RISK MANAGEMENT MAGAZINE

Vol. 16, Issue 1
January – April 2021

EXCERPT

https://www.aifirm.it/newsletter/progetto-editoriale/

A possible holistic framework to manage ICT third-party risk in the age of cyber risk

Andrea Giacchero and Jacopo Moretti

A possible holistic framework to manage ICT third-party risk in the age of cyber risk

Andrea Giacchero and Jacopo Moretti (Cassa Depositi e Prestiti)[1]

Article submitted to double-blind peer review, received on 30th March 2020 and accepted on 16th February 2021

Abstract

Third-party risk for external ICT services, which concerns both the outsourced services and the third-party products, is a crucial issue for a financial institution, because a cyber attack on a vendor can be a threat for the data of its customers.

For this reason, financial institutions should adopt a holistic risk management framework to stress the effectiveness of the mitigating actions even when they engage a third-party provider.

Risk analysis of external ICT services is necessary to prepare proper mitigation plans that provide enough resources allocation. This paper proposes a possible management framework whose aim is providing indications on security measures and controls to implement against the possible sources of ICT third-party risk, and defining a proper internal process that a financial institution should adopt. In this context, the framework also embodies a model to pick the best vendor among those that a financial institution could choose for an ICT service, which is based on a risk assessment technique focused on the three information security dimensions (confidentiality, integrity, and availability) and on the Borda method.

*****

La gestione dei rischi connessi a servizi ICT esterni (sia servizi ICT in outsourcing sia quelli forniti da terze parti) è un tema cruciale per gli istituti finanziari, dal momento che un attacco cyber nei confronti di un fornitore rappresenta una minaccia per i dati dei suoi clienti.

Gli istituti finanziari dovrebbero implementare un framework di risk management olistico al fine di stressare l'efficacia delle azioni di mitigazione anche nel caso in cui decidano di affidarsi ad un fornitore terzo.

L'analisi dei rischi connessi ai servizi ICT esterni è propedeutica alla definizione di piani di mitigazione che prevedano un'adeguata allocazione di risorse. Il presente paper propone un possibile framework di gestione che mira a fornire indicazioni sulle misure di sicurezza e sui controlli da implementare in merito alle possibili fonti di rischio e a definire un robusto processo interno di gestione. Il framework prevede un modello per scegliere il miglior fornitore - tra una lista di possibili fornitori - per un servizio ICT: tale modello è basato su un risk assessment incentrato sulle tre dimensioni di sicurezza delle informazioni (riservatezza, integrità e disponibilità) e sul metodo Borda.

Keywords: third-party risk; operational risk management; ICT risk assessment.

DOI 10.47473/2020rmm0082

1. Introduction

New technologies entail an evolution of the business models that leads financial institution to implement external Information and Communication Technologies (ICT) services to quickly put in place solutions not available within the organization.

Since 2017, ICT outsourcing risk (together with legal and reputational risks) is one of the main concerns for the Top Management of the European banks according to the yearly survey on European banking system published by European Banking Authority (EBA). Furthermore, outsourcing risk is one of the Top 10 operational risks for 2019 according to a survey of Risk.net[2]. Also, the Operational Riskdata eXchange Association (ORX) highlights that third-party risk is one of the Top 5 emerging operational risks[3]. Thus, there is a wide agreement between authorities and practitioners in considering ICT third-party risk as a priority for a financial institution. The adoption of financial technology (fintech) of third-party service providers poses operational risks that need to be carefully managed to maintain an effective oversight of the emerging risks related to new technologies, which may require specialist competencies (Basel Committee on Banking Supervision, 2018).

In this context, a financial institution should increase its operational resilience, which refers to the ability of absorbing and adapting to shocks due to the impact of any disruption to the outsourced function or failure of the service provided (European Banking Authority, 2019A). External ICT services, indeed, embodies new risk sources in the concept of outsourcing risk, which is the risk that <<*engaging a third party, or another Group entity (intra-group outsourcing), to provide ICT systems or related services adversely impacts the institution's performance and risk management*>> (European Banking Authority, 2017).

The purpose of this paper is to define a third-party risk management framework for external ICT services (which concerns both the outsourced services and the third-party products) that a financial institution could implement.

[1] The authors report no conflicts of interest. The authors alone are responsible for the content and writing of the paper

[2] https://www.risk.net/risk-management/6470126/top-10-op-risks-2019#cxrecs_s.

[3] https://managingrisktogether.orx.org/research/operational-risk-horizon-2019

The proposed framework, inspired by the EBA Guidelines (European Banking Authority, 2019A) and by the Circular 285/2013 of Banca d'Italia (Banca d'Italia, 2013), describes the steps that a financial institution should put in place to handle the resort to an external ICT service, providing the implementation of organizational information security measures and evaluate the adequacy of such measures. Indeed, a financial institution must identify, assess, monitor, manage, and mitigate all the risks associated with an external ICT service. More precisely, the framework provides a model that contains the guidelines to choose the best vendor for a given ICT service using a risk assessment methodology based on the three information security dimensions, namely confidentiality, integrity, and availability. However, the framework we propose can also be useful for companies of other industries that use external ICT services, indeed, the phases of the management process described in Section 3 represent general rules to follow.

When a financial institution needs to implement a new ICT service always faces a so-called 'make-or-buy' decision, namely choosing which activities <<should be provided 'in-house', and which should be bought in>> (Ford & Farmer, 1986). Walker & Weber studied the effects of cost and uncertainty (Walker & Weber, 1984), as well as the interaction between the market competition and uncertainty (Walker & Weber, 1987) on 'make-or-buy' decisions. According to the authors, the comparative analysis of production costs is the strongest criterion that influences the decision, even though both the volume uncertainty and the supplier market competition present significant effects. However, in recent years, regulators are increasingly drawing the attention also to risk management aspects.

A financial institution that decides to resort to an external ICT service must clearly define which part of the service remains under the domain of the organization and which part is handled by the vendor (Boardman & Sauser, 2008). Understanding the boundary between internal and external domain is crucial to define rôles and responsibilities in managing an external ICT service (Power, Desouza, & Bonifazi, 2006).

All the innovative projects implemented by a financial institution together with a third-party provider in the ICT field could increase the ICT risk, especially because information asymmetry could weaken the effectiveness of the oversight on vendor's information security measures (Banca d'Italia, 2019).

An external ICT service requires an agreement of whatever sort between a financial institution and a supplier. This agreement must prescribe how the supplier execute an internal process, a service, or an activity on behalf of the financial institution. The definition of the agreement with a third-party must specify whether the ICT service is an outsourced service or a third-party product. In case of an outsourced ICT service, the financial institution should assess whether would realistically be able to implement the service (even if the company has never implemented the service). Note that, as a general rule, outsourcing is a viable solution to carry out the business services of a company for several reasons, indeed, it permits e.g. to focus on core business functions, to compensate a lack of capabilities, and to acquire quickly current technologies. For larger-sized companies, ICT outsourcing is mainly motivated by strategy, while firms with smaller ICT staff and fewer resources resort to ICT vendor because of economic reasons (González, Gascó, & Llopis, 2016). In this context, ICT third-party providers bring extensive world-class resources, such as access to new technology, tools and techniques that a financial institution may not have, together with and a competitive advantage through expanded skills (Ghodeswar & Vaidyanathan, 2008). ICT vendors strengthen the value chain of their customers making available the industry best practices to use assets more effectively and efficiently (Farrell, 2004).

