A STUDY ON INFORMATION SECURITY IMPACT ON THE DELIVERY OF IT MANAGED SERVICES

Răzvan Cristian Ionescu[1], Marieta Olaru[2], Georg Sven Lampe[3] and Teodora Elena Fogoros[4]
[1)2)3)4)] *The Bucharest University of Economic Studies, Romania*
E-mail: razv77@gmail.com; E-mail: olaru.marieta@gmail.com;
E-mail: georg.sven.lampe@gmail.com; E-mail:teodora.elena@icloud.com

Please cite this paper as:

Ionescu, R.C., Olaru, M., Lampe, G.S. and Fogoros, T.E., 2020. A Study on Information Security Impact on the Delivery of It Managed Services. In: R. Pamfilie, V. Dinu, L. Tăchiciu, D. Plești, C. Vasiliu eds. *6th BASIQ International Conference on New Trends in Sustainable Business and Consumption.* Messina, Italy, 4-6 June 2020. Bucharest: ASE, pp. 958-965

Abstract
The outsourcing of the IT infrastructure administration or contracting of some specialized IT services are common practices for many organisations. The reasons are multiple and vary, from the lack of internal IT competent staff up, to the fulfilment of some cost decrease performance indicators imposed by the top management or by the shareholders.
In almost all outsourcing plans, the security of the data should be a concern of the managers in charge with these decisions. Moving of the sensitive data or granting access to this data to an external IT services provider is a delicate decision that might involve a high risk for the organisation. A prior discussion and analysis between the organisation and the future IT services provider might be welcomed before the outsourcing decision.
On the other hand, from IT services provider perspective, the delivery of the IT services to its clients must be performed by respecting a set of best-practice requirements and one of these is the preservation of the security of the clients' data.
The authors of this paper aimed to study the impact of the information security upon the process of delivery of IT managed services from an IT services provider's perspective.

Keywords
Information security, IT service delivery, business continuity, security incident, IT outsourcing, service provider

JEL Classification
M15, O18, L86, O14

Introduction

The provision of outsourced IT managed services to any organisation should not target only the quality aspects of the service delivery but also the security issues involved in the delivery

process due the fact the IT services provider has direct access to its clients' infrastructure and sensitive information. Any IT service provider that has access to the confidential information of its clients should be responsible to protect it from any potential security threat. Taking into consideration the digitalized times we face and the technology advancement, the digitization of business processes turns into a challenge for organizations with regards to data security and confidentiality (Fogoros et al., 2020).

As observed by Kiehne and Olaru (2017) in their study, the 4.0. Industry mostly focuses on technical aspects, such as data protection. Preservation of the security means preservation of several information parameters like confidentiality, integrity, availability (Ionescu et al., 2018) but also of the others, such as: resilience, reliability and non-repudiation. Furthermore, the globalization and the internationalization of businesses made organizations deal with security requirements and local law regulations (Marquardt et al., 2018).

Another possible integration for any service delivery implementation might be with the legal requirements regarding the privacy of the individuals (General Data Protection Regulation applicable starting 2018). If the services of the IT service provider process any personal data of the employees, clients or of the third parties of the provider and/or its clients or suppliers, it is mandatory to apply security measures to protect these personal data (Ionescu et al., 2019). This security environment can be implemented by defining some specific security measures and roles based on the specific risks (Dhillon et al., 2006) identified in the provision of the IT managed services. Beside the hardware and software components involved in the delivery of services, the employees used to manage and deliver the IT services can affect the security overall, due to their intentional or unintentional behaviour which might trigger some incidents (Bauer et al., 2017). Therefore a security awareness programme and a security culture should be developed (Da Veiga et al., 2010) in the organisation of the IT services provider but also in the ones of its clients. Specific security roles should be established in both types of organisations to manage the fulfilment of the security objectives (Ashenden et al., 2013, Hooper et al., 2016). These specific roles should also be involved in the sharing of security advice and troubleshooting (Dang-Pham et al., 2016). These roles from both the IT service provider and its clients, must communicate and report each other the security incidents, when these occur.Beside the security incidents, changes of the context in which the IT services are delivered, occur also every once in a while. Therefore, both the IT service provider and its clients must be engaged, communicate and interact to have an effective information security environment (Bauer et al., 2017). No matter the source, amplitude and negative impact of a change of the context in which the IT services are delivered or of the type of the security incident, the IT service provider should have defined and designed resilience mechanisms of its delivered services and infrastructure to resist and continue to deliver the IT services to its clients according to signed Service Level Agreements (SLAs) (Millar et al., 2018). Each potential failure of an organization should be turned into an innovation tool, not in a hidden loss, keeping in mind the fact that every company is challenging the concept of being good in all fields. Though, we must underline the role of the top management, as being in charge with the communication of the importance of security maintenance on business process and allocation of ressources (Ionescu et al., 2019).The research carried out by the authors proposes to study the impact of the information security upon the delivery of the IT managed services by an IT provider to its clients. Integration of security issues into the delivery of IT services raises several problems such as: extra costs that the IT service provider must consider before the delivery of the services, the use of specific competence and infrastructure, process integration know-how and increased complexity of the internal processes used for the delivery of the contracted services.

