

Information security in offshoring business processes – design and implementation of controls guidelines

Master thesis submitted to Delft University of Technology
in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

in Management of Technology

Faculty of Technology, Policy and Management

by

Agnieszka Lecka

Student number: 4255208

To be defended in public on 12/12/2018

Graduation committee

Chairperson : Dr. R.M. Verburg, EIT
First Supervisor : Prof. dr W.A.G.A (Harry) Bouwman, E and I
External Supervisor : Dr. Albert Plugge

Table of Contents

Summary	5
Chapter 1 - Introduction	5
1.1. Context	5
1.1.1. Outsourcing	5
1.1.2. Data protection	6
1.1.3. Information security management	7
1.2. Problem formulation and research objective	10
1.2.1. Problem owner	10
1.2.2. Problem definition	11
1.3. Practical relevance	12
1.4. Academic relevance	12
1.5. Research question	12
1.6. Concept overview	14
1.6.1 Outsourcing & Offshoring	14
1.6.1. Financial Institution	14
1.6.2. Regulations	14
1.6.3. Data protection regulations	15
1.6.4. Information Security	15
1.6.5. Information Security Management	15
1.6.6. Information Security Controls	15
1.7. Core concepts relationship	16
Chapter 2 - Literature review	19
2.1. Research on offshoring in financial institutions	19
2.1.1. Motivation	20
2.1.2. Subject of outsourcing	21
2.1.3. Risks	22
2.1.4. Outsourcing models	23
2.2. Research on information security in financial institutions engaged in outsourcing	24
2.2.1. Information security risks faced by financial institution engaged in offshoring	24
2.2.2. Meaning of information security for financial institutions	25
2.3. Research on data protection regulations	25
2.3.1. Means of data security provision	25
2.3.2. Data protection as corporate image factor	26
2.4. Research on Information Security Management	26
2.4.1. Definition	26
2.4.2. Motivation	26
2.4.3. Challenges and risks	26
2.5. Implications of literature review for research model	27
Chapter 3 - Research methodology	29

3.1.	Research approach	29
3.1.1.	Observation	30
3.1.2.	Questionnaire	30
3.2.	Case Study Observation.....	30
3.3.	Questionnaire	31
3.3.1.	Sampling.....	32
3.4.	Discussion	33
3.4.1.	Internal validity.....	33
3.4.2.	External validity.....	34
3.4.3.	Construct validity	34
3.4.4.	Reliability	34
Chapter 4	- Case study observations	35
4.1.	Financial industry overview	35
4.1.1.	Market position	35
4.1.2.	Case under study.....	35
4.1.3.	Observation	37
4.1.4.	Conclusion	40
Chapter 5	- Survey Results	42
5.1.	Background of respondents:.....	43
5.1.1.	Demographics:.....	43
5.2.	Practical relevance	44
5.2.1.	Offshoring development	44
5.2.2.	Motivation for offshoring	45
5.2.3.	Risks in offshoring	45
5.2.4.	Potential response to aforementioned risks	49
5.2.5.	Practical relevance summary	49
5.2.6.	Information security management	49
5.2.7.	Conclusion	53
Chapter 6	- Summary & discussion	54
6.1.	Summary	54
6.1.1.	What information security related risks do the Swiss financial institutions face when offshoring?	56
6.1.2.	What challenges do Swiss financial institutions face when implementing and maintaining the information security controls?	57
6.1.3.	How to design information security controls that will contribute to information security risk (probability and impact) reduction in case of a Swiss financial institutions engaged in offshoring?	57
6.2.	Conclusion	60
6.3.	Academic relevance	61
6.4.	Practical relevance	62
6.5.	Rigor of research	62

6.6.	Limitations.....	62
6.7.	Reflection.....	63
Appendix I: Questionnaire – questions and answers summary		64
1.1	Online version.....	73
1.2	Offline version.....	85
1.3	Questionnaire	86
Appendix II.....		96
Works Cited		64

Summary

In the times of emerging technologies and rising individuals' awareness more light is shed on privacy and associated risks. This does not go unnoticed by regulators, that develop and enforce tighter requirements towards organisations. Simultaneously, outsourcing relationships develop and offshoring as well as nearshoring are still popular among cost-optimisation methods. While many security methods are discovered and developed and numerous standards and best practices exist that talk about information security management systems, there is only limited literature on how to develop and implement these controls so that they bring the expected value.

The goal of this research was to present guidelines for designing and implementing information security management system controls on basis of identified risks and issues with controls existing at the time. This was to support existing financial institutions with improving their internal controls for information security when engaging in offshoring relationships. The goal was achieved through qualitative methods: case study observation followed by a questionnaire that was distributed among and answered by information security advisors and specialists with extensive experience in financial sector. Case study is a Swiss globally operating bank that outsources its processes to a number of offshore and nearshore locations. The bank has had a number of controls and processes already well established at the time of the research.

This research confirms that financial institutions face various obstacles and issues at different phases of offshoring. The most commonly identified included: dispersed responsibilities, issues arising at the time of offshoring that could be identified prior to decision to outsource and finally – lack of power to enforce technical controls over vendors. The guidelines developed include but are not limited to: focus on additional areas when preparing for offshoring initiative, establishing and defining responsibilities across different teams in the organisation and with the vendor and defining detailed contractual clauses.

The findings from this thesis also open opportunities for further research – to investigate the relationship between these guidelines and efficiency of information security management system or to quantify impact of these guidelines in order to prioritise them. Similar research could also be conducted in other sectors and organisations to provide evidence for the research generalization.

Keywords: ISMS, information security management system, privacy, offshoring, bank, financial institution

Chapter 1 - Introduction

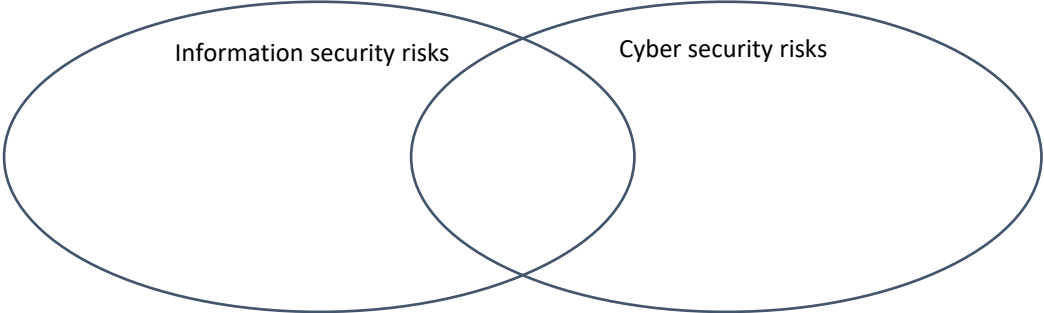
This section of the thesis will shed the light on problem description through a brief introduction of the problem context (outsourcing, data protection and information security management with regard to financial institutions) followed by the problem description, its background and the research objective. By the end of this chapter, relevance of this research to the academic and practical environments should be clear and understood.

1.1. Context

1.1.1. Outsourcing

Although outsourcing is a notion that has been present in the business for at least 20 years now (McLellan & Beamish, 1994), recent reports still predict further growth of outsourcing in the future (TechNavio, 2016). Especially that given the technology development such as cloud computing, easier

process and data transfer between companies and countries are enabled (Deloitte Development LCC, 2012)



(Deloitte, 2014). Offshoring, outsourcing and subcontracting is easier now than ever, thanks to the technology developments (Willcocks, 2014) (Deloitte, 2014), but also thanks to improved telecommunication capacities between countries and lower costs (Leavitt, 2007) (Gabzhalilov, 2016).

According to a Grant Thornton’s report from 2014, 40% of global businesses had outsourced or were planning to outsource business processes. (Grant Thornton, 2014) The motivation, subject, risks and models of offshoring presented in academic research are discussed in Chapter 2.

Financial institutions are no different in this matter. Outsourcing is a critical part of their management of business operations and control of costs (Skadden, Arps, State, Meagher & Flom LLP & Affiliates, 2014). The back office outsourcing market in the financial services sector is expected to reach CAGR (Compound Aggregated Growth Rate) of 7.46% in the upcoming five years (TechNavio, 2016) while the outsourcing market in general is assumed to rise by 6% CAGR (TechNavio, 2016).

This shows that outsourcing, despite local technology and capability development, will not fade in the nearest future (Professional Outsourcing Resources, 2014) (TechNavio, 2016).

1.1.2. Data protection

There is also another booming trend – cyber-attacks and private data misuse. (Savitz & Toubba, 2011; Symantec, 2016; Maughan, Wugmeister, & Titus, 2006).

Although the definition of cyber-attack is the topic of academic discussions itself (Hathaway, et al., 2012) delivering a simplified generic definition is no longer that easy. Cyber-attacks in this thesis should be understood as any action intending to undermine the function of a computer network. Not all cyber-attacks will aim to obtain access to confidential data for the further purpose of misuse or to impact the functionality of financial systems. These are, however, the key risks identified as consequences of cyber-attacks faced by financial institutions. Information security risks on the other hand do not have to be related to cyber risks, as despite the fact that increased amount of information is stored and processed within IT systems, some information is still stored in hard copy or accessed and processed by humans. Employees may disclose confidential information and the risk of them doing so is an information security risk, but it can be (does not necessarily have to be) a cyber risk as well.

The relationship between the risks therefore can be presented in a simple diagram as below:

FIGURE 1 THE RELATIONSHIP BETWEEN INFORMATION AND CYBER SECURITY RISKS

The estimated average cost of data breach, regardless of the vulnerability exploited, is continuously rising – at \$4 million in 2016 (Yépez & Dixon, 2016) compared to \$3.5 million in 2014 (Ponemon Institute LLC, 2014), when data breach incidents count was estimated at 1541 instances. (Verizon, 2014) Cyber-attacks in the financial sector, in most cases, are related to identity theft rather than accessing financial information (Reisinger, 2015). Identity theft or fraud related to cyber-crime has become a serious issue in the digitalized world, with the number of cases increasing dangerously (BBC, 2015) (Kolah, 2015). As a result regulators and organizations have also started to focus on the problem of data protection. (PwC, 2014)

The cyber-attacks carry risks so high, that regulators try to protect customers and introduce guidelines, regulations and legislations. In 2003 the Fair Credit Reporting Act was established, requiring financial organizations to implement identity theft prevention programs. Regulation was later updated in 2013 with the Dodd-Frank Act (PwC, 2013). In late 2013 the Federal Reserve Board, the biggest financial regulator in the United States issued guidelines for managing the risks of outsourcing by financial institutions. Meanwhile in Europe, the majority of the countries focuses on the secondary crime – fraud, rather than identity theft itself. Exceptions are Estonia, France, Slovenia and Poland. However, despite the introduced regulations in the four aforementioned countries, there is a published survey that shows that the population does not consider existing legislations to be effective in fighting the identity theft. Also ENISA (European Network and Information Security Agency) released Guidelines for Information Security awareness in financial organizations in 2009, and the European Data Protection Supervisor released Guidelines on data protection in EU financial services regulation in 2014, followed by General Data Protection Regulation released by European Commission in April 2016.