For many organizations, outsourcing and third-party products are 'silver bullets' to solve operational drawbacks (Power, Bonifazi, & Desouza, 2004). In particular, purchasing external ICT services represents one of the most important and successful strategies to reduce organization's ICT cost and to focus the efforts on their core business rather to ICT operational activities. However, ICT outsourcing can be the source of serious information security risks. Therefore, risk analysis of external ICT services is necessary to prepare proper mitigation plans that provide enough resources allocation (Khidzir, Mohamed, & Arshad, 2013).

As a general rule, a financial institution resorts to an outsourcing agreement when it decides to commit to a third-party the management and the responsibility of an ICT service that supports its core business, due to the lack of adequate internal resources and expertise. On the other hand, we refer to a third-party product when the external ICT service supports activities different from the core business. We refer to a third-party product even when an ICT service supports core business activities, but the government of the system remains under the responsibility of the financial institution.

A financial institution should implement a unique internal process to assess and manage the ICT third-party risk, both for the outsourced ICT services and the third-party products. However, the outsourced ICT services require a more complex approach to execute an ex-ante assessment on the potential outsourcing that involves several functions of the financial institution (e.g., Risk Management, Compliance, ICT). During the assessment, the financial institution should - inter alia - provide a cost-benefit analysis and stress both its ability to re-internalize the activities and the reliability of the potential vendors. The risk assessment framework should embody tacit and explicit knowledge together, even if the former factor is more difficult to formalise or standardise in the renewal of a third-party provider contract with respect to the latter one (Currie, 2003). In other words, as it creates a structure of formal and informal relationships, mitigation of ICT outsourcing risk also depends on relationship management between vendor and client (Levina & Ross, 2003). For the particular case of application development vendors, a company should also evaluate the size and typology of the project, and also future business (Gopal, Sivaramakrishnan, Krishnan, & Mukhopadhyay, 2003). However, today the recourse to outsourced ICT services and third-party products is a common practice among financial institutions (regardless of their dimensions), which concerns several kind of ICT services (e.g., applications, software development, software maintenance, network and server management). Thus, as ICT third-party risk management is a main concern for all the financial institutions (Haller & Wallen, 2016), the Board of Directors and senior management of a financial institution must ensure that outsourced activities are conducted in a safe-and-

sound manner (Board of Governors of the Federal Reserve System, 2013).The paper is organized as follows: Section 2 provides a list of potential third-party risk sub-categories. In Section 3 and in its sub-sections is elicited a possible framework to manage ICT third-party risk while the conclusions are presented in Section 4.

2. Third-party risks

In the context of a globalized economy, the complexity of the outsourcing projects is continuing to increase also due to the number of parties involved (Power, Desouza, & Bonifazi, 2006).

Consequently, a financial institution - instead of focusing on the short term costs - should decide to outsource an activity both considering its long-term needs in terms of know-how and quality, and the risks that the outsourcing could imply (Prasad & Prasad, 2007). According to Gandhi et al. (Gandhi, Gorod, & Sauser, 2012), the identification of the third-party risk typologies and their prioritization becomes a key factor to the success of an outsourcing project and to guarantee a competitive advantage.

For these reasons, the decision concerning the outsourcing of an ICT service is subject to a periodic review (Carter, Maltz, Yan, & Maltz, 2008). Layton et al. state (Layton, Zechnich, & al., 2008) that the risk identification phase should be preliminary with respect to the decision of picking an outsourcer and that this phase should provide a risk management holistic approach for the entire outsourcing life cycle. In the first place, according to (Bott & Milkau, 2015), before resorting to an outsourcer a financial institution should manage a strategic risk which concerns a 'make or buy' decision to optimize the available resources (e.g., cash flows, workforce).

ICT third-party risk is an endogenous risk for a financial institution, because it concerns a choice between outsource or doing an activity, and between several possible vendors for a given activity (Aubert, Benoit, Patry, & Suzanne, 2005).
Nakatsu and Iacovou (Nakatsu & Iacovou, 2009) use a Delphi survey[4] to list the main risks related to ICT outsourcing. In a decreasing order of importance, the authors cite the lack of communication, poor change controls, absence of top management support, failure to manage end-user expectations, lack of customer's project management know-how, and inadequate vendor's staffing by vendor.
A complete list of potential risks that could be connected to a third-party relationship is difficult. However, below we try to synthesize the main ICT third-party risks[5]:

a) choosing an inappropriate vendor that negatively influences the execution of a project. A common error is choosing a vendor with a procurement process based on a 'race to the bottom' economic offer (the so-called 'winner's curse' phenomenon), which could push the vendor to stress its managers to achieve the expected profits even in adverse circumstances for the customer (Feeny, Lacity, & Willcocks, 2005). Thus, a financial institution should choose a vendor on the basis of several attributes like reputation, experience, and price instead of just picking the one with the lowest cost (Ruzaini, Aris, Arshad, & Mohamed, 2008);
b) insufficient expertise of the vendor which, once concluded the agreement, sends its most talented employees in search of new customers (Sullivan & Ngwenyama, 2005);
c) overdependence on a single vendor, which would be difficult to substitute in case of evident inefficiencies without an exit strategy (Bahli & Rivard, Validating Measures of Information Technology Outsourcing Risks Factors, 2005). Since many ICT projects are not separable, the management by different providers may turn out to be difficult (Fan, Suo, & Feng, 2012). However, re-internalizing an outsourced function could be a quite difficult and long process, especially in case of a full outsourcing (Harland, Knight, Lamming, & Walker, 2005), mainly because of the high costs involved in recreating the ICT department and hiring the staff for it (Earl, 1996);
d) economic aid to a vendor under financial stress (so-called 'step-in risk') to protect the company from potential reputational damages due to the vendor;
e) violation of the contractual clauses with respect to the execution of the activities from the vendor (Carter, Maltz, Yan, & Maltz, 2008);
f) loss of know-how, due both to an inadequate training of the internal staff and to an insufficient transfer of knowledge from the vendor (Verwaal, Verdu, & Recter, 2008);
g) disruption of the business continuity, which could cause huge financial losses;
h) security threats, both for possible personal data leakage and cyber-attacks. The risks linked to the storage and transfer of data stems from the faculty of accessing to systems and to customer data attributed to the vendor. Indeed, the cyber risk management in financial institutions should consider several items, including third-party risk management (e.g., especially in case of cloud computing providers who are not subject to the regulation of the financial sector authorities) (Financial Stability Board, 2018). The typology of contractual agreement directly influences potential information security threats (Alner, 2001).