Research Methodology

The research methodology for this study included two methods. First, a specific literature extensive review, in which the authors studied research articles, legislation, international standards, best practices and studies regarding information security and IT service management system.Second, the performance by the authors of this study of several external audits in four organisations that deliver IT managed services to their customers. The authors checked the level of compliance of these organisations according to the service management system described in the ISO/IEC 20000-1 requirements standard. Three of the studied companies are from Romania and offer their IT services to external clients and the forth is from Germany and offers the IT services internally (the client is internal). The audits have been performed in the period 2010-2019. Among the audited clauses was also the information security ones that have been integrated in their service management system. The authors used audit checklists to investigate the compliance of these companies with their internal rules and procedures developed for the IT service management system. Other investigation methods were the interview of the staff of these companies about the security measures applied in the provision of the IT services to the clients and the analysis of their records and IT systems. By applying these methods, the authors checked the security measures applied for each stage of the service management process (planning and design, development, delivery, maintenance and change/removal of the IT services). The authors compared their results with the requirements of the service management system, which are documented in the procedures of the audited organisations and issued nonconformities and recommendations for the improvement for the service management systems. The results were also used to generate statistics regarding the importance given by the audited companies to the security measures within the service management processes. The analysis of the results of the audits and the literature review were used to study whether the service management process can be improved by integrating with other information security management processes such as risk, change, availability, capacity and communication.

Research Results

Analysis of the specific literature concluded that specific standards and guidelines were issued for the IT service providers, which define the requirements for the service management. The most known references in terms of best practices in IT service management are Information Technology Infrastructure Library (ITIL®), Control Objectives for Information and Related Technology (COBIT®) and ISO/IEC 20000 family of international standards for the service management issued by International Organization for Standardization (ISO).The last version of ISO/IEC 20000-1, which was issued in 2019 is aligned with the Annex SL issued by ISO and facilitates the integration with the ISO/IEC 27001 standard for the information security management system. Therefore the general requirements regarding the information security from the ISO/IEC 20000-1 can be understood and integrated easily with the specific information security requirements from ISO/IEC 27001. Even the scopes of the ITIL, COBIT, ISO/IEC 20000-1, ISO/IEC 27001 are quite different, there are some common aspects in all of the above specifications. A comparison between the common requirements from ISO/IEC 27001 and ISO/IEC 20000-1 with regard to the technical processes is illustrated in the fig.no.1.

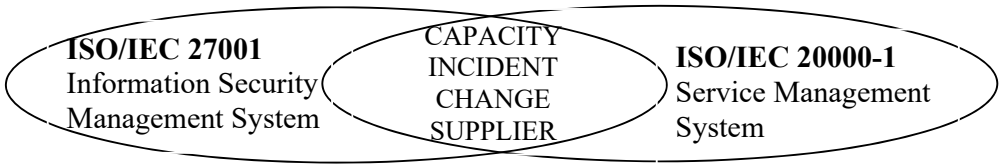

Fig. no. 1 Similarities between ISO/IEC 27001 and ISO/IEC 20000-1 technical processes

Source: Authors, 2020

The comparison below excluded the general management clauses from the two standards corresponding to the Plan-Do-Check-Act improvement cycle, which are also common, and focussed more on the technical management processes.

The requirements for the capacity and change management process are very similar, even the scopes of the two international standards are different. ISO/IEC 27001 is focused on the protection of all types of organisations by protecting their sensitive information, while ISO/IEC 20000-1 is addressed only to the services providers and defines the framework, in which their services deliver to the clients at all times by respecting the service level agreements.