Aside to the demanding regulations, organizations also need to respond to the rising cyber threats (McNeal, 2014). Although the investment did not rise immediately when the cyber threats arose, recent cyber-attacks in the banking industry caused the financial institutions to re-think their spending (Drinkwater, 2014) (Martin, 2014). A recent Deloitte survey on offshoring shows that 23% of respondents relate their offshoring decisions to cyber threats, while 50% of respondents begun changing their processes due to identified cyber risks. (Deloitte, 2016) Research on data protection in outsourcing and in financial institutions is also discussed in Chapter 2.

1.1.3. Information security management

One of the solutions to address the rising cyber threats and regulatory requirements is the implementation of holistic programs (Lainhart i Ballister, 2016) that will address the information security related risks for various types of data, across entire data processing cycles and across the whole organization. An example of a holistic program is the Information Security Management System. (Aleksandrova, 2014) (Ernst&Young, 2014) Information Security Management system should be understood as a management system or program aiming at information security provision. Information Security Management consists of many aspects, such as: standards, procedures, policies, management system audits, certification & accreditation, codes-of-practice, process ISMS, product ISMS, assurance and culture, human, ethical, social and legal issues (Eloff & Eloff, 2003). Standards

promote controls and code of practice to be implemented to ensure basic information security environment and compliance with the standard's requirements. The first international standard on information security management ISO1799 was released in 2000. Procedures and policies constitute the basis of information security management systems and they can define processes across the entire organization. Policies will be more generic, such as information security policy specifying generic ruleset that the organisation has decided to follow, or acceptable use policy that defines the rules for users on how they can use company's assets. Audits are the processes that aim to verify whether the processes conducted are in line with the set policies or standards. Audits usually have a baseline set by standard or compliance requirements and they serve the purpose of internal or external confirmation of adhering to them. External audits (and for some standards even internal self assessments) can result in certification or accreditation. For example, when an entity is granted an ISO 27001 certification, it provides information that the entity operates in line with the standard requirements without giving confidential details to business partners or vendors. Codes of practice on the other hand will specify generic guidelines on how to achieve a level of information security satisfying the standard requirements. Some standards can be codes of practice at the same time. ISO 17799 is actually called "Code of practice for information security management" and it specifies how to initiate, build, maintain and improve information security management in company. Codes of practice can also be issued by governmental and supervisory bodies as a source of information to refer to, that gathers information on how to achieve one's goals. (Eloff & Eloff, 2003) then divide the areas that codes of practice can be applied to: human, process and product (technology). Some of the standards and codes will set requirements onto security culture, awareness, training and ethics. People need to be trained, inter alia, how to identify information security risks and how to address them. Process component of ISMS can be a software change management process that requires approval of qualified personnel (that will be able to identify risks and see how they are addressed). Standards and codes of practice can often require certain processes to be in place such as risk assessments being conducted before new system is introduced to the IT environment. Finally, products also constitute in large part to information security management because certain equipment or architecture can be more prone to cyber-attacks than other. For example, following 2017's ransomware attacks – Windows XP or Windows Server 2003 would be considered high risk and would not constitute a high information security level. Assurance, similarly to audit, aims at reassuring that company operates in line with the rules it had set up. Assurance can mean monthly testing of patches installed to server operating system on servers that process sensitive information. Such test will serve the confirmation that the process of patching is working properly as defined in procedures and therefore in line with policies and codes of conduct. Other components of information security management system are related to culture, ethical, social and legal aspects. Although Eloff has combined these aspects into one component of information security management, the fact that they are mentioned highlights the importance of each individual's approach towards information security as a part of overarching information management system.

All of the aspects discussed above can be managed with mechanisms and controls, which is a widely used term defining actions that aim at assuring achievement of the company's objectives – whether directly or indirectly. The controls may be preventive – such as access rights being granted to users on business-need basis to prevent the users from accessing information they do not need access to, or detective – actions of users are reviewed post factum to detect instances where actions performed by a user were not in line with business objectives and user role. They may be performed manually (user actions undergo manual review performed by IT employee who reads through user's logs) or automatically (user action log is scanned with a use of automated tools so each inappropriate action triggers e-mail alerts to assigned stakeholders. The controls also can have different levels of granularity

– from high level – such as the rule of access rights being granted on business-need basis to very detailed level such as the rule that no user in System X should have access right A and B at the same time. The trade-off between high level and very well defined controls is that on one side high level controls will be suitable for more companies, across more industries in various situations with different risk profiles; on the other hand they are difficult to understand and implement. Detailed controls are easier to understand and implement, but there is no one-size-fits-all solution.

Lack of this universally applicable solution is partially addressed by work performed by international standard organisations that define and frame information security management system to some extent, too. The international standards then can be used as a baseline across numerous organisations or industries.

The information security management system is for example the focus of one of international standards – ISO 27000 family. ISO 27000 introduces the concept of Information Security Management System and useful vocabulary including the definition of ISMS itself as “that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security”. ISO 27001 focuses on design and implementation of high quality ISMS. This is the standard from the entire family that is most often used across industries as baseline of security levels. Compliance with the standard itself can also serve as a control already (one of certification and accreditation type). The standard consists of over hundred controls suggested to establish a holistic information security management system divided into 35 control objectives across 14 sections. The sections include, among others, policies, organization, asset control, access management and others. However, the requirements of ISMS focusing specifically on the relationship with third parties are limited (A.15 in Appendix controls; ISO27001:2013). The relevant section focuses mainly on managing the supplier service delivery and briefly mentions (a) monitoring of the services provided and (b) continuous improvement of information security in the relationship. The standard covers numerous aspects of information security management, therefore it provides only high level controls drawn from market best practice. The ISO standard only addresses the risks arising from established relationship with vendor, while the offshoring process can carry information security risks across different phases of the offshoring – from the moment a company makes a decision to outsource until contract with vendor is terminated and all data is deleted or handed over. Additionally, the standard is directed to companies across all industry sectors, therefore it cannot provide detailed guidance to be used by one sector, such as financial institutions, in particular. As the 27000 standards are international and do not hold any geographical limitations to its applicability, they cannot relate to country or region specific regulatory requirements. It means that for some countries, where legal requirements towards information security have been defined, certification may not be sufficient to comply with these requirements. ISO27002 provides code of practice, ISO27003 is an implementation guidance, and ISO27004 develops the concept of monitoring, measurement, analysis and improvement. The ISO27000 family consists of another twenty eight standards, including ISO27009 that is to help internal functions of organisations modify requirements of ISO27001 to suit specific industry sector more.

More detail on the academic and practical work with regards to information security management systems and their practical relevance is summarized in Chapter 2.

Having introduced the current state of outsourcing, data protection and information security management topic, the context of this thesis becomes more clear. The context of the problem that this research is addressing is the rapid development of risks that financial institutions face with regards to data protection. Financial institutions process larger volumes of highly confidential data as part of their core operations. They are engaged in more outsourcing and offshoring arrangements. National

and international regulations require more focus on customer data protection and customers themselves become more aware of the risks associated with data breaches. On top of these, financial institutions and customer data are commonly targeted by cyber-attacks. The market currently responds to these developments with generic guidelines on implementation of information security management systems. Understanding of this context is crucial for a more detailed definition of the problem and the related research objective.

1.2. Problem formulation and research objective

1.2.1. Problem owner

As many external factors impact the situation of financial institution and constitute the problem at stake, the issue of finding the explicit problem owner becomes complex. It is clear that it is the financial institution that has to be able to respond to the challenges of external environment and address the information security, compliance and reputation risks, while maintaining its business operations. Financial institutions, especially in Switzerland, the domain of our study, hire thousands of employees and hundreds of contractors and, clearly, not all of them are engaged in information security or offshoring related processes to be assigned responsibility of this problem. The organizational structures of financial institutions are so complex, that the responsibility of similar issue can be assigned to employees of IT, IT security, information security, risk or even procurement or compliance departments. Each of them have potential impact on the shape of the outsourcing process or information security management system. Employees of IT department would be expected to have the knowledge of IT infrastructure underlying bank processes, including structures of data and network communication in place. Employees of IT security or information security departments will be the ones with knowledge of the bank information security controls and acceptable risk levels. Compliance departments are usually responsible for identification of and response to new and changing legal requirements. Finally, procurement will be responsible for vendor selection process management, while transition managers will manage the whole offshoring process. At times, even the operational employees will have impact on the risks as they will know what data is used in the process and how the criticality of this data in the process should be assessed. Possibly, there are separate teams to conduct vendor risk assessments prior and during the offshoring relationship. The number of different actors that do have an impact on data protection in offshoring across the financial institution can actually be considered a problem of its own. According to scientific research, implementation of information security focus is not a pure technical issue, it may also become strategic or even a legal issue (Birman, 2000). The process of outsourcing processes in a way that maintains institution's levels of information security, addresses not only the cybercrime, but also the data protection regulations and internal challenges, needs to be supported by general policies, structures and procedures that come from the management board or the executives. For this reason and also the fact that the problem to be addressed appears multidimensional and it affects wide group of financial institution's customers – the true problem owner of this issue is located high in the organizational structure: position that is responsible for ensuring information security and compliance across the entire organization, often globally. It could be either Chief Operations Officer, Chief Risk Officer, Chief Information Officer, Chief Technology Officer or Chief Information Security Officer. The title of the position depends on the maturity of organization (among other factors), but most major Swiss banks have Chief Information Security Officers appointed supported by large teams constituting to so called Chief Information Security Office. In some banks, the position has not been assigned and the information security remains the responsibility of Chief Technology or Information Officers.

The result of this research is expected to serve as guidance for the financial institution's decisive body – CXO – with addressing the aforementioned information security challenges that financial institution faces when offshoring to offshore third party vendors in era of developing cyber threats and privacy requirements. The CXO is expected to minimize information security risks, therefore reducing compliance and reputation risk. They are facing the constantly changing environment but have many teams engaged in offshoring at their disposal. The complex problem of security risk cannot be addressed with an universal solution that will suit every organization. In fact, even industry specific solution will most likely not be suitable for every company in the industry, as each entity uses different technology infrastructure, has processes organized differently and differs in risk appetite. At the same time, the guidelines available on the market and regulatory requirements appear too generic and therefore difficult to be applied without in-depth analysis.