Information security risk is one of the most critical risk sub-category of ICT third-party risk (Davison, 2003). Typical examples of information security risks are theft of personal data, information leakage, extraction and unauthorized manipulation of intellectual properties (Hinson, 2007). These risks, caused by lack of control on threats and vulnerabilities, refer to natural or man-made events that could have an adverse impact on organizational assets (Kaplan R. , 2004). Regardless

[4] <<Technique using a group of people who are either involved or interested in the research topic to generate and select a more specific research idea>> (Saunders, Lewis, & Thornhill, 2009).
[5] See also (de Sá-Soares, Soares, & Arnaud, 2014) and (Shroff & Bandi, 2018) for a comprehensive catalog information system outsourcing risks and for a list of possible misconduct risk, respectively.

of the benefits of outsourcing services, a company must consider all the activities, internal processes, and controls to protect information, data, and their underlying infrastructures. In this context, confidentiality, integrity, and availability represent the core values of information security (Vorster & Labuschagne, 2005) that a financial institution should always monitor. Confidentiality refers to the restrictions on the use of different kinds of information, while integrity is the assurance that information has not been adulterated and availability is the guarantee that only authorized users have access to information and connected assets when required (Parker, 2002). The growing interconnectivity between a financial institution and their third-parties amplifies the risk that the attack vector is a third-party vendor (Mallinder & Drabwell, 2013).
Other critical risks in ICT outsourcing projects regards complexity management, due to the use of new technologies, and team risks, both concerning communication problems and conflicts between customer and seller due to divergent work styles (Abdullah & Verner, 2012). In addition to the risks described above, a financial institution should also consider other kind of risks, such as liquidity, interest rate, pricing, legal, and foreign currency translation risk (Federal Deposit Insurance Corporation, 2019).
Third-party risk can be also related to frequent staff and senior management changes at the service provider (McCahery & de Roode, 2018). Furthermore, a company could face a strong opposition if its staff consider outsourcing as a threat to their jobs (Brooks, 2006), consequently, the situation of uncertainty caused by outsourcing could lead to low productivity, loss of motivation, and anxiety (Walden & Hoffman, 2007).
Financial institutions should make a risk analysis to weigh the dependencies from third parties in their supply chain, aiming at identifying the best solutions to improve cyber resilience (especially in case of third parties not subject to banking supervision) and at improving ICT risk management (Basel Committee on Banking Supervision, 2018). To guarantee a strong oversight on cyber risk, financial institutions should implement an ex ante risk assessment activity and an ongoing monitoring based on the same framework established for ICT risk management. An integrated approach is necessary to manage the risk assessment process across the entire supply chains (Kleindorfer & Saad, 2005). To strengthen their resilience and to deal with unexpected events, financial institutions should increase their flexibility (Waters, 2011). In particular, developing digital resilience is necessary to design business processes and technology architectures together with the cybersecurity defenses needed to protect critical information assets (Kaplan, Bailey, O'Halloran, Marcus, & Rezek, 2015). The Tiber EU (European Framework for Threat Intelligence-based Ethical Red Teaming) issued by the European Central Bank provides a set of guidelines to financial institutions to execute the penetration testing activity (on a voluntary or on a mandatory basis) aiming at verifying the cyber-resilience of the institutions. If the infrastructure outsourced and a third party is included in the scope of the test, it is necessary to include all the information about that third party (European Central Bank, 2018).

Concerning both the security of data (focusing, in particular, on personal and confidential data) and of the applications, financial institutions should choose vendors which present high information security standards levels, constantly monitoring the respect of these standards. In view of the weakest link principle, information security is a broader theme that interests all the player of the markets, instead of being a worry just for the single participant and for the suppliers of critical ICT services (European Banking Authority, 2019B). Also the G7 Cyber Expert Group - whose mission is addressing the increase in sophistication, frequency, and persistence of cyber threats in the financial sector - stressed the importance of establishing an adequate strategy and a strong framework for information security in terms of nature, dimension, complexity, risk profile, and culture of the single financial institution, especially for ICT services provided by third parties (European Commission - G7 Cyber Expert Group, 2016).

ICT third-party risks are currently exacerbated due to tighter regulatory requirements in the field of data processing and of data security (Vőneki, 2018). More precisely, for the personal data that are stored (or that are going to be stored), information security measures should be applied both to the automatic and to the manual data processing, so that the protection of any physical person is technologically neutral and does not depend on the techniques employed (European Parliament, 2016).

3. A possible ICT third-party risk management framework

The ex-ante analysis of the ICT third-party risk requires the implementation of a risk assessment based on the three drivers (confidentiality, integrity, and availability) provided by the EBA (European Banking Authority, 2019B), and on specific further information on the vendors, which could be necessary due to the riskiness of the external ICT services. The main aim of the risk assessment is to verify the adequacy of the security measures to mitigate ICT third-party risk. In case of an outsourced core function, a financial institution could provide a more detailed due diligence about the future trustworthiness of the vendor to express a risk opinion on the decision to resort to a third-party.

Risk exposure, once made explicit, converts the unexpected into an option selected intentionally, being aware of what it is selected and what it is discarded. Thus, the risk assessment essentially concerns an analysis of the vendor's financial statement and strategy to determine its creditworthiness. Furthermore, the risk assessment provides a risk concentration analysis based on the vendor portfolio for ICT services. In this context, a financial institution should continuously monitor the adequacy of the procedures and of the security measures adopted by the vendors of its external ICT services. This monitoring constitutes an ex-post analysis aiming at identifying possible changes that could undermine the stability and the performance of the same vendors.

The risk opinion on the decision to entrust to a third-party an ICT service is generally preliminary with respect to the settlement of the contractual agreements, which define the responsibilities about the management of the ICT services mentioned in the contract. In line with a risk-based approach, the higher the riskiness of an ICT service, the higher the number of the protection clauses. This opinion should also assess the risk of supplier's ecological or social misconduct (Khidzir, Mohamed, & Arshad, 2013).

Taking inspiration from EBA Guidelines (European Banking Authority, 2019A), the ICT third-party risk management internal process can be divided into three main phases:

a) **ex-ante analysis of initiative approval and vendor selection**, in which the financial institution should assess the potential impact of the agreement with a third-party in terms of operational, compliance, and reputational risk, as to verify whether the agreement increases the risk exposure. Specifically, the risk assessment should consider both the data classification and the relevance of the reference operation to evaluate – inter alia – potential risks as losing the direct control of the critical components of the external ICT service, data leakage, and unauthorized use of company's tools subsequent to a cyber-attack;
b) **contractualization**, to establish proper protection clauses, in coherence with the service configuration. For instance, the protection clauses should prescribe that the vendor respects the information security policies of the customer[6] and should provide one or more exit strategies;
c) **monitoring of the external ICT services**, which should provide (i) a monitoring procedure on vendor's activities, according to a method and a frequency compliant with the riskiness of the internal processes supported, (ii) an internal Contact Person (CP) for the external ICT service dedicated to the implementation of the security measures against potential threats and vulnerabilities, and (iii) periodic reports to the internal control functions.

Thus, a financial institution that resorts to an external ICT service must adopt a control framework for all these phases of the procurement process.