A difference between the other common technical processes is for incident, supplier and continuity management. In information security management system, the incident management process is focussed on how to manage a security incident that affects critical assets of the organisation, while in service management system, the incident management process refers how a disruption in the provision of a service is managed for a client. So the purpose of this process is different in the two standards. Supplier management in information security refers to the control of the activities of organisation's suppliers, with the objective to mitigate the possible information security risks, which might appear from this interaction with the supplier's organisation and its staff. In service management system, the supplier management process is focused on the respecting of the engagements taken by supplier, so the service level agreement between the service provider and its clients to be respected in all cases, no matter what happens with the subcontracted processes or the supplier. The continuity process in service management system refers to the continuity of delivery of the contracted services that are under the service level agreements and focus more on accessibility and availability of these services. In information security management system, the continuity process refers not only to the developing of a business continuity plan with various scenarios, but also to keep the critical assets of the organisation safe, even in the event of any business disruption or security incident.

The service management system can be improved as well, if the IT service provider uses the principles from the information security management system. As an example, the risk analysis required by the service management system can be completed with the one from the information security management system.

So, for each IT service, the IT service provider should identify which are the critical information and assets that should be protected. For each item in the risk analysis, the IT service provider should identify possible threats, vulnerabilities, risks and security measures to mitigate these risks. It should be a single integrated risk analysis in which all risks must be managed by an integrated risk management procedure. The usage of a single risk management procedure will assure comparable and reliable results.

As regards the framework of the service management system, ISO/IEC 20000-1 contains most principles of ITIL® and can be used to audit IT service providers and other types of services providers which have their services of delivery based on IT technologies. Following the audits performed, the authors identified several specific information security risks associated with

the IT service delivery processes. Other information security risks, valid in general for all types of organisations, haven't been summarised here.
In table no.1 the authors identified these specific security risks and for each of them, pointed out which attribute of the information security is most probable to be affected in case, that specific risk is not mitigated by the implementation of effective security measures.

Table no. 1 Specific information security risks associated with the processes of IT service management

Type of information security risk	Impact upon information within the delivered IT services
Lack of security requirements in the service design phase	Confidentiality, Availability, Integrity
Lack of the cyber-security attack scenario from the service continuity plan	Availability
Configuration management database does not contain all configuration items used in the delivery of the services	Availability, Integrity
The (new) staff of the IT service provider is not trained regularly with the security procedures	Confidentiality, Availability
Lack of enough human resources (replacements) to manage all the delivered IT services	Availability
The suppliers of the IT provider are not monitored properly as regards the fulfilment of the security rules	Confidentiality, Availability
Poor recording in the Knowledge database of all of the workarounds for the security incidents	Confidentiality, Availability
Lack of recording the customers plans for change as regards the delivered services	Availability, Integrity
Not all security incidents are recorded and investigated by the IT service provider	Confidentiality, Availability, Integrity
Knowledge and/or Configuration database could not be updated every time. Their content is not accurate	Integrity
Lack of testing the releases before their deployment	Confidentiality, Availability, Integrity
The security risks are not considered in the release plans	Confidentiality, Availability, Integrity

Source: Authors, 2020

The identification of the risks above might help the organisations which offer IT managed services to their clients, to identify their security vulnerabilities better and to propose suitable security measures to keep these risks under control.
The list above is not exhaustive and might be improved with other security risks in dependence of the specific context of each IT service provider. Some specific information security issues have been discovered during the audits of the IT service providers.
The authors consider the application of the associated corrections will improve the security of the IT managed services, thus the IT service provider will provide safer services to its clients. Studying the infrastructure and the way the IT service provider manages its delivered services towards its clients has identified the security improvements.
A summary of the identified security improvements is illustrated in fig.no.2.