In addition to practical value that this research is to bring, from academic perspective, this research is to provide information on information security risks that financial institutions face when they engage in offshoring. From literature study, as described in Chapter 2, it was noted that currently available research does not provide details on information security controls effectiveness to address information security risks associated with offshoring risks for any industry in particular, including financial industry.

1.2.2. Problem definition

In order to formulate the problem at stake, let us summarize the context of the issue. This research tackles truly multidimensional issue: the information security risks emerging from outsourcing processes in which financial institutions engage with external vendor, especially when located outside of the country, needs to be supported not only by regulators, but also by the strategy, organization and coherent, overarching information security management system. As explained before the system translates to many elements such as strategy, organisation, human aspects, technology or code of practice – or as discussed, a set of defined control activities across all these elements. On top of various ways to address the problem, there is a large number of stakeholders of the issue including CXO, information security specialists, offshoring programme managers, vendor's management and employees, risk and compliance office or data privacy officer.

The problem at stake therefore is addressing information security risks that emerge from offshoring with effective information security controls that constitute information security management system and consider regulatory requirements and emerging cyber threats in a Swiss financial institution.

The guidance should take into account the current state of organisation – its size, structure and processes as well as success and failure stories from the market to help the bank address the risks in a way that will be efficient and lasting. The focus of the guidance will be the risks associated with offshoring process from the decision to outsource to the go-live phase, when process is being performed by the vendor entirely.

The guidance should serve the design of effective information security management controls i.e. processes, solutions, organisation that will aim at more efficient management of information security across the offshoring process.

The stated problem lead to exact objective of this research, to provide guidance on design of internal controls that suit the organization, that address information security risks that emerge from offshoring and consider regulatory requirements and developing cyber threats, and that, finally, work effectively across the organisation.

1.3. Practical relevance

Development of Information Security Management System controls focused on offshoring relationship for Swiss financial institution will address information security risks, coming from emerging technology (employees using cloud services to transfer information between each other), internal challenges (dispersed responsibility for maintaining satisfactory levels of information security) and stricter regulations coming from national and international bodies and advisory boards in the process of offshoring should be understood that as development of additional mechanisms, controls and processes that will constitute an ISMS. This research will focus on the case of Swiss financial institutions outsourcing to an Indian vendor, however the mechanisms designed as result of this research should also serve as guidance to other financial institutions, conscious about information security in outsourcing. In the design process, the scientifically proven challenges of implementing information security will be addressed, so that the outcome of this thesis can be widely used as future reference for design of additional information security controls aimed at managing information security in their offshoring activities. Guidance on how to implement the mechanisms will contribute to the improvement of the financial institution information security practice.

1.4. Academic relevance

It is important for this research to also bring value to academic research on top of the practical value it brings. Currently available academic research focuses on identification of ISMS elements, developing threat landscapes and technical means to improve information security. As elaborated in more detail in Chapter 2, most academic research is focused on information security best strategies and practices, but does not respond to a particular problem faced by Swiss regulated financial institutions or institutions engaged in offshoring, and especially not to a institution that is facing both challenges.

There are at least eight publications that show differences and similarities between regulations towards information security and privacy across various countries and regions, but none of them show the rising issues and problems related to implementation of the regulatory requirements to financial institutions. (Ruiter & Warnier, 2011) (Tan, 1999) (Jie, 2008) (Wu, Lau, Atkin, & Lin, 2011) (Johnson & Lincke, 2014) (Boehm, 2015) (Tovino, 2017) (Bygrave, 2014)

Also data breach is academically investigated, however academic literature is often missing the insights from different perspectives. Literature will usually provide information based on strategic or technical cases and market observations. By providing analysis of different perspectives (information security consultants, cyber security consultants, outsourcing consultants as well as financial institutions specialists and offshore vendor employees) on information security in offshoring this research can fill the literature gap to certain extent. It provides data on information security management in outsourcing that takes into account the increased threat of cyber-attacks, stricter regulations and organizational challenges as observed by the specialists in recent years.

1.5. Research question

We have presented the practical problem at stake and its current context – the regulatory requirements, developing technology and cybercrime and offshoring as a risk-bearing but still cost efficient practice. The question now stands how this research tackles this problem. The problem formulation and context alongside to defined research objective allowed identification of research questions, answer to which is provided by this paper.

The research questions formulated below were generated on basis of the introductory literature review, summarized broadly above and in detail in Chapter 2 aside to the already defined research objective.

1. How to design effective information security controls that will contribute to information security risk (probability and impact) reduction in the case of Swiss financial institutions engaged in offshoring?

Information Security Management Systems, understood as part of overall management have been used to address information security risks across variously sized companies in different sectors, different locations. We already know that information security management system translates into a set of control activities that are defined per organisation.

It is common to apply Information Security Management System controls to address information security level throughout organization in general. The purpose of this research is to identify how the guidelines and characteristics of the control design process and the controls themselves to efficiently address the risks faced by specific case of engagement in offshoring relationship. In order to define this relationship between successful information security management system and reduction of information security risks the following sub-questions needed to be answered first. The answers to the questions were derived with the use of literature study, case study observation and a questionnaire (survey) distributed to information security specialists from financial institutions, consulting companies and third party service providers as detailed out below.

2. What information security related risks do Swiss financial institutions face when offshoring?

The risks in general constitute to at least one of the following categories: reputational, compliance, or financial. The impact of information security breach on all of the three categories of risks needed to be understood in order to address them by relevant information security controls. For the purpose of designing the controls that will address compliance risks, relevant legal requirements needed to be explored. Similarly to identifying controls in place the information on the current risks and their relevancy was commenced with literature and industry report study, followed by case study observation and survey, where respondents were asked to, inter alia, identify and rate most relevant risks. One of the risks that required more detailed study than others was the risk of regulatory incompliance. This is because regulatory compliance serves the baseline of security controls to be implemented across different organisations. To obtain better understanding of compliance risks, relevant legal regulations, academic literature, industry reports and supported with sources of knowledge for Switzerland applicable regulations were studied including: website of International Comparative Legal Guides, website of Swiss Bankers Association and the portal of Swiss Government. On top of information security risks that emerge from offshoring, we have to ensure that the guidelines are overcoming current obstacles of being efficiently implemented.

Design of controls therefore needed to address potential implementation and maintenance obstacles caused by organizational or technical aspects.

3. What challenges do Swiss financial institutions face when implementing and maintaining the information security controls?

The answer to this question consisted of two subparts. First of all it was important to identify existing information security controls by study of existing academic literature, through case study observation and via a survey, where respondents with financial institution and consulting background provide their insights on what they have seen and experienced with regards to ISMS at Swiss banks. Knowing that banks continuously make attempts to improve their information security controls, it was also important to understand what makes some controls work better than others. Identification of implementation challenges helped to maintain the focus of this research on increasing the efficiency of existing controls. The challenges were raised by respondents in the

semi-structured questionnaire, so that the challenges from financial institution and vendor perspective could be identified. Finally, it was important to investigate the potential impact that the security controls can have and in what ways on probability and impact of information security risk materialization.

On basis of the information gathered from academic and industry reports, as well as current legislation documents and the information on currently implemented controls, related risks and challenges from the questionnaire and case study observations, we are able to deliver a qualitative analysis of the findings and identify the key factors of information security management system controls that ensure higher impact on information security risks.

Before we further elaborate on the current context to finally move on to the research results and answers to the above questions we first will discuss some of the presented concepts in more detail in order to obtain common understanding and present the introductory relationship between them.

1.6. Concept overview

1.6.1 Outsourcing & Offshoring

Outsourcing became a business strategy no earlier than in 1989 (Mullin, 1996). As a strategy, it involves contracting out activities to a third party supplier. We speak of outsourcing in case when the third party supplier, also called a service provider, can be located also onshore, in the same country as the client. Offshoring, on the contrary, is contracting out activities to a third party supplier located specifically outside of the client's country implying that the clients' data need to be transferred outside of the country or the supplier needs to be granted access to client's data from another country (Colwill, 2006). Graham et al. mention that outsourcing transaction is not solely process transfer. Outsourcing can also define transfer of a department or capability (Graham, 1996). Some authors, when defining outsourcing, focus on the level of service provided. Graham et al. state that the level of service should be at minimum the same, as before the transfer (Graham, 1996).

In this thesis outsourcing will be treated as a transfer of corporate activities from the location run and managed by the outsourcing company to the process receiver's staff, offshore location and management.

1.6.1. Financial Institution

Financial institutions can be perceived as institutions playing the role of financial intermediaries between primary saving and borrowing sectors (Kumar, Strategies and Structures of Financial Institutions, 2014). Financial intermediary is an institution that not only takes a role in transforming funds gathered from many individuals into financial asset (Krugman & Wells, 2006), but also resolve the limitations of imperfect financial market by collecting the information that buyers and sellers do not have access to – accept funds from surplus units and channel the funds to deficit units (Madura, 2014). The financial intermediaries include mutual funds, pension funds, life insurance companies and banks (Krugman & Wells, 2006).

1.6.2. Regulations

Kumar in his workings defines financial regulations as the laws and rules governing financial institutions, aimed at protecting investors and supporting financial stability (Kumar, Regulatory Environment of Financial Institutions, 2014). Among the regulations that affect financial institutions we also find the regulations regarding privacy and data protection. These should be understood as laws and regulations, that advocate and mandate security processes, data protection and breach reports (Wong, 2013).

This research focuses on regulations and directives directed to banks as financial institutions in terms of information security, data protection and data confidentiality.

1.6.3. Data protection regulations

Data protection regulations, as spoken of in this paper, should be understood as a mean towards human right to privacy. Human rights, including the right to data privacy, are usually defined by constitutional law. For example, Swiss Constitution highlights each person's right to protection against the misuse of his or her personal data. EU data protection act requires processing of the data to be fair and conducted lawfully and only conducted when the data was obtained for specified and lawful purpose. The data gathered should be adequate to the process for which is used. According to the EU law, personal data is any information relating to identified or identifiable natural person; an identifiable person is one who can be identified by identification number or one or more data elements specific to the person's physical, physiological, mental, economic, cultural or social identity (Office of Data Protection Commissioner, n.d.) (Walder Wyss, 2015).

Additionally to Data Protection Acts, across the world some governments decided to establish regulations specific for financial data. In the United States, Right to Financial Privacy Act ensuring protection of customer financial data was established in 1978 and amended by USA PATRIOT Act in 2001. Also the Bank Secrecy acts should be mentioned here as they describe the cases in which the exchange of customer related information between financial institutions is allowed.

1.6.4. Information Security

Information security is the response to the data protection regulations. It can be defined as the preservation of the confidentiality, integrity and availability of information (von Solms & van Niekerk, 2013) The three concepts of confidentiality, integrity and availability are the primary concepts of information security, also known in the form of CIA triad. Confidentiality should be understood as a component of privacy as it refers to protecting the information from unauthorized access. Integrity assures that information is not modified in an unauthorized manner. Finally, availability stands for accessibility to the information for authorized users and employees, at required times. There are also other models explaining information security, such as Parkerian hexad, yet CIA triad is the most widely used and known (Andress, 2014).