The following sub-sections provide a more detailed description of the security measures related to the three main phases of the procurement process.

3.1 Ex-ante analysis of initiative approval and vendor selection

Before the initiative approval, the financial institution should nominate an internal CP for the ICT service[7], which has the appropriate skill to classify the external ICT service, to put in place the preliminary risk assessment, and to control the activities carried out by the vendor. The CP is responsible for the management of the contract and, in particular, both for executing controls on external ICT services and for sending periodic reports to the internal control functions.

The set of external ICT service would constitute an inventory, which should contain several information (e.g., data typology, internal processes supported by the ICT service, list of users) that may contribute to make a more precise risk assessment of the ICT services. To be effective, the CPs should continuously update the inventory for any substantial change (e.g., purchase of a new external ICT service, new and different kind of data inserted in the service).

A CP, using the information of the inventory, classifies an external ICT service (before its purchase), distinguish between the outsourced services and the third-party products. According to the classification of the external ICT service classification, the CP defines a proper set of security measures. As a matter of principle, a financial institution should adopt the same set of security measures for all the external ICT services, regardless of their classification.

However, the staff that a company dedicates to these controls is generally limited, thus, it is convenient to divide external ICT services into homogeneous clusters and rank these services in terms of their riskiness. Note that, as a general rule, outsourced ICT services require a higher number of security measures, while, among the third-party products, the company should identify (at least) two different clusters to distinguish the services that require stronger measures from those with a non-material riskiness (e.g., hardware assistance).

As already mentioned, for the outsourced ICT services, the financial institution should assess its ability to re-internalize the activities if necessary. Thus, the company should maintain the technical and managerial skills to re-internalize the outsourced activities, complying with the current regulatory requirements.

Before the conclusion of an agreement with the vendor, a financial institution should perform a preliminary risk assessment. Indeed, after the classification of an ICT service within a cluster, to comply with the regulator, the financial institution should assess the inherent riskiness of that service. As a general rule, one should estimate inherent riskiness for all the contracts related to a vendor of an ICT service. The aim of the risk assessment is ranking - in a decreasing order of riskiness - the potential vendors for an ICT service, starting from those with the highest rating class.

The preliminary risk assessment should, however, estimate a residual riskiness to verify that the vendor respects the standard of the financial institution in terms of information security measures. A financial institution should perform this assessment in case of new ICT services, updates of an existing one, major incidents that significantly modify the risk profile of the vendor, and/or for significant changes in the internal processes that the ICT services support.

More precisely, the analysis provides the following steps:

- Inherent risk calculation
- Vendor's controls adequacy calculation
- Residual risk calculation

[6] Including a correct treatment of the data based on their classification (e.g. confidential, sensitive).
[7] It would be desirable to choose an employee of the ICT function.

Often, when a company decides to acquire a new ICT service, it has not historical loss data and (sometimes) process owners are inexperienced in managing the operations, thus the estimation of probability and of the potential impacts stemming from risk events is very hard. For this reason, the risk assessment approach described in this paper does not require expert opinions. Indeed, the methodology provides a list of multiple-choice questions centered around the three dimensions of information security, namely confidentiality, integrity, and availability (Khidzir, Mohamed, & Arshad, 2013).

The main aim of this risk assessment is comparing the riskiness of the potential vendors of a given ICT service for a company. This approach is coherent with a security-by-design concept in which companies use ICT services to develop their products in step with their cybersecurity. Indeed, a company should run the risk assessment during the vendor selection for an ICT service.
We propose a qualitative model that match the scores of the inherent risk and the vendor's control adequacy to proper rating classes (represented on a color scale). The model combines the inherent risk rating and the vendor's control adequacy rating by using a heat map[8] to calculate a residual risk rating.

Inherent risk calculation

A first set of multiple-choice questions concerns the estimation of the three inherent risk ratings, one for each information security dimension of the ICT service. The information needed to answer these questions should be known for a company so that the CP could estimate the inherent riskiness of the pair ICT service/vendor by its own. For illustrative purposes, Table 1 provides an example of questions and possible answers (together with a numerical score) for each of the three information security dimensions. Note that the methodology provides a 'yes or no' answer for all the questions (this is a convenient approach to make the output of the analysis easier to interpret).

Information security dimension	Question	Possible answers (score_IR)
Confidentiality	Does the ICT service handle confidential data?	Yes (1) No (0)
Integrity	Does the ICT service handle data to be included in the financial statement?	Yes (1) No (0)
Availability	Does the ICT service provide more than 100 users?	Yes (1) No (0)

Table 1 - Possible questions for the calculation of the inherent risk rating

For instance, a company could calculate this inherent risk rating assigning a score to each of the possible answers of every single question. Summing up the scores of all the questions, a company could estimate an inherent risk rating by choosing appropriate cutoffs for the range of possible scores. Table 2 lists the set of inherent risk rating classes (in a decreasing order of significance) based on an illustrative set of ranges for the quotient 'score_IR summation / max potential score_IR summation' (IR_SCORE).

Risk Rating class	IR_SCORE
Very High	100% ├ 75%
High	75% ├ 50%
Medium	50% ├ 25%
Low	25% ├ 0%

Table 2 - Inherent risk rating classes

In Table 2 we match the 4 score ranges defined to as many risk rating classes, where different levels of criticality are represented by different colors on an appropriate color scale. For instance, the red class stands for a 'Very High' inherent risk.

Vendor's controls adequacy calculation

Each vendor must provide the information to answer to a second set of multiple-choice questions that aims at verifying its internal control systems. These answers lead to a controls adequacy rating of a given vendor with respect to a given ICT service (to calculate this rating, a company should sum up the score of all the questions, as for the inherent risk rating). Table 3 provides some possible questions and answers (together with a numerical score) to determine the vendor's controls adequacy with respect to each of the three information security dimensions.

[8] A two-dimensional data representation in which colors represent the output.

Information security dimension	Question	Possible answers (score_CA)
Confidentiality	Does the vendor have a Security Operation Center?	Yes (1) No (0)
Integrity	Does the vendor shield all its devices with an anti-malware protection?	Yes (1) No (0)
Availability	Does the vendor back up the data?	Yes (1) No (0)

Table 3 - Possible questions for the estimation of the vendor's controls adequacy rating

Table 4 lists the set of vendor's controls adequacy classes based on an illustrative set of ranges for the quotient 'score_CA summation / max potential score_CA summation' (CA_SCORE).

Vendor's controls adequacy rating class	CA_SCORE
Adequate	100% - 75%
Partially adequate	75% - 50%
Partially inadequate	50% - 25%
Inadequate	25% - 0%

Table 4 - Vendor's internal controls adequacy rating classes

In Table 4 we match the 4 score ranges defined to as many vendor's internal controls adequacy rating classes, where different levels of criticality are represented by different colors on an appropriate color scale.