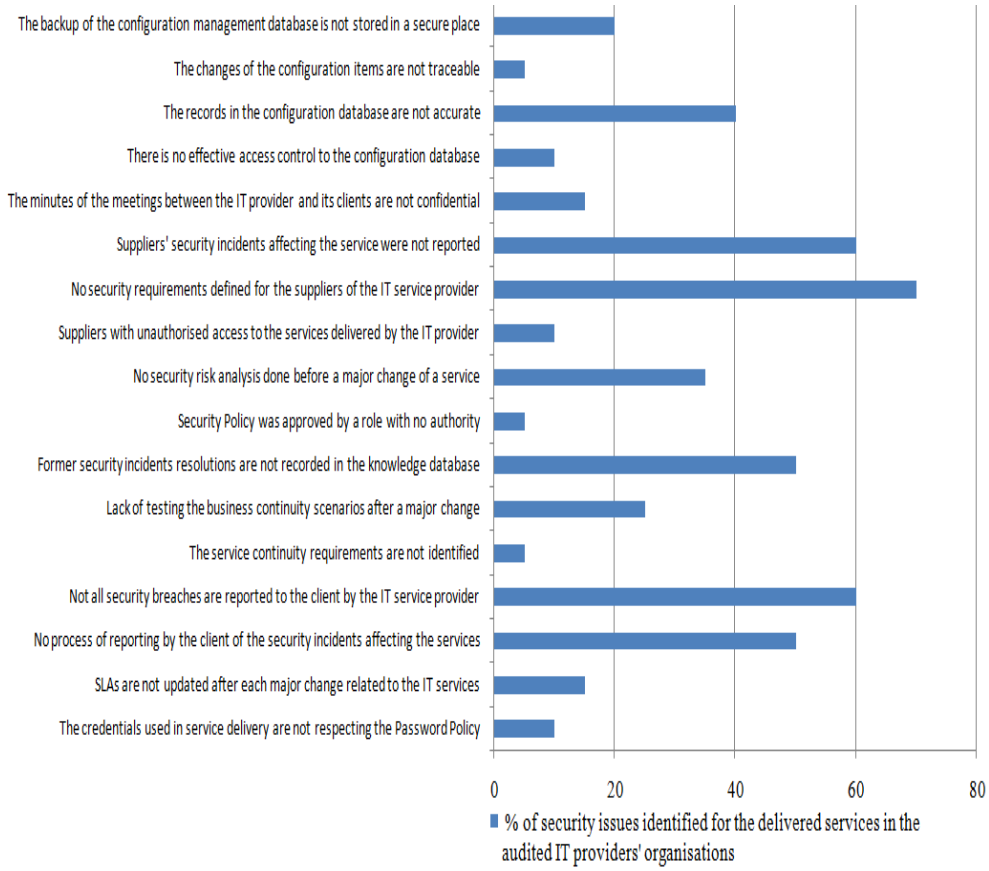

Fig. no. 2 Percents of security issues identified for the delivered services in the audited IT providers' organizations

Source: Authors, 2019

In the chart above , on horizontal axis is illustrated the percent of security issues (out of the total number of 20) discovered by the authors during the performance of the audits in the IT providers organisations. On the vertical axis are documented the specific information security issues identified in managing of the IT services by the IT providers.Centralisation of the results shows the IT service providers were focused mostly on the quality parameters of the delivery of the IT services, as the clients' satisfaction was a top priority in most of the cases. Most of the key performance indicators (KPI) mentioned in the service level agreements, signed between the IT service provider and its clients, were in stronger relationship with the quality aspects rather than with the security of information during the delivered services. This could explain also the lack of attention of the IT service providers to the relationship with their suppliers as regards the information security requirements, especially when they outsourced some processes or part of them, related to their delivered IT services. As it can be seen from the graph above, the IT service providers didn't include proper security requirements in their contracts with the companies to whom they outsourced some parts of the delivered IT services. This created a vulnerability in the organisation of the IT service provider and, in consequence, in the organisations of the clients of the IT service provider. To eliminate this vulnerability, the IT service provider should have defined or transfered the security clauses that it had signed with its clients, to its suppliers and to require them to transfer them in turn, to their sub-suppliers in case they have contact with any components of

the delivered IT service. In this way the IT service provider could mitigate the security risks for the whole suppliers chain. Monitorization of the fulfilment of the imposed security clauses to the suppliers must be performed from time to time, on a regular basis, to assure that they are respected continuosly and corrective actions must be applied if any non-fulfilment of contractual requirements is identifed during these checks.