1.6.5. Information Security Management

Information Security Management process may include tasks such as security planning, policy formation, staffing, risk management, security technology selection, threat assessment, countermeasure implementation, performance monitoring and maintenance (Nazareth & Choi, 2015).

ISO27001, as discussed before is one of the most popular international standard implemented in organizations. The standard defines the information security management system as 'that part of overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security' including 'organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources'. The overall process aims at 'selection of adequate and proportionate security controls that protect information assets and give confidence to third parties' (Ashended, 2008).

This paper will treat information security management as processes that aim at provision of data confidentiality, integrity and availability.

1.6.6. Information Security Controls

Information security controls is a term that is used often when information security management system is discussed. Information security controls are defined as administrative, management,

technical, or legal methods, also called safeguards or countermeasures, used to manage risk. Controls can include practices, policies, procedures, programs, techniques, technologies, guidelines, and organizational structures. SANS Institute extends understanding of managing risk by presenting it as avoiding, counteracting and minimizing loss or unavailability due to threats acting on their matching vulnerability (Northcutt, n.d.).

Having defined the key concepts that are under investigation in this paper, the next chapter will summarize the existing literature on the interrelations of the aforementioned four concepts (outsourcing, financial institution, data protection regulations and information security management).

1.7. Core concepts relationship

As it can be easily observed, the concepts introduced are highly related. This section summarizes the relation between the aforementioned concepts and provides graphical representation, which will serve as a guideline for this research.

First we were introduced to outsourcing as a trend across industries with financial industry being no different. Financial institutions outsource their core activities, but also accounting tasks, internal audit, human resources, project management and others.

Although very popular, outsourcing itself carries numerous risks, especially when outsourcing to another country. Very often, however, the benefits of the outsourcing outweigh the risks and companies decide to direct their processes to another side of the globe. In case such decision is made, the client (the company that will no longer be handling the process) must address all these risks during and after the process of transition. Inter alia, one could identify the risks that lead to data breach, especially that most of the data in any process is now stored digitally (Accenture, 2015).

The problem of addressing risks and information security issues across different stages of transition and post-transition processes is so complex that it requires a dedicated part of cross-functional management system implemented via relevant information security controls.

This summary gives us an overview of what concepts are the focus of this research and the graphical representation of their relationships can be seen in Figure 2 and Figure 3.

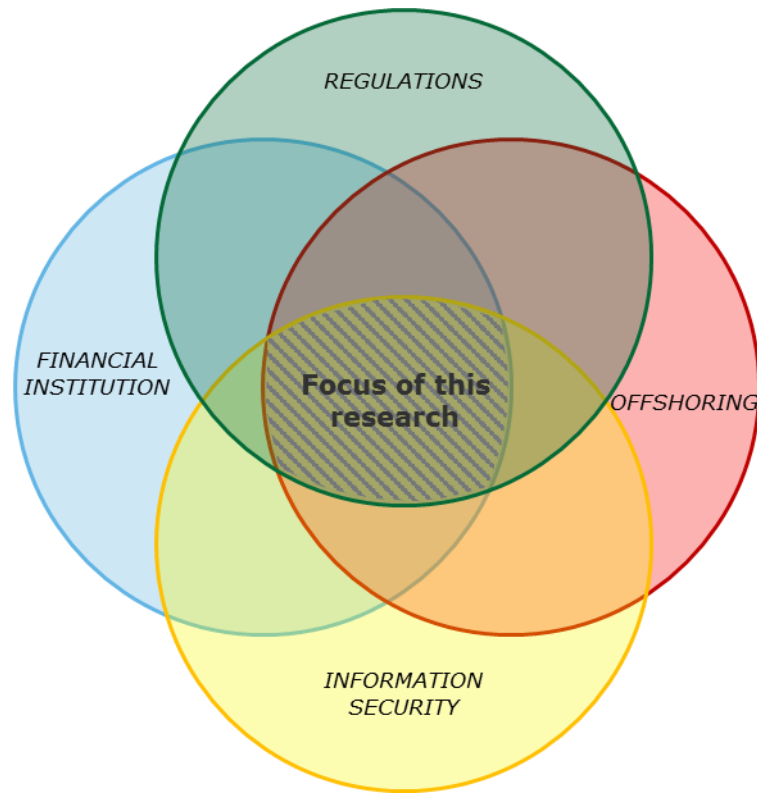


FIGURE 2 CORE CONCEPTS

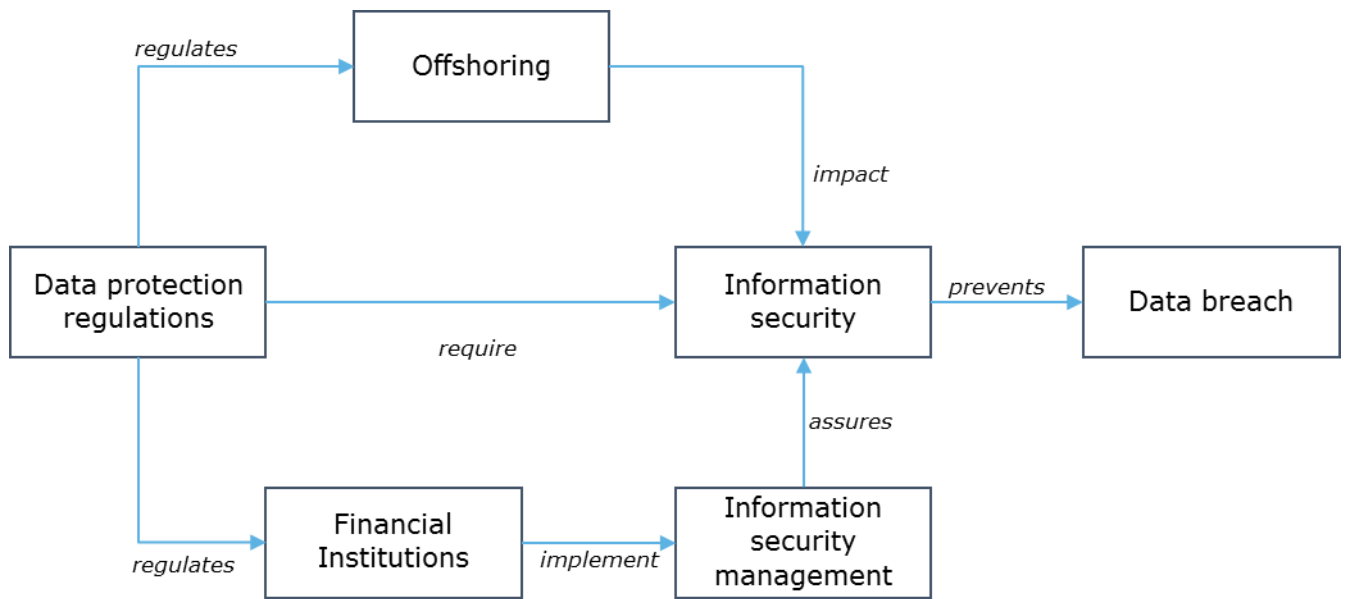


FIGURE 3 CORE CONCEPTS AND THEIR RELATIONSHIP

The generic core concepts and their relationship model is used in the next chapter as the baseline structure of literature review. In the literature review the concepts and the relationship between them will be further investigated for better understanding. Confirmation and further development of this model through literature review also serves as the basis on which the questionnaire was designed ensuring its relevancy and completeness.

Chapter 2 - Literature review

The topic of information security management in financial institutions' outsourcing, although very specific, is broad and widely related to many fields of academic research. The section is structured by interrelation between concepts as the point where they all overlap were the main focus of the literature review: an extensive number of publications and articles may be found on each of the concepts separately, therefore focus on interrelations created a natural limit to the literature review scope. From studying Figure 1, the following interrelations have been drawn: offshoring at financial institutions, information security at financial institutions engaged in offshoring, information security regulations, offshoring regulations and financial institution regulations. As financial institution regulations tackle many more challenges other than offshoring or information security (i.e. they focus on financial aspects in major part in order to ensure soundness and stability of financial markets), this literature research focuses on the remaining four areas: offshoring at financial institutions, information security at financial institutions engaged in offshoring and finally information security and offshoring regulations.

This section of the thesis concludes the findings of academic research conducted in these areas in order to present proven concepts relationship and models. This section of the thesis will also support the argument on how this research complements the existing literature.

Additionally, the below literature review together with the following chapter, both serve as a basis for the research design process, highlighting issues and problems that should be tackled during interview or observation sessions.

It has to be noted here that due to limited availability of literature on this narrow topic, both scientific articles as well as industry reports were studied to provide better understanding of the issue. However, it is the scientific articles that were considered trustworthy and reliable, while industry reports served only for context study. [Research on offshoring in financial institutions](#)

The topic of business process offshoring in scientific literature is not novel. The first scientific article on outsourcing was published in 1976 – “A manufacturer looks for quiet tires”. The market size of outsourcing and offshoring varies between sources, but all agree on its rapid development. In 1989 and 1990, the size of US outsourcing market was estimated at \$26 billion (Harker, 2012), while global IT outsourcing value was estimated at \$9 billion (Lacity & Willcocks, 2009). In 1994 a research presented outsourcing as already booming with market value in financial industry only exceeding \$8 billion (McLellan & Beamish, 1994), while a survey conducted in 1998 showed the worldwide spending on outsourcing services reached \$86 billion in 1996 (Baldwin, Irani, & Love, 2001). In 2013, the global outsourcing contract value for business and IT services outsourcing was about \$648 billion with the 4.8% compound annual growth expected through and to the end of 2018 (Fersht & Snowdon, 2013).

The concepts from the initial concept model were *financial institutions* and *offshoring*. For each of these terms we have identified cognate terms on the basis of initial keyword review.

Financial institution: *financial organization, financial organisation, banking company, bank, banking, financial industry, financial sector, financial services.*

The reason for not being able to use solely *financial* was that initial search of literature returned a significant number of publications on *financial aid, financial networks, financial products, financial management, financial jeopardy, financial performance*, which are found irrelevant.

Offshoring: *outsourcing, BPO, global sourcing*

Articles for the following part of this section are publications found by searching “financial institution” or “financial organization” or “financial organisation” or “banking company” or “bank” or “banking” or “financial industry” or “financial sector” or “financial services” and “offshoring” or “outsourcing” or “BPO” or “global sourcing” in abstract/title/topic/keywords fields across popular scientific search engines: Scopus (554 articles found), Science Direct (49), Web of Knowledge (220) and Google Scholar (994). The search altogether resulted in 1382 unique academic publications on financial institutions engaged in offshoring – only two out of all concepts as presented in concept relationship model. The number was obtained by exporting the searches from each of the search engines and removing duplicates on basis of title and year of publication were removed to obtain this number.