Residual risk calculation

Combining the inherent risk rating and the vendor's controls adequacy rating (both represented on the color scale), by using for example the illustrative heat map in Fig. 1, a company can estimate the residual riskiness for each of the information security dimensions. The colors of the heat map represent the residual risk areas: the red cells indicate 'Very High' risks, the orange cells indicate 'High' risks, the yellow cells indicate 'Medium' risks, and the 'Green' cells indicate 'Low' risks. The overall residual riskiness, which is a qualitative measure to compare the potential vendors of an ICT service, is equal to the highest residual riskiness among those of the information security dimensions due to a prudential approach.

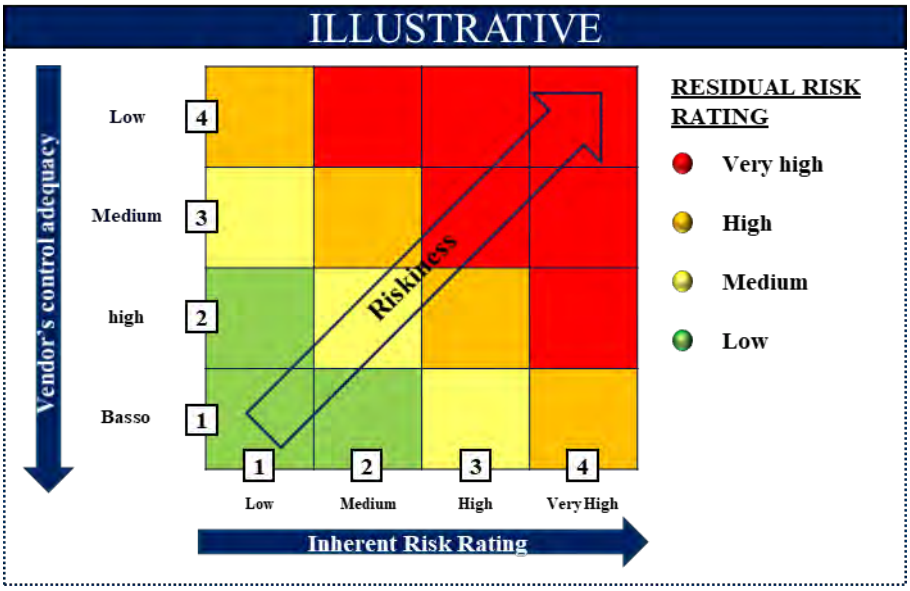

Figure 1 - Vendor's internal controls adequacy classes

The results of the preliminary risk assessment are useful but not binding for the conclusion of the agreement with a vendor. Indeed, these results provide a qualitative riskiness of a given ICT service and an indication on the maturity degree of both the technological and managerial measures that the vendor implemented. Thus, the residual riskiness is one of the criteria of the vendor selection activity. Furthermore, the company should always verify that the residual riskiness of the ICT service is compatible with its risk appetite: otherwise, the company could decide either not to implement the ICT service or to tolerate the risk. Indeed, deciding whether implementing a new external ICT service depends both on the risk appetite and on the strategic business choices.

The residual risk rating classes allow to rank the potential vendors of an ICT service in terms of their residual riskiness. However, two or more vendors could present the same residual risk for a given ICT service. In this case, the methodology provides the application of the Borda Method (Lansdowne & Woodward, 1996) to rank - in a decreasing order of riskiness - vendors with the same residual risk. More precisely, the approach provides that the vendors would be ranked by 3 criteria, namely:

1. Score of the questions to estimate vendor's controls adequacy of the confidentiality dimension (CON_CON)
2. Score of the questions to estimate vendor's controls adequacy of the integrity dimension (CON_INT)
3. Score of the questions to estimate vendor's controls adequacy of the availability dimension (CON_AVA)

The Borda Method provides to sort the scores of each criterion to achieve 6 rankings of the potential vendors of an ICT service. In case of a 'tie' between the scores of two or more vendors for a given criterion, Borda Method assigns a position equal to the average of the associated positions to the vendors in a 'tie' situation. From this hypothesis follows that, considering M_j vendors in a 'tie' situation, their ranking is equal to:

$$P_j = \frac{1}{2}\left(2C_j + 1 + M_j\right) \qquad \text{Eq. (1)}$$

Where

P_j position of the vendors in a 'tie' situation;

M_j number of vendors in a 'tie' situation in the j-th position;

$C_j = \sum_{s=1}^{j-1} M_s$ number of vendors having a better ranking with respect to those in a 'tie' position.

Then, Borda method brings the three rankings comparable using the so-called 'Borda Count' defined by the following equation:

$$b_j = \sum_k \left(N - r_{jk}\right),$$

Where

b_j Borda count of the j-th vendor;

N overall number of vendors;

r_{jk} ranking of the j-th vendor for the k-th criterion.

Then, Borda method requires to calculate the so-called Borda Rank sorting the Borda counts of each vendor for each criterion. Table 5 and Table 6 provide a numerical example concerning five vendors with 'very high' residual riskiness (the data in this table is artificial, however, the scores simulate practical cases). Note that the higher the score of a vendor's controls adequacy, the lower its riskiness and, consequently, the lower its ranking.

VENDOR	Overall residual riskiness	CON_CON	CON_INT	CON_AVA	Borda rank CON_CON	Borda rank CON_INT	Borda rank CON_AVA
Vendor A	Very high	50	30	30	5	2.5	2.5
Vendor B	Very high	45	50	30	3.5	5	2.5
Vendor C	Very high	20	30	25	1	2.5	1
Vendor D	Very high	30	25	45	2	1	5
Vendor E	Very high	45	40	35	3.5	4	4

Table 5 - Numerical example of Borda Method (part 1)

VENDOR	Borda count CON_CON	Borda count CON_INT	Borda count CON_AVA	Borda count overall	Borda rank overall
Vendor A	0	2.5	2.5	5	3
Vendor B	1.5	0	2.5	4	5
Vendor C	4	2.5	4	10.5	1
Vendor D	2	4	0	6	2
Vendor E	1.5	1	1	4.5	4

Table 6 - Numerical example of Borda method (part 2)

Table 7 contains the final ranking of the vendors and shows that the riskiest vendor is C while the less risky is B.

VENDOR	Borda rank overall
Vendor C	1
Vendor D	2
Vendor A	3
Vendor E	4
Vendor B	5

Table 7 - Final risk ranking of the numerical example

3.2 Contractualization

A proper contractual framework must consider the 'modularity' of the protection clauses regarding security measures which should both consider the reference cluster and the characteristics of the ICT service. More precisely, regardless of the cluster chosen for the ICT service, contractual agreements should at least provide the protection clauses defined by EBA's guidelines (European Banking Authority, 2019B). However, all the contractual agreements related to external ICT services must contain a clause that obliges the vendor to supply the documentation needed to the company to realize an adequate ex-post monitoring on the services. Furthermore, the agreements should also provide the possibility for the customer to execute audits on the ICT service and on-site inspections. In this context, a weak agreement could lead to difficulties in managing the contract (Smuts, Kotzé, van der Merwe, & Loock, 2015).
The outsourcing contract should provide, at the end of the outsourcing relationship, that the vendor guarantees maintenance and/or training to key personnel of the financial institution (Jothi Kandan & Idris, 2010).
The management of an ICT service outsourcing contract provides a cost for a financial institution, as well as the cost re-integrate the outsourced activity into its internal processes (Nordås, 2020), which is a faculty explicitly written in the agreement.