Conclusions

The integration of security requirements, based on a risk analysis, in the delivered IT services, starting from the design phase of the service, might constitute a competitive advantage for any IT services provider, when they negotiate their contracts with the future clients. Consideration of security issues should be done starting from the design phase of the IT services to decrease the costs. Focusing on the security aspects as well, not only on the quality of the services (e.g.: fulfilment of the key performance indicators from the service level agreements), could help the IT services providers to avoid security incidents that might put in danger the contractual engagements with the clients. Investment in security might be considered less expensive than payment of penalties due to possible malfunctions of the provided IT services. In some cases, the security component might be understood as a key performance indicator among other quality monitored indicators for the IT service. Thus, it might be inserted in the contractual agreements between the IT service provider and its clients as an obligation for the quality of the services, not only as an option. Customisation of the security level and measures of the delivered IT services should consider aspects such as: critical assets and services to be secured, targets mentioned in the service level agreements between the provider and the client, client's needs, objectives and contractual engagements with its customers, level of integration of IT services in the client's business activities, capacity and competence of the IT service provider to take over some specific tasks, as well as financial aspects which cannot be ignored. Securing all these components is a complex process due to the variety of items, issues and involved objectives. As with some IT service providers, it is possible to deliver services that process personal data of their clients or of the third parties. Therefore, the legal requirements of General Data Protection regulation will apply. In this case, the application of security measures for the delivered IT service is no longer on option but an obligation of the IT provider. The authors of this research conclude not only there is a clear link between the information security and service management, but also that the two concepts can be integrated successfully. If implemented well, the impact of the information security upon service management is a positive one. The adoption of security measures from the design phase of the service, to testing, delivery, maintenance and even removal of service phase, reduces the risk of incidents so the IT service provider will be less financially exposed in front of its clients. Furthermore, the IT service provider might be helped by the adoption of an integrated information security management system at this system is much more detailed with regard the specific security measures than the service management system alone.

Future directions of research regarding the information security implications in the IT service management could comprise the review of other methodologies like CMMI-SVC® and ISO 15504, as these best practices have not been the object of the current study.

References

Ashenden, D. and Sasse, A. 2013. CISOs and organisational culture: their own worst enemy? *Computers & Security*, 39(part B), pp.396-405.

Bauer, S., Bernroider, E.W.N. and Chudzikowski, K. 2017. Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in bank. *Computers & Security*, 68, pp.145–159.

Dang-Pham, D., Pittayachawan, S. and Bruno, V. 2016. Impacts of security climate on employees' sharing of security advice and troubleshooting: empirical networks. *Business Horizons*, 59(6), pp.571-584.

Da Veiga, A. and Eloff, J.H.P., 2010. A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), pp.196-207.

Dhillon, G. and Torkzadeh, G. 2006. Value-focused assessment of information system security in organizations. *Information Systems Journal*, 16(3), pp.293-314.

Fogoros, T.E., Maftei, M., Bitan, G.E. and Kurth, B.L., 2020. Study on methods for evaluating employees performance in the context of digitization. In *Proceedings of the 14th International Conference on Business Excellence (ICBE)*. Bucharest, Romania, pp.1-14.

Hooper, V. and McKissack, J., 2016. The emerging role of the CISO. *Business Horizons*, 59(6), pp.585-591.

ISO/IEC 27001:2013, 2013. *Information technology -- Security techniques -- Information security management systems* – Requirements. International Organization for Standardization. [Retrieved September 01, 2019], <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en>.

ISO/IEC 20000-1:2018, 2018. *Information Technology – Service Management* – Part 1: Service Management system Requirements, International Organization for Standardization. [Retrieved December 27, 2019], <https://www.iso.org/standard/70636.html>

Ionescu, R.C., Ceausu, I. and Ilie, C. 2018. Considerations on the implementation steps for an information security management system. *Proceedings of the 12th International Conference on Business Excellence (ICBE). 2*2nd of March 2018, Bucharest, Romania, pp.1-13

Ionescu, R.C., Grab, B. and Hassani, Y., 2019. Study on the effects of information security management system in the context of E.U. General Data Protection Regulation application. *Quality-Access to Success*, 20(S2), pp.321-327.

Ionescu, R.C., Olaru, M. and Sargut, K., 2019. Study of the Information Security Impact on the Business Continuity. *Proceedings of the 34th International Business Information Management Association Conference (IBIMA)*, Madrid, Spain, 11/13-14/2019, pp.4279-4287.

Kiehne, J. and Olaru, M., 2017. Implementing Industrie 4.0 strategies: Beyond Technical Innovations. In: *4th BASIQ International Conference on New Trends in Sustainable Business and Consumption,* pp.363-371.

Marquardt, K., Olaru, M., Golowko, N. and Kiehne, J., 2018. Study on economic trends, drivers and developments of the 21st century. In: *5th BASIQ International Conference: new trends in sustainable business and consumption*, pp.65-73.

Millar, C., Lockett, M. and Ladd, T. 2018. Disruption: technology, innovation and society. *Technological Forecasting & Social Change*, 129, pp.254-260.