The papers were then assessed for their relevance on the basis of title, keywords and abstracts. Out of all results, just 142 articles were found relevant (the initial results also covered topics such as renewable energy, manufacturing sector development, cryptocurrencies and financial markets, macro-prudential regulations stating financial requirements, logistics as well as offshore countries economy development as it is associated with offshoring).

The first conclusion to be drawn from the literature review is that there is relatively little literature describing the processes of outsourcing by financial institutions. While the reason behind limited research could be due to there being little difference between outsourcing in the financial sector and in any other sector, what the researchers mention in their works is the banks’ reluctance to respond (Kazmierczyk & Macholak, 2014). Within the available literature, the areas that are most often covered by the research workings are Computer Science (43%) and Management (35%). Some articles are market specific - often discussed markets include African (Kenya, Namibia), Asian (India, China, Malaysia), American (USA) and European (Germany, UK).

To summarize the topics frequently occurring in the scientific articles, the following paragraph lists examples of the research investigating different aspects of outsourcing. Overall, most of scientific articles available focus on the decision to outsource (Penter, Wreford, Pervan, & Davidson, 2013) (Lin, Devinney, & Holcomb, 2016), risks (Bott & Milkau, 2015) (Strong, Cater-Steel, & Lane, 2014) (Jimmy Gandhi, Sauser, & Gorod, 2012) and opportunities (Bataev, 2015) (Ee, Abdul Halim, & Ramayah, 2013) (Franke & Wullenweber, 2006), current state or outsourcing development (McLellan & Beamish, 1994) (Graham, 1996) and its impact on the local and global markets (Fragoso-Diaz, 2015) (Gupta, Ganguli, & Ponnampalnam, 2015) (Babin & Nicholson, 2012). Some focus on successful strategies of outsourcing (Aksin & Masini, 2008) (Goodman & Ramer, 2007) (Kazmierczyk & Macholak, 2014) (Kalakota & Robinson, 2004) (Mullin, 1996). However, little percentage shows the aspects of information security (Kull, 2011) (Du, 2014) (Roses, Hoppen, Ballaz, & De Mello Freire, 2006) or even vendor management (MacKerron, Kumar, Benedikt, & Kumar, 2015), not to mention Switzerland specific research on outsourcing (Beutler, 2008) – topics that are related to this research in the largest extent. Relevant insights from these papers are grouped into three sections: motivation, subject of outsourcing, risks and outsourcing models. These are presented in the below sections of this chapter.

2.1.1. Motivation

Out of the 142 studied scientific papers, 17 describe the common reasons behind outsourcing. The motivation behind outsourcing was researched as familiarity with the generic goal of outsourcing is

expected to bring value to the design phase of Information Security Management controls. In the case studies or nation-wide analyses the reasons behind the growing outsourcing market include shortage of skilled human capital, privatization and deregulation pressures, emerging technologies (Baldwin, Irani, & Love, 2001) as well as enhancement of performance, reduction of costs, access to expertise and strategic reasons (Suryanarayan & Sabyasachi, 2013). The research among Polish banks showed that it is the desire to reduce costs rather than the desire to increase the quality of services that motivates the decision to outsource (Kazmierczyk & Macholak, 2014). In case of the Kenyan banking sector, the main reason for outsourcing is the perceived cost reduction, but other motives include focus on core competence, improved services, access to specialized vendor and flexibility (Barako, 2008) (Koech, Minja, Koyier, & Wachira, 2016). Also, Beutler shows in his research that Swiss banks decide to outsource for the benefits like cost reduction, access to talent pools, access to market, process optimization and some strategic benefits (Beutler, 2008).

In their work, Tas and Sunder compare the financial sector to the manufacturing industry, hence concluding that the main motivation behind the decision to outsource is process efficiency and optimization (Tas & Sunder, 2004). The reasons for outsourcing across all industries are similar with key drivers being cost reduction and economies of scale or focus on core competencies (Dinu, 2015) (Kakabadse & Kakabadse, 2005) (Sparrow, 2004) (Mehta, Armenakis, Mehta, & Irani, 2006) (Saxena & Bharadwaj, 2009) (Mahmoodzadeh, Jalalinia, & Yazdi, 2009) (Wu & Park, 2009), access to technology advancements (Sahgal & Malhotra, 2005) access to qualified workforce focus on core competencies (Dinu, 2015) (Ghodeswar & Vaidyanathan, 2008), reaching global markets, improvement of service quality or as a part of expansion strategy (Sharma & Loh, 2009) (Iqbal & Munir Dad, 2013)

The aforementioned reasons for outsourcing can relate easily to the three views that are extensively cited in general outsourcing literature: Transaction-Cost view, Competence Based View and Relational View. Transaction-Cost view supports the theory that cost reduction is the most important factor behind the decision to outsource (Sparrow, 2004) (Sahgal & Malhotra, 2005) (Kakabadse & Kakabadse, 2005) (Sharma & Loh, 2009). Competence-based view explains organizations' decision to outsource as a result of focusing on organizations' core competencies (Leavy, 2004) (von Rosing, et al., 2015), although later research shows, that organizations also outsource their core processes (Mehta, Armenakis, Mehta, & Irani, 2006) (von Rosing, et al., 2015). Finally, Relational View that highlights the importance of client-vendor relationship and the opportunities it carries: competitive advantage by process efficiency improvement on both sides (Mehta, Armenakis, Mehta, & Irani, 2006) (Saxena & Bharadwaj, 2009) (Kakabadse & Kakabadse, 2005) (Vaxevainou & Konstantopoulos, 2014).

2.1.2. Subject of outsourcing

In banking industry, the popular functions to be outsourced included IT systems, back-office operations, call centers and human resources operations (Harangus, 2010). In 2001 the most popular functions to be outsourced were the ones from areas of Information Technology and Information Systems, with hardware maintenance being the most outsourced service and mainframe and data center management to follow (Baldwin, Irani, & Love, 2001). There is little literature on the subject of outsourcing that banks engage into, but multiple workings refer particularly to IS outsourcing (Dhillon, Syed, & Sa-Soares, 2016) (Gorla, The impact of IT outsourcing on information systems success, 2014) and some to outsourcing as well as some of the core processes (Silva, Guerra, Tabak, & de Castro Miranda, 2016). Generally, companies begin outsourcing with processes that have low impact on their operations (Beutler, 2008). As they introduce more core processes offshore, the firms in financial industry focus on back-office processes such as check clearing, payment processing or credit rating (Tas & Sunder, 2004).

As per research in 2008, the infrastructure processes were the first to be outsourced by Swiss banks due to low impact on bank's performance. Infrastructure processes include data processing, networks and desktop services (Beutler, 2008). In comparison, in 2014, in Poland, the most outsourced service was security, followed by legal and training services, IT, Transportation and recruitment and with remuneration, incentives, staff legal, social issues service to close the list (Kazmierczyk & Macholak, 2014). The Kenyan study of banking sector showed that the most outsourced service is ATM and card processing, followed by debt collection, IT, HR and Sales and Marketing (Barako, 2008), while the popular process to be outsourced by the Kazakhstani banks is card processing (Tayauova, 2012).

2.1.3. Risks

Another side of outsourcing research studied to a certain extent is risk management (Leavy, 2004) (Mehta, Armenakis, Mehta, & Irani, 2006) (Bott & Milkau, 2015) (Strong, Cater-Steel, & Lane, 2014) (Jimmy Gandhi, Sauser, & Gorod, 2012). Outsourcing organizations should maintain a comprehensive risk management framework to address various categories of risks (Gonzalez, Llopis, & Gasco, 2013).

Literature identifies a number of outsourcing risks and groups them into categories, where possible. One categorization divides the risks into operational risks, strategic risks and other risks that do not fall into any of these categories (Iqbal & Munir Dad, 2013). Aron et al. presents strategic risks as vendor's deliberate actions directed at the client. It could be intellectual property loss, loss of local experts to perform the actions in house (Herath & Kishore, 2009) (Aron, Clemons, & Reddi, 2005). Operational risks include decline in service quality, unforeseen, increasing costs, wrong vendor selection and inefficiently defined IT requirements (Aron, Clemons, & Reddi, 2005) or, as Deutsche Bank recognizes: fraud risk, business continuity risk, regulatory compliance risk, information technology risk, outsourcing risk and legal risk (Kumar, Cases on Universal Banking, 2014).

Another categorization of risk suggests vendor attitude problems, vendor competence problems, vendor coordination problems and in-house competence problems (Gorla & Lau, Will negative experiences impact future IT outsourcing?, 2010). Still, such division does not cover all of the possible risks that outsourcing transactions carry (Kazmierczyk & Macholak, 2014).

Risks that remain outside of the mentioned categories include client-vendor culture (Sparrow, 2004) (Ramingwong & Sajeev, 2007), loss of privacy and control (Sparrow, 2004) (Swartz, 2004) (von Rosing, et al., 2015), loss of internal know-how or poor contract management (Mahmoodzadeh, Jalalinia, & Yazdi, 2009). Additionally, DeutscheBank identifies outsourcing risks as a separate category.

The risks identified through national financial industry analyses across different countries do not deviate from the risks mentioned above. Analysis of Kenyan banking sector shows that reputational and strategic risks are more important than compliance or operational risks. However, as the author admits it can be caused because the outsourcing in Kenya is performed within one country rather than offshore (Barako, 2008). The biggest problems faced by the Kazakhstani banks show hidden costs, but also quality problems and more rarely loss of managerial control and threat to security and confidentiality (Tayauova, 2012). Institutions from in the German banking sector, engaged in outsourcing also chose strategic and financial risks (part of operational) as the main risks behind outsourcing (Gewald & Dibbern, 2009). Swedish banking institutions remain sceptical towards outsourcing some of their processes due to financial consequences of cumulative risks they cannot afford when outsourcing processes related to their core business, loss of integrity and process control, misunderstood system requirements and finally language and cultural barriers, that will impact the control, integrity and quality of service (Jonsson, Moeller, & Lillieskold, 2007).

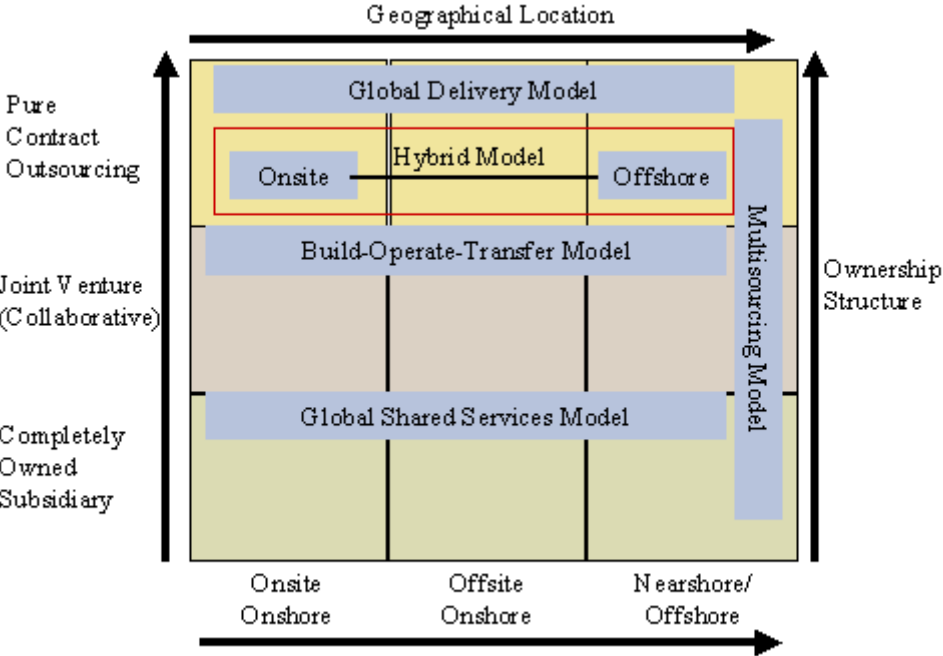
Some research confirms that completeness of contract clauses on outsourcing risks is greater for BPO deals with penalty clauses rather than BPO deals without a penalty system (Gellings & Wuellenweber, 2007).

2.1.4. Outsourcing models

Another focus of existing literature is the operational and organizational aspects of outsourcing: there are publications available that put the process of outsourcing and developed certain process models.

MIT Press highlights the evolution of captive center model. Captive center should be understood as a subsidiary or branch office located nearshore or offshore, providing back office services, owned by the offshoring entity, entirely or partially (Oshri, 2011). Captive centers were a trend also in 2014 (Ochri, Kotlarsky, & Willocks, 2013) The opposite model to the captive center is the outsourced model, which stands for outsourcing products, services or functions to third-party organization (Lewin & Peeters, 2006). Outsourcing can at times bring more value to the company at stake with example of Citibank as a proof (Mukherjee, Gaur, & Datta, 2013) It is important to note here, that despite the trends, recent research shows that global financial service firms have adopted a multi-sourcing pendulum strategy by experimenting with different configurations to explore the optimal supply base for a given function (Liang, Wang, Xue, & Cui, 2016).

Some extensive work on models between the full ownership and no ownership of the offshore location was done by Kalakota and Robinson. Their work shows the different strategies on the basis of the location of the service provider and ownership structure between entity and its service provider. Having defined three categories for geographical location (Onsite Onshore, Offsite Onshore and Nearshore/Offshore) and three categories for ownership structure (Pure Contract Outsourcing, Joint Venture, completely owned subsidiary) the matrix of outsourcing business models can be presented.



Source: (Kalakota & Robinson, Offshore Outsourcing Business Models, 2004)

The matrix allowed placing each of the strategies to show the differences and similarities between them. Global Delivery Model is usually ran by advisory sourcing company (Accenture, IBM, Infosys) in multiple locations (close and far from the client) to ensure better communication between the client and the service provider. The companies usually serve numerous large clients, and using economy of

scale can distribute the required competences more effectively, while also being more adaptive to clients' requirements or sudden structuring changes. Global Shared Service Model is the previously described Hybrid model. Build-Operate-Transfer model emerged from numerous failures of entities to build an offshore center. The build phase is based on a contract with the offshore partner to deliver an office space with competent employees. The vendor in such cases is responsible for any legal and administrative issues, while preparing the site for work. The Operate phase is the agreement for the offshore partner to conduct necessary management services: staffing, payroll, security, accent training. Finally, when the client is ready to absorb the unit and control and manage processes, people and facilities offshore, they are given the option to transfer. It is the option to transfer that requires the team and the office to be built up separately, as otherwise running vendor entity would be at risk of losing some of its capital to the client due to transfer. Multi-sourcing is practically contracting numerous offshore suppliers to reduce the concentration risks and hence, the monopoly that one provider may have. Some companies (Citibank, American Express) locate their subsidiary near the number of contracted vendors in order to enhance cooperation between company's employees and vendors' employees at company's offshore site. In other cases, the central unit that cooperates with the wide network of service providers is not the subsidiary but selected one vendor.

As one can observe, hybrid units have also been identified on the market. Strategy of hybrid units implies the delivery of the service to be completed with the combination of offshore and onshore processes (Kalakota & Robinson, *Emerging Business Models in Offshore Outsourcing*, no date available).

2.2. [Research on information security in financial institutions engaged in outsourcing](#)

Out of the 142 documents found using the search formula from the section above (articles that cover the topic of financial institutions and offshoring), only seven focus on information security. They were searched within the previous results (142) in order to ensure that they cover all three core concepts of this research: financial institution, offshoring and information security. Within the information security domain, they focus on: provision of security for compliance (Kull, 2011), data privacy in cloud computing (Wenge, Lampe, Muller, & Schaarschmidt, 2014), internet bank security (Du, 2014), outsourcing in the days of cyber crime (Amant, 2007), secure outsourcing of scientific computations (Atallah, Pantazopoulos, & Spafford, 2002), as well as end to end privacy in outsourcing human intensive processes (Hung, et al., *End-to-end privacy control in service outsourcing of human intensive processes: A multi-layered Web service integration approach*, 2007) (Hung, et al., *Towards end-to-end privacy control in the outsourcing of marketing activities: A web service integration solution*, 2005). These seven articles are therefore the articles that cover three out of four core concepts of this research: financial institution, offshoring and information security.

2.2.1. [Information security risks faced by financial institution engaged in offshoring](#)

Multiple articles, although not entirely focused on information security but on outsourcing risks or challenges do mention information security as one of these risks (Beutler, 2008). The information security risks that are still present (whether lower or higher) when financial institution engages in offshoring are loss of intellectual property, data leakage, incompliance. These become even higher risks due to lower visibility over security, pressure on timely reactions in business relationships and low awareness among employees and consumers. (Johnson, Goetz, & Pfleeger, 2009) Another article focused on offshoring risks highlights the underestimated impact of inadequate information security mechanisms not aligned to neither the outsourced activity nor to the location and vendor. The word underestimated is used, because these can lead to intellectual property breach or data breach that will follow with long-term consequences. (Nassimbeni, Sartor, & Dus, 2012). These conclusions are based on generic industry research and generalised across other industries, including financial institution.

The next subsection highlights the meaning of information security to financial institutions, so that in the later stage of the research the risks specific to financial sector can be identified.

2.2.2. Meaning of information security for financial institutions

Financial institutions similarly to other organizations operating in service industries, process large amounts of customer data, including sensitive data, in their daily transactions. Contrasting to healthcare industry, where employees of the organization are largely concerned about errors in patient information, employees of the banking industry are concerned about improper access to customer information. Protection of information processed by financial institutions and belonging to the most important assets or properties is one of the institution's most significant objectives. Some researchers mention that understanding and protecting personal privacy in information systems is even more critical in the industries where the event of customer data misuse may have harmful effects (Earp & Payton, 2006). Beutler claims that Swiss privacy law is the biggest challenge in offshoring conducted by banks (Beutler, 2008).

2.3. Research on data protection regulations

Wenge et al. in their work on cloud computing, where cloud computing is defined as a specific case of outsourcing, present a summary of legal requirements and satisfactory technical solutions out of the available (Wenge, Lampe, Muller, & Schaarschmidt, 2014). Legal requirements list was delivered on the basis of over 25 documents applicable to different countries across the globe. The list constituted of the following requirements: secure data access, secure personal data transfer, prevention of data access through third persons, secure data outsourcing and data processing, data integrity, confidentiality and availability, geographical requirements, secure cross-border data transactions, right to audit, transparency of data transfer processing, compliance, security guarantees and, finally, defined roles and responsibilities. (Wenge, Lampe, Muller, & Schaarschmidt, 2014)

2.3.1. Means of data security provision

The results of the research performed by Wenge et al. showed corresponding tools on basis of academic research. Therefore, means to provide data security and satisfy legal requirements include: role-based and right-based access management, access control lists, data labelling, need to know principle, least privilege principle, implementation of ISO27000 controls, multi-factor authentication, physical access control, anonymization and pseudonymization of data, virtual private network, data encryption, securing of transfer channels, security staff trainings, prohibition of access, monitoring and logging, physical segregation, EU standard contract with third countries, user consents, auditing, public-key infrastructure, business continuity and disaster recovery measurements, contractual obligations, application of European local territorial laws to branches abroad, cloud-provider certifications, risk management frameworks, PCI DSS, reporting and SLAs. (Wenge, Lampe, Muller, & Schaarschmidt, 2014) Other researchers confirm the proposed solutions one by one (Nassimbeni, Sartor, & Dus, 2012), (Fenn, Shooter, & Allan, 2002). They suggest to address this issue in outsourcing is inclusion of metrics corresponding to information security in the Service Level Agreement (SLA) or to take the third party implemented security mechanisms during the supplier selection or to draw quality controllers' attention to data protection related problems (Nassimbeni, Sartor, & Dus, 2012) (Fenn, Shooter, & Allan, 2002). South African service provider case study was concluded with the finding that the data protection compliance does not only depend on the controls implemented by the client such as aforementioned contract or employment relationship, but also the manner in which employees are paid, managed and on what contract basis they are employed (Ball, 2010).

2.3.2. Data protection as corporate image factor

Aside to the compliance requirements, research from as early as 1988 conducted by LeBlanc and Nguyen considers information security as one of the factors contributing to customer-personnel interaction. Among seven factors representing components of perceived quality, customer-personnel interaction receives the lowest score (LeBlanc & Nguyen, Customers' Perceptions of Service Quality in Financial Institutions, 1988). Similar research was repeated in 1996, by the same researchers. In their second work, confidentiality of transactions was considered as a factor of reputation of directors, which was proven to have the highest impact on the corporate image variance (38,5%) (LeBlanc & Nguyen, Cues used by customers evaluating corporate image in service firms, 1996) Although the studies do not prove the point directly, other sources openly admit the increased awareness of customers towards their privacy and data protection (Graeff & Harmon, 2002) (Hung, et al., Towards end-to-end privacy control in the outsourcing of marketing activities: A web service integration solution, 2005) (Dolnicar & Jordaan, 2006) (Hille, Walsh, & Cleveland, 2015).