3.3 External ICT services Monitoring

The first line of defence of a financial institution (typically, the support and the business functions) has to put in place controls - on a continuous basis - on the external ICT services. To comply with EBA's guidelines, these controls must meet a risk-based approach, indeed, the number of controls is proportionate to the riskiness of the purchased service, to the supported activities, and/or to the cluster to which the service belongs.

The set of ex-post controls on external ICT services can be included in an inventory, in which the company specifies the characteristics of the controls (e.g., typology, frequency, reference documentation). In this context, company should send to the supplier a periodic questionnaire to identify any deterioration of the adequacy degree of the controls. In this questionnaire, the supplier must specify any cyber incidents, providing a detailed description of the event and of the root causes: the financial institution should analyze these incidents to decide whether to continue the supply relationship. More precisely, the financial institution should verify whether the supplier understood the causes and put in place effective countermeasures.

3.4 Reporting to the internal control functions

The CPs should transmit to the internal control functions of the financial institution a synthetic report with the main evidences of the control activities. This report should include, at least, a qualitative judgment on the results of the controls that highlights any criticality, the list of vendor's incidents and the security measures that the vendor adopted before and after every single incident, and indicators on the respect of contractual service levels in the reference period of the report (including a comparative analysis with subsequent periods and the indication of possible payment due to contractual penalties).

To guarantee full knowledge and governance of the risk factors that affect an external ICT service, the CP should promptly inform the internal control functions of the company over anomalies that could compromise the service or could give rise to material risks. In this manner, the CP and the internal control functions can decide whether making a communication to the governing bodies.

4. Conclusions

The recent growing resort to third parties for ICT services, which can contribute to increase the consequences of cyber risk, entails many challenges for financial institutions that have to guarantee a mitigation strategy against their ICT third-party risk exposure. In this context, the first challenge is probably that of defining a framework to increase efforts on vendor's control especially to manage cyber risk, which is still much less understood than many other risk types as credit risk or market risk (Cohen, Humphries, Veau, & Francis, 2019). This increase could even jeopardize the survival of some existing arrangements (Mourselas, 2019).

In this paper, we present a holistic ICT third-party risk management framework. The first step is an ex-ante analysis of initiative approval and vendor selection, we stress the need for a preliminary risk assessment to choose the best vendor for an ICT service. The risk assessment technique provides the three following steps:

- Inherent risk calculation, which aims at estimating a rating of the potential riskiness of the ICT service as a function of its characteristics (this activity is carried out by the CP);
- Vendor's controls adequacy calculation, for which the company requests to the vendor several information on the security measures in place;
- Residual risk calculation, obtained as a combination of the inherent risk rating and of the vendor's controls adequacy. This activity includes the application of the Borda Method when two or more vendors present the same residual risk.

Once chosen the best vendor, in the second step (contractualization), the financial institution should write down the agreement with the vendor including all the necessary protection clauses. Note that the protection clauses represent the indispensable prerequisite to guarantee an effective monitoring of the vendor on an ongoing basis, which is the main activity of the third (and last) step.

Outsourcing of ICT services (in particular, cloud services) is one of the best solutions for the financial institutions that will face the near future main trends concerning these services, namely the growing necessity of quickness, easiness, and accessibility. In this context, it is necessary to analyze the possible outcomes of this kind of outsourcing (Hanafizadeh & Zare Ravasan, 2018), because the third-party risk related to ICT services will become more and more crucial for the cyber security programs that aim at guaranteeing the integrity, confidentiality, and traceability of data. Indeed, according to Khan & Estay (Khan & Estay, 2015), a cyber-attack <<not always comes from the front door>>. Cyber security is a really relevant issue, since many silent attacks are carried out every day. Cyber risk is different with respect to the other security risks, due to the ease at which a hacker can identify vulnerabilities (Singer & Friedman, 2014). Cybercriminals aims at obtaining sensitive and personal information continuously analyzing vulnerabilities modifying their strategy due to the security measures of the targeted company (PWC, 2015). Furthermore, also a senior official at the European Central Bank affirmed that financial institutions that use external data storage and analogous digital technologies have a good chance of being hacked (Comfort, 2019). Again, according to FBI (Federal Bureau of Investigation) Director James Comey, there are big companies that have been hacked and those who don't know they have been hacked (Cook, 2014).

Financial institutions should strengthen security measures on vendors of ICT services asking adequate information security standards. Thus, financial institutions need to rethink to the ICT third-party risk mitigation[9]: on the one hand, companies should put in place a framework integrated at all the levels of the company to anticipate future trends of the threats. On the other hand, financial institutions should use more and more modern technologies (e.g., machine learning, deep learning, and analytics) and different data sources to guarantee an effective vendor selection.

Taking into consideration agency theory and transaction cost theory, we identify four main risk scenarios associated with external ICT services: lock-in, contractual amendments, unexpected transition and management costs and disputes and litigation (Bahli & Rivard, 2003). These scenarios are mainly due to the absence of a proper oversight on vendor's activity that could entails many drawbacks, in terms of (i) loss of control, (ii) weakening of both the development ability and creativity, (iii) decrease of the employee motivation (which could intend the outsourcing of an activity as a potential source for job losses), (iv) high economic costs for the transactions, and (v) threats for the data confidentiality. These drawbacks could be exacerbated in case of an ill-defined contract, if the monitoring of the service levels is insufficient or when the financial institutions did not define an exit strategy to prevent potential criticalities.
Theft of intellectual property is another kind of strategic risks related outsourcing (Aron, Clemons, & Reddi, 2005). Therefore, trust between the two parties is one of the key factors for success in the outsourcing arrangement, useful to avoid legal action and to establish a long-term relationship (Babin, Bates, & Sohal, 2017).

The management of a financial institution has to build key in-house capabilities and to learn how to manage outsourcing (Lacity, Khan, & Willcocks, 2009). This aspect is crucial because the client company's staff may see outsourcing as a threat to their jobs and, thus, may oppose to this solution (Brooks, 2006). Last but not least, fourth-parties (namely the supplier's suppliers) could be an additional risk source in the context of ICT third-party risk (Awasthi, Govindan, & Gold, 2018). A possible strengthening of the ICT third-party risk management framework is a theme left for future research. In conclusion, the need of implementing an effective control framework for the ICT third-party risk is increasingly debated among financial institutions because it represents a priority in which they must invest in the near future.

Andrea Giacchero and Jacopo Moretti

[9] See (de Sá-Soares, Soares, & Arnaud, 2014) for a comprehensive catalog of mitigation actions.

Bibliography

- Abdullah, L., & Verner, J. (2012). Analysis and application of an outsourcing risk framework. *The Journal of Systems and Software, 85*(8), 1930-1952.
- Alner, M. (2001). The effects of Outsourcing in Information Security. *Information Systems Security, 10*(2), 35-43.
- Aron, R., Clemons, E., & Reddi, S. (2005). Just right outsourcing: understanding and managing risk. *Journal of Management Information Systems, 22*(2), 37-55.
- Aubert, B. A., Dussault, S., Patry, M., & Rivard, S. (1999). Managing the risk of IT outsourcing. *In Proceedings of the 32nd Annual Hawaii International Conference on Systems Sciences. 1999. HICSS-32. Abstracts and CD-ROM of Full Papers*, pp. (pp. 10-pp). IEEE.
- Aubert, B. A., Patry, M., & Suzanne, R. (2005, Fall). A Framework for Information Technology Outsourcing Risk Management. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 36*(4), 9-28.
- Awasthi, A., Govindan, K., & Gold, S. (2018). Multi-tier sustainable global supplier selection using a fuzzy AHP-VIKOR based approach. *International Journal of Production Economics, 195*, 106-117.
- Babin, R., Bates, K., & Sohal, S. (2017). The Role of Trust in Outsourcing: More Important Than the Contract? *Journal of Strategic Contract and Negotiation, 3*(1), 38-46.
- Bahli, B., & Rivard, S. (2003). The Information Technology Outsourcing Risk: a Transaction Cost and Agency theory-based Perspective. *Journal of Information Technology, 18*(3), 211-221.
- Bahli, B., & Rivard, S. (2005). Validating Measures of Information Technology Outsourcing Risks Factors. *Omega, 33*(2), 175-187.
- Banca d'Italia. (2013, December). *Circolare n. 285 del 17 dicembre 2013 34° aggiornamento.* Retrieved from https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/circolari/c285/aggiornamenti/Circ-285-Rist-int-34-agg.pdf
- Banca d'Italia. (2019, December). *Indagine Fintech nel sistema finanziario italiano.* Retrieved from https://www.bancaditalia.it/compiti/vigilanza/analisi-sistema/approfondimenti-banche-int/Allegato_2_Indagine_Fintech.pdf
- Basel Committee on Banking Supervision. (2018, December). Cyber-resilience: Range of practices. Retrieved from https://www.bis.org/bcbs/publ/d454.pdf
- Basel Committee on Banking Supervision. (2018, February). Sound Practices: Implications of FinTech Development for Banks and Bank Supervisors. Retrieved from https://www.bis.org/bcbs/publ/d431.pd
- Board of Governors of the Federal Reserve System. (2013). *Guidance on Managing Outsourcing Risk.* Retrieved from https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf
- Boardman, J., & Sauser, B. (2008). Systems thinking: Coping with 21st century problems. *CRC Press*.
- Bott, J., & Milkau, U. (2015). Outsourcing Risk: A Separate Operational Risk Category? *Journal of Operational Risk, 10*(3).
- Brooks, N. (2006). Understanding IT Outsourcing and its Potential Effects on IT Workers and Their Environment. *The Journal of Computer Information Systems, 46*(4), 46-53.
- Carter, J., Maltz, A., Yan, T., & Maltz, E. (2008). How procurement managers view low cost countries and geographies. *International Journal of Physical Distribution & Logistics Management, 38*(3), 224-243.
- Cohen, R. D., Humphries, J., Veau, S., & Francis, R. (2019). An investigation of cyber loss data and its links to operational risk. *Journal of Operational Risk, 14*(3).
- Comfort, N. (2019, August 19). *ECB Says the Next European Bank Hack Is Just a Matter of Time*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2019-08-19/ecb-says-the-next-european-bank-hack-is-just-a-matter-of-time
- Cook, J. (2014, October 6). FBI Director: China Has Hacked Every Big US Company. *Business Insider*. Retrieved from http://www.businessinsider.com/fbi director-china-has-hacked-every-big-us-company-2014-10
- Currie, W. (2003). A knowledge-based risk assessment framework for evaluating web-enabled application outsourcing projects. *International Journal of Project Management, 21*(3), 207-217.
- Das, T., & Teng, B. (2000). Instabilities of strategic alliances: an internal tensions perspective. *Organization Science, 11*(1), 77-101.
- Davison, D. (2003, December). *Top 10 Risks of Offshore Outsourcing*. Retrieved from ZDNet: https://www.zdnet.com/article/top-10-risks-of-offshore-outsourcing/
- de Sá-Soares, F., Soares, D., & Arnaud, J. (2014). Towards a theory of information systems outsourcing risk. *Procedia Technology, 16*, 623-637.
- Earl, M. J. (1996). The risk of outsourcing IT. *Sloan Management Review, 37*(3), 26–32.
- European Banking Authority. (2017, September 11). Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process - SREP. *EBA/GL/2017/05*.
- European Banking Authority. (2019A, February). Final Report on EBA Guidelines on outsourcing arrangements. *EBA/GL/2019/02*.
- European Banking Authority. (2019B, November). EBA Guidelines on ICT and security risk management. *EBA/GL/2019/04*.

- European Central Bank. (2018, May). TIBER-EU FRAMEWORK (How to implement the European framework for Threat Intelligence-based Ethical Red Teaming). Retrieved from https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf
- European Commission - G7 Cyber Expert Group. (2016, October). *G7 fundamental elements of cybersecurity in the financial sector*. Retrieved from https://ec.europa.eu/info/system/files/cybersecurity-fundamental-elements-11102016_en.pdf
- European Parliament. (2016). General Data Protection Regulation. *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
- Fan, Z.-P., Suo, W.-L., & Feng, B. (2012). Identifying risk factors of IT outsourcing using interdependent information: An extended DEMATEL method. *Expert Systems with Applications, 39*(3), 3832–3840.
- Farrell, D. (2004). Beyond offshoring. *Harvard Business Review, 82*(12), 82-90.
- Federal Deposit Insurance Corporation. (2019, June). Compliance Examination Manual: Third Party Risks. Retrieved from https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/7/vii-4-1.pdf
- Feeny, D., Lacity, M., & Willcocks, L. (2005). Taking the measure of outsourcing providers. *MIT Sloan Management Review, 46*(3), 41-48.
- Financial Stability Board. (2018, November). *Cyber Lexicon.* Retrieved from https://www.fsb.org/wp-content/uploads/P121118-1.pdf
- Ford, D., & Farmer, D. (1986). Make or buy—a key strategic issue. *Long Range Planning, 19*(5), 54-62.
- Gandhi, J., Gorod, A., & Sauser, B. (2012). Prioritization of outsourcing risks from a systemic perspective. *Strategic Outsourcing: An International Journal, 5*(1), 39-71.
- Ghodeswar, B., & Vaidyanathan, J. (2008). Business process outsourcing: an approach to gainaccess to world-class capabilities. *Business Process Management Journal, 14*(1), 23-38.
- González, R., Gascó, J., & Llopis, J. (2016). Information Systems Outsourcing Reasons and Risks: Review and Evolution. *Journal of Global Information Technology Management, 19*(4), 223–249.
- Gopal, A., Sivaramakrishnan, K., Krishnan, M., & Mukhopadhyay, T. (2003). Contracts in Offshore Software Development: An Empirical Analysis. *Management Science, 49*(12), 1671-1683.
- Haller, J., & Wallen, C. (2016). *Managing third party risk in financial services organizations: a resilience-based approach.* Retrieved from https://resources.sei.cmu.edu/asset_files/whitepaper/2016_019_001_473742.pdf
- Hanafizadeh, P., & Zare Ravasan, A. (2018). An empirical analysis on outsourcing decision: the case of e-banking services. *Journal of Enterprise Information Management, 31*(1), 146-172.
- Harland, C., Knight, L., Lamming, R., & Walker, H. (2005). Outsourcing: assessing the risks and benefits for organisations. *International Journal of Operations & Production Management, 25*(9), 831-850.
- Hinson, G. (2007, December). Top Information Security Risk for 2008. CISSP Forum. Retrieved from http://www.naavi.org/cl_editorial_08/Top_information_security_risks_for_2008.pdf
- Jothi Kandan, M., & Idris, N. A. (2010). *Guidelines on Information Security in ICT Outsourcing.* CyberSecurity Malaysia. Retrieved from https://www.cybersafe.my/pdf/guidelines/Guidelines_on_Information_Security_in_ICT_Outsourcing.pdf
- Kaplan, J., Bailey, T., O'Halloran, D., Marcus, A., & Rezek, C. (2015). *Beyond Cybersecurity: Protecting Your Digital Business.* John Wiley & Sons.
- Kaplan, R. (2004). A matter of trust. In *Information Security Risk Management Handbook.* Auerbach Publications: Boca Raton.
- Khan, O., & Estay, D. A. (2015). Supply chain cyber-resilience: Creating an agenda for future research. *Technology Innovation Management Review, 5*(4), 6-12.
- Khidzir, N. Z., Mohamed, A., & Arshad, N. H. (2013, December). ICT Outsourcing Information Security Risk Factors: An Exploratory Analysis of Threat Risks Factor for Critical Project Characteristics. *Journal of Industrial and Intelligent Information, 1*(4), 218-222.
- Kleindorfer, P., & Saad, G. (2005). Managing disruption risks in supply chains. Production and operations management. *14*(1), 53-68.
- Lacity, M., Khan, S., & Willcocks, L. (2009). A Review of the IT Outsourcing Literature: Insights for practice. *The Journal of Strategic Information Systems, 18*(3), 130–146.
- Lansdowne, Z. F., & Woodward, B. S. (1996). Applying the borda ranking method. *Air Force Journal of Logistics, 20*(2), 27-29.
- Layton, M., Zechnich, D., & al., e. (2008). The risk intelligent approach to outsourcing and offshoring. *Risk Intelligence Series*(8). Retrieved from www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_risk_riskintelligent_
- Levina , N., & Ross, J. (2003). From the Vendor's Perspective: Exploring the Value Proposition in Information Technology Outsourcing. *MIS Quarterly, 27*(3), 331-364.
- Mallinder, J., & Drabwell, P. (2013). Cyber security: A critical examination of information sharing versus data sensitivity issues for organisations at risk of cyber attack. *Journal of business continuity & emergency planning, 7*(2), 103–111.
- McCahery, J., & de Roode, A. (2018). Governance of financial services outsourcing: Managing misconduct and third-party risks. *European Corporate Governance Institute (ECGI)-Law Working Paper No. 417/2018, Tilburg Law School Research Paper Forthcoming*.

- Mourselas, C. (2019, June 10). *Financial firms toil to meet new EU rules on outsourcing*. Retrieved from https://www.risk.net/risk-management/6714296/financial-firms-toil-to-meet-new-eu-rules-on-outsourcing
- Nakatsu, R., & Iacovou, C. (2009). A comparative study of important risks factors involved in offshore anddomestic outsourcing of software development projects: A two-panel Delphi study. *Information & Management, 46*(1), 57–68.
- Nordås, H. K. (2020). Make or buy: Offshoring of services functions in manufacturing. *57*(2), 351-378.
- Parker, D. (2002). Toward a New Framework for Information Security. In S. Bosworth, & M. Kabay, *Computer Security Handbook. 4th ed.* New York: John Wiley & Sons.
- Power, M., Bonifazi, C., & Desouza, K. (2004). The ten outsourcing traps to avoid. *Journal of Business strategy, 25*(2), 37-42.
- Power, M., Desouza, K., & Bonifazi, C. (2006). *The Outsourcing Handbook: How to Implement a Successful Outsourcing Process.* London: Kogan Page Publishers.
- Prasad, A., & Prasad, P. (2007). Moving out: toward understanding the complexity of outsourcing in the age of globalization. *Business Renaissance Quarterly, 2*(3), 67-91.
- PWC. (2015). Insurance 2020 & Beyond: Reaping The Dividends Of Cyber Resilience. Retrieved from http://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf
- Ruzaini, S., Aris, H. S., Arshad, N. H., & Mohamed, A. (2008). Conceptual framework of risk management in IT outsourcing project. *WSEAS Transactions on Information Science & Applications, 5*(4), 816-831.
- Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students.* Pearson education.
- Shroff, B. P., & Bandi, R. K. (2018). Impact of IT Multisourcing on vendor opportunistic behaviour-A research framework. *ACIS 2018 Proceedings.* Sidney.
- Singer, P., & Friedman, A. (2014). *Cybersecurity: What Everyone Needs To Know.* Oxford, UK: Oxford University Press.
- Smuts, H., Kotzé, P., van der Merwe, A., & Loock, M. (2015, October). Threats and opportunities for information systems outsourcing. *In 2015 International Conference on Enterprise Systems (ES)* (pp. 110-120). IEEE.
- Sullivan, W., & Ngwenyama, O. (2005). How are public sector organizations managing IS outsourcing risks? An Analysis of Outsourcing Guidelines from three Jurisdictions. *Journal of Computer Information Systems, 45*(3), 73-87.
- Verwaal, E., Verdu, A., & Recter, A. (2008). Transaction Cost and organizational learning in strategic outsourcing relationships. *International Journal of Technology Management, 41*(1-2), 38-54.
- Vőneki, Z. T. (2018, December). OPERATIONAL RISK AFTER THE CRISIS. *Economy and Fincance (GÉP), 5*(4). Retrieved from http://www.bankszovetseg.hu/magunkrol.cshtml?lang=eng
- Vorster, A., & Labuschagne, L. E. (2005). A framework comparing different information security risk analysis methodology. *In Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries*, (pp. 95-103).
- Walden, E. A., & Hoffman, J. J. (2007). Organizational form, incentives and the management of Information Technology. Opening the black box of Outsourcing. *Computers & Operations Research, 34*(12), 3575-3591.
- Walker, G., & Weber, D. (1984). A transaction cost approach to make-or-buy decisions. *Administrative science quarterly, 29*(3), 373-391.
- Walker, G., & Weber, D. (1987). Supplier competition, uncertainty, and make-or-buy decisions. *Academy of Management journal, 30*(3), 589-596.
- Waters, D. (2011). *Supply chain risk management: vulnerability and resilience in logistics.* London, UK: Kogan Page Publishers.