only view the balances of their bank accounts, in an anonymized manner. You have assessed that a failure of your internet banking application would have limited impacts and would not prevent your material activities to continue. Also, you have assessed that a data leakage would have limited reputational impact due to the anonymization. Therefore, you have concluded that this IT outsourcing is not material.
- Scenario B: Your institution significantly relies on the internet banking application, the "online banking" is a core activity of your bank. In this case, you have assessed that a failure of the internet banking application would have major impacts on material activities. Therefore, you have concluded that this IT outsourcing is material.
- Scenario C: The internet banking application is available to your customer, in addition to a wide network of agencies. You have analysed that a data leakage would not have a significant impact on your reputation. Moreover, you have analysed that in case of failure of the internet banking application, the customers can come back to one of your agencies. Therefore, you have defined a threshold on the number of customers using mainly the internet banking application instead of visiting an agency and you decide the outsourcing not to be material below this threshold. You frequently monitor the number of agencies using this application to possibly requalify the materiality of the IT outsourcing.

Example 5: Email system

Your institution intends to outsource the hosting of the email system.

You have assessed that this project is an "IT outsourcing" because an external provider will perform IT operational functions (i.e. the hosting of the email system and maintenance operations).

In this example, we will use two different scenarios to evaluate the materiality of the IT outsourcing.

- Scenario A: Your email system is used for internal and external communication but they are not time critical and other alternative means of communication are easily available. Also, you intend to backup the emails and store a copy at your premises. You have assessed that a failure of the email system would not have significant impact on your business activities and you would be able to quickly redeploy an email system by restoring your backup files. Finally, you have assessed that a data leakage would only have limited impact on your company reputation (mainly because your internal policy forbids the use of email for the exchange of sensitive information). Therefore, you have concluded that this IT outsourcing is not material.
- Scenario B: Your email system is used for internal and external communication and you have several business processes that highly rely on emails, without alternative means. You have assessed that a failure of the email system would have a significant business impact. Therefore, you have concluded that this IT outsourcing is material.

The same reasoning may also apply for Voice-over-IP (VoIP) / telephony to determine the materiality of VoIP / telephony outsourcing.

Example 6: Firewall

Your institution intends to outsource the hosting of a firewall.

You have assessed that this project is an "IT outsourcing" because an external provider will perform IT operational functions (i.e. the hosting of the firewall and maintenance operations).

In this example, we will use two different scenarios to evaluate the materiality of the IT outsourcing.

- Scenario A: This firewall will only be used to filter traffic for remote access to your institution's network. You have evaluated that, in case of failure of the outsourced firewall, your internal network would not be accessible from outside of your institution (e.g. the firewall is configured to fail closed). You have assessed that this would not have a significant impact on your business activities (e.g. because the remote access is only used in case of exceptional working from home) and you would be able to quickly resolve the situation (e.g. by implementing an alternate firewall). Also, you have assessed that only encrypted data will transit through the firewalls, as only encrypted communications are authorized for remote access; hence, you have assessed that a data leakage would not have impact on the reputation of your institution. Therefore, you have concluded that this IT outsourcing is not material.
- Scenario B: The firewall is used to filter all inbound and outbound traffic. You have assessed that a failure of the firewall would open all your network ports, hence putting at stake the security of your institution and you would lose control over your internal network. Therefore, you have concluded that this IT outsourcing is material.

Example 7: Disaster Recovery Plan (DRP)

Your institution intends to outsource the hosting of infrastructure that is used in case of disaster.

You have assessed that this project is an "IT outsourcing" because an external provider will perform IT operational functions (i.e. the hosting of the systems and maintenance operations).

In this example, we will use two different scenarios to evaluate the materiality of the IT outsourcing.

- Scenario A: Your institution intends to use this outsourced infrastructure in case of disaster affecting IT systems that support non-business-critical activities (e.g. the hosting of your public web site). In the event of a disaster, you have evaluated that a failure of the DRP infrastructure would not have significant business impact. Also, you have assessed that a data leakage would not have reputational impact as the information is public. Therefore, you have concluded that this IT outsourcing is not material.
- Scenario B: Your institution intends to use this outsourced infrastructure in case of disaster affecting your main IT infrastructure, hence this outsourced infrastructure supports the continuity needs of all your business activities. In the event of a disaster, a failure of the DRP infrastructure would have both a business impact and a regulatory impact. Indeed, as stated several in CSSF circulars (e.g. 12/552, 17/654, 17/656), your institution shall be able to continue its critical functions in case of exceptional events or crisis. A failure of ensuring continuity would be in breach with the CSSF requirements. Therefore, you have concluded that this IT outsourcing is material.