2.4. Research on Information Security Management

The search for “isms” or “information security management” within the results of previous searches brought no results. As there is also little academic research on information security management processes in financial institutions or in outsourcing processes, this section will summarize the findings related to Information Security Management across industries and areas of interest. The following section has been divided into definition of information security management systems, the motivation behind implementation of ISMS and the challenges and risks that implementation of ISMS faces.

2.4.1. Definition

Information Security Management Systems are designed and implemented in order to manage and operate information security system continuously in terms of technology, management and hardware, for the aim of the information security that is to achieve confidentiality, integrity and availability. (Jo, Kim, & Won, 2010)

2.4.2. Motivation

Financial institutions are required to implement information protection management systems, also called information security management systems (ISMS) by governmental bodies ever since the security threats increased with development of electronic financial transactions. (Kim, et al., 2016) The main goal of the ISMS is to protect governments' or organizations' information assets and intercept any existing risks for secure information management of their customer and themselves. (Jo, Kim, & Won, 2010)

2.4.3. Challenges and risks

One of the key aspects that is analyzed in the academic research are the challenges that information security management implementation carries. Werlinger et al. have identified eighteen challenges on the basis of 36 semi-structured interviews with IT security specialists. The researchers suggested division of the challenges into three categories: human, organizational and technological. The identified human factors included: lack of training and experience, culture within the organization, communication of security issues. Risk estimation, open environments and academic freedom, lack of budget, security as low priority, tight schedules, business relationships with other organizations, distribution of IT responsibilities, access control to sensitive data, size of the organization and top management support are the constitute to organizational factors. Technological factors include complexity of systems, vulnerabilities, mobility and distributed access and lack of effective security tools (Werlinger, Hawkey, & Beznosov, 2008). Some of these challenges have been identified in

another independent research work. The von Solms' identified "deadly sins" of ISM focus on the low awareness of information security management concept. Not seeing ISM as a complex, multi-dimensional issue related to entire organization and its employees on all levels that requires planning and monitoring can cause problems in ISM implementation. Additionally, successful implementation of ISM requires support of adequate organizational structure (roles and responsibilities in information security field) and tools and mechanisms. Researchers also highlight that it is crucial to plan Information Security Management on the basis of identified risks (von Solms & von Solms, 2004).

Organizational culture

Impact of organizational culture on the success of ISM implementation is the factor in the area of researchers' focus. Culture can be explained as the manner in which processes and operations are performed in order to protect information assets (Da Veiga & Martins, 2015). Practical application of information security management has been analyzed for Saudi Arabian organizations. The authors separate information security management into three techniques to be used simultaneously and continuously: avoidance, deterrence and segregation of corrective measures. The brief survey conducted by the researchers showed that in most organizations the employees are not aware of information security policy and policy breach consequences (Alsaif, Aljaafari, & Khan, 2015). Such problems can be addressed by one of the developed frameworks – The Human Diamond that aims at raising awareness and responsibility among organizations' employees and, more specifically, teaching the proper usage of information assets (AlHogail, 2015), rewarding the information security compliant behavior (Box & Pottas, A model for information security compliant behaviour in the healthcare context, 2014) or developing Information Security Awareness programs focusing on positive emotions (Box & Pottas, Improving information security behaviour in the healthcare context, 2013) and monitoring the implemented model, for example using information security culture assessment (ISCA) (De Veiga & Martins, 2015)

Technology

On top of models aiming at building or improving information security culture, the conducted literature study, brought into focus also models that address technological factors such as lack of proper technology and supporting tools. Nazareth & Choi model can serve as information security investment decision support (Nazareth & Choi, 2015)

Although no research has been identified on the process of information security control design, this matter is explored in further detail in the next chapter, explaining what are the controls, what role do they play in Information Security Management and why they are a key matter for the purpose of this research.

2.5. Implications of literature review for research model

There is additional research focused on comparison of regulations from Europe, US and Asia-Pacific region. Nevertheless, analysis of such broad choice of regulations deviates from the topic of this research. This paragraph is to highlight the importance of data protection in financial institutions on one side and show literature gaps with regards to banks' perspective on application of the regulations. The scientific research on data breach is highly limited. Science Direct search of articles with 'data' and 'breach' in the title, abstract or keywords returned 472 results, out of which 81 was related to information security rather than geo- or marine- engineering. The 81 articles were published in journals and editorials as follows: Computer Fraud & Security, Network Security, Computer Law & Security Review, Infosecurity, Computers & Security, Information Security Technical Report and Digital Investigation. Out of the 81 articles published in scientific sources only one happened to be a scientific

research focused on dual-use of open source security software, without reference to banking or financial sector.

The above described literature study allows identification of some aspects that will be later applied during design of controls. First of all, existing literature confirms that financial institutions engage in outsourcing and offshoring, what makes them face associated risks. These risks include information security, data protection and compliance risks. The literature therefore confirms the possible further practical use of this study, but also implies some guidelines on possible controls such as contract clauses.

The revised model of concepts addressed by this research is presented below in Figure 5. The literature review gave more understanding around information security, what impacts information security in offshoring and why it may be important to the financial institution to maintain compliance with regulations. The revised model helped structuring the observations as well as designing the questionnaire that were used as data collection methods in this research.

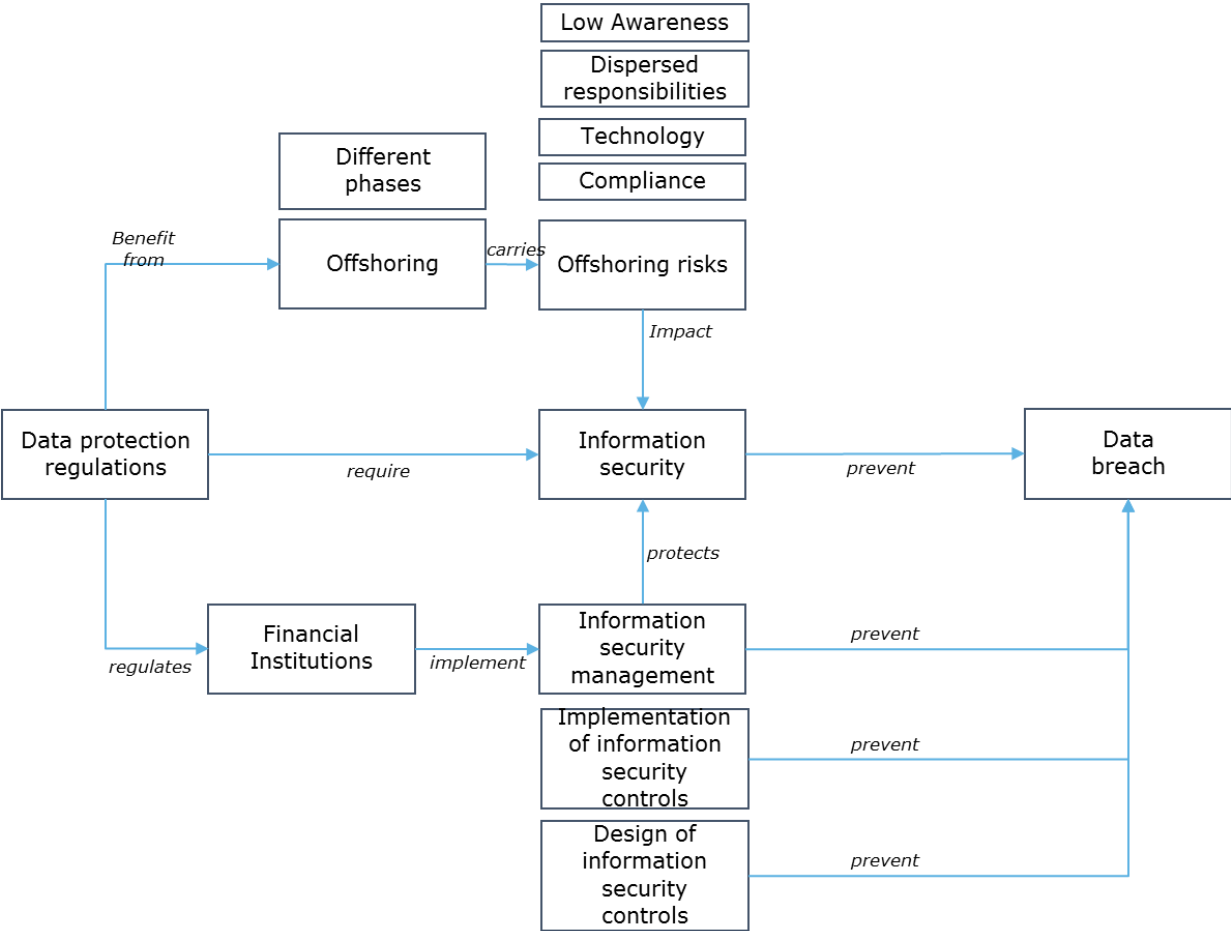


FIGURE 4 CONCEPT RELATIONSHIP REVISED

Chapter 3 - Research methodology

Before we introduce the research methodology and the reasoning behind data collection methods in this chapter, let us once again look at the purpose of this research. The end goal of this research was to identify the principles that would help the financial institution improve Information Security Management System and its controls to make it more efficient in the current, extremely complex, environment that takes into account the regulatory requirements as well as developing threats and conscious customers. What added another layer of complexity is that the financial institutions had been responding to increasing requirements and technology risks over past decades and the guidelines must take into account the fact that the controls are not being designed from scratch, but rather starting with the existing situation. As shown in the literature review this approach was rather unique, because it was very specific, prepared for a specific scenario. Unlike available sources, it focused on a particular situation of the case under study that may be possible to extrapolate onto other industry organisations or other geographical locations.

3.1. Research approach

The goal and outcome of this research was subjective: the situation continues to change and develop, organisations are in different situations, but also every management consists of people of different backgrounds, culture and experience. This is why the design of the research was based on the constructivist research philosophy. Throughout the research, it was assumed that reality – in this case information security risks, relevant internal control design and implementation challenges – are subject to interpretation of human beings but also to context and environment. The goal of this research was to provide guidance for internal control design and implementation that will address offshoring risks and ensure controls' effectiveness. This could only be achieved by understanding the concepts of the relationship between information security risks and information security management in the process of offshoring. As the research context is also specific (Swiss financial institution engaged in offshoring to an India-based vendor), yet broad (it only defines the industry sector and geographical location) it also proves the constructivist philosophy.

As the concept of information security risks, information security management and outsourcing in financial institutions is both new and complex, this mixed method research was selected to investigate the concepts at stake and deliver the answer to the research question "How can information security controls contribute to information security risk (probability and impact) reduction in the case that a Swiss financial institutions engaged in offshoring?". Mixed method implies that qualitative and quantitative information has been collected and analysed to answer this question and to identify controls and controls features that will have the largest impact on data protection improvement at Swiss financial institutions. The methods were mixed at data collection level as the data was collected using qualitative (observation) and quantitative (questionnaire) methods. Also the levels of observation varied across the used methods with observation being focused on one particular organisation and questionnaire looking at any Swiss financial institution engaged in offshoring (in order to eliminate strengths and weaknesses of the particular organisation at stake and provide information and viewpoints from representatives of different groups of respondents).

The non-experimental mixed method research was selected as the most beneficial for this thesis, as it allowed triangulation of data, complementarity of results, gathering and presentation of more comprehensive data. It helped addressing the limited availability of quantitative data, yet allows comparison of qualitative insights originating from different sources. Mixed method research also supports validation of the results acquired, based on the individual methods for data collection used in this thesis and therefore contributes to the broader generalizability of the research results. These two features of mixed methods research were particularly important in this project, as the results of

this research – guidelines for internal control systems – were to be applicable across financial institutions engaged in offshoring.

Data collection methods used in this research included participatory observation of a case study followed by a written questionnaire with closed and open-ended questions. The methods were applied sequentially. Results of the observations had impact on the structure and questions of the questionnaire. The quantitative questionnaire also served a bigger part in delivering the answers to the research questions due to the limited nature of the observation (observer placed for a limited time in one team of a global organisation was not capable of observing enough detail with regards to the research concept models).

3.1.1. Observation

In the first part of the research – the observer was placed in one of the teams of the Swiss financial institution that was engaged in managing the transition initiatives (process offshoring). As per suggestions given by (Merriam, 1998) the primary focus at the start of the observation was to confirm the purpose of further study shifting later towards people, activities, processes and policies as well as communication and interactions in order to confirm offshoring risks, information security management practices within the real case example of organisation.

3.1.2. Questionnaire

In the second part of the research, expert's point of view on the problem was gathered. The written questionnaire helped reach the research objective of identifying the efficiency factors of information security management system controls in order to improve existing sets of controls. This was achieved by asking the respondents about the most common obstacles in achieving high effectiveness of controls, by validating the importance of information security risks and current state of offshoring in financial institutions. When choosing questionnaires as the method of data collection, we had in mind its advantage of reducing the impact of external factors on the respondent's answers. By using online survey tools, the respondents were able to provide answers at a time convenient to them without the presence of third parties, therefore the risk of their answers being impacted by mood, emotions, behaviour or feelings was reduced.

The details of these two data collection methods and the activities performed as part of this research follow in the next sections of this chapter.

3.2. Case Study Observation

In order to validate the concepts identified in the literature review, confirm the practical relevance of the research as well as to assure better questionnaire design and questionnaire results understanding, observation of a case study was conducted. The observation lasted for six months and focused on the aspects identified in the literature research, subject to observatory limitations.

The observations were performed by:

- identification and study of relevant corporate documentation available on financial institution's resources;
- Observation of transition managers who are responsible for the management of offshoring a business process to an offshore vendor and ensuring the process enablers such as know-how or technology are made available to the vendor, following their consent.
- Observation of analysts and managers of vendor risk management teams – who are responsible for conducting periodic risk management, following their consent.
- Observation of analysts responsible for risk analysis of technology supporting the business processes in the process of transition to the vendor, following their consent.

- Participatory observation at monthly meetings of Project Management Office teams where current issues in managing business process offshoring were discussed.

Following the initial phase of the observation, where rapport was built and relationships as well as observation context were established, the focus of the observation shifted to more detailed areas of the offshoring process. Throughout the course of observation, different processes and procedures were identified while meetings discussed various offshoring issues. The meetings and processes helped to structure the more focused part of the observation in the following sections:

- [Processes preceding decision to outsource a process](#) – observation focused on identification of processes related to outsourcing but preceding the decision to outsource, including identification of the corporate strategy that translated to offshoring decisions and criteria used for selection of the process to be offshored. The processes were identified mainly in the study of offshoring policies and procedures, as well as observation of transition managers in the team.
- [Processes preceding selection of the vendor](#) – these processes were included to be under observation in order to identify the criteria on which selections of the vendors are made and other related processes that lead to vendor selection – performed by study of the available policies and shadowing transition managers.
- [Transition process](#) – thanks to participant observation and being part of project management team of the organisation, transition process became a natural part of the observation.
- [Vendor Risk Management](#) – observation in this area helped verifying whether the case under study currently identifies and reacts to risks evolving from engaging in an offshore relationship or from engaging in an offshore relationship with, what risks are identified. The data was obtained from the project management office meetings, available documentation and shadowing team’s analysts engaged in offshoring supporting processes.
- [Information security culture in the organization](#) – given the risks that human error or unawareness brings to materialization of information security risks, the culture and awareness building activities with regards to information security was also observed.
- [Information security culture in the offshore location](#) - analogically to observation of the information security culture in the onshore location, the observation puts the spotlight on the knowledge and awareness of information security risks among offshore employees.

Results obtained from the participatory observation are discussed in Chapter 4: Case study observations. However, due to constrain that all information needs to be dealt with in a confidential way, we can only provide a holistic overview and details cannot be provided. Nevertheless, the details were taken into account during analysis and summary of findings.

Subject to availability, but notes on each of the information security risk reducing concepts and challenges related to information security as mentioned in the previous chapter of this thesis were from the real life observation as well as from questionnaire responses.

3.3. Questionnaire

The questionnaire was developed following observation of the case study to formulate an understanding of how processes work in a financial institution, how personnel is trained and what the organisational culture is as well as learning what the offshoring process scheme involves (what the process looks like, who is engaged etc.).

The target audience of the questionnaire was later selected to be among the experts in the financial institution, offshoring and information security fields so a sound knowledge of the wording and concepts was assumed.

The questionnaire was structured into the following sections:

- **demographics** – to confirm the background and experience of the respondent (the most important difference to note here was whether the respondent is providing the responses from a vendor or financial institution perspective)
- **assessment of current state of offshoring** – to establish common understanding of current risks and developments
- **current practices to address emerging risks** – to understand where the focus of information security is in the industry, what are the current levels of information security practices and what are the potential impacts of data breach and how are incidents addressed;
- **better practices to address emerging risks** – respondents were asked to provide information on what they believe could improve the information security levels in financial institutions: we asked about shift of focus, assignment of responsibilities, risk analyses timeliness and features of effective internal controls and internal control system such as information security management system.

The questionnaire form that was sent to the respondents is presented in Appendix I: Questionnaire.

The questionnaire has been distributed among selected respondents, who are informed of the purpose of the research. Moreover, the respondents were aware that the research may be beneficial to them as well and this fact should limit untruthful and encourage thoughtful responses.

3.3.1. Sampling

The data for the purpose of this research was collected via a written questionnaire with closed and open-ended questions, distributed among experts in the field of outsourcing, data protection and information security management in financial institutions.

The access to experts specializing in this narrow field of focus, where six of the core concepts meet, is highly limited. For this reason, the selection of experts is a convenience sample, – as the field of information security management, data protection regulations and financial institutions is new and developing, the access to experts in the field is crucial. However there is no database including all experts where we could draw a sample from. However, to improve the data quality the experts were selected from different institutions, i.e Swiss bank, Scottish bank, International bank, Indian service provider, Dutch, Polish and English consulting companies, providing different perspectives, such as senior management and operational staff on the topic. It was also made possible to give access to the questionnaire based on a snow-ball approach.

The questionnaires will be distributed among; experts from consulting companies specializing in financial industry advisory, experienced transition managers responsible for managing the process of outsourcing in a financial institution, staff representatives of the vendor who are responsible for serving the bank and information security specialists from consulting companies as well as financial institutions. Representatives from financial institutions (transition and program managers, information security specialists) were selected in a way so that at least one of the respondents represents a Swiss financial institution. Also representatives from consulting company and offshore vendor company were selected in a way so that at least one of the respondents represents a firm that serves Swiss financial institution.

In the end, fifteen responses were collected. The number is limited and there is a few insights and reasons behind this:

- the questionnaire answers were only collected across two month period; although the contacts were informed of the deadline some may not have found the time to provide the answers
- the questionnaire was detailed and took 20 minutes to complete – some respondents did not find the time to complete the questionnaire, some took the questionnaire on three different attempts
- the questionnaire was to be distributed to a number of subject conference participants as promised by professor Tomi Dahlberg, but was only distributed during one conference.

The respondents were approached directly in person where possible with the advantage of my own professional network. I selected current and former employer staff and consultants I had a chance to work with in the fields of information security, banking and offshoring. All respondents approached directly completed the questionnaires.

Other respondents were approached via the LinkedIn network – also on basis of my professional network, their current and past employers and fields of experience. As the LinkedIn messages did not bring the best results in terms of response, the link to the survey was then distributed by professors Harry Bouwman, Tomi Dahlberg and Albert Plugge to their networks (both related to information systems management, offshoring and banking).

In order to improve the number of gathered responses, the e-mail and LinkedIn recipients were also sent two reminders. One five days and the second one ten days after sending the initial message with the questionnaire link.

Questionnaires were then examined in terms of words, phrases and sentences to identify information related to any of the research questions. Similar views on certain topics were then organized by relevant categories. The number of questionnaires allows manual coding, followed by manual analysis and classification of answers.

Atlas.TI was used in parallel to structure the interpretation of the responders and take into account the possible impact that their position in the company or in the outsourcing relationship may have on the concept perception, in case the manual interpretation did not provide all the insights. As the research has inductive nature, the coding was also performed manually, taking into account the respondent's answers and ideas mentioned.

3.4. Discussion

Now that we have discussed the main steps in our research we want to pay attention to reliability and validity issues.

3.4.1. Internal validity

The research was prone to internal validity issues as the number of specialists available was low and there could be large bias of personal experiences on the day of data collection (such as stress). The associated risk of that is that incorrect or limited guidelines and principles will be drawn from analysis.

For that reason the research was conducted via questionnaire as well as case study observation and both approaches have been planned carefully to address the risks of low internal validity. Questionnaire were distributed to independent respondents, representing different players in the offshoring process (consulting, banking, vendors). Additionally, in order to improve the internal validity – case study observation was participant observation, where the researcher was observing the

company, the organisation and the employees in the natural setting by participating in everyday, business as usual activities. Participant observation is believed to increase the validity of research as it generally provides the researchers with a better understanding of studied phenomena. (DeWalt, 2002)

3.4.2. External validity

As the scope of the research was limited to a particular geographic location and one industry sector, the results can only be generalized to companies that are facing similar risks and challenges. This research expects however, existence of many variables that are out of the scope of this research (organizational structure of the institution, revenues, market position and current public perception) but could potentially have impact on the internal control design and implementation efficiency.

3.4.3. Construct validity

Open-ended questions helped increasing the construct validity and allow respondents to add factors or insights that were not taken into account when the questionnaire was created. Limited literature on the topic and the constantly changing environment internally and externally did not allow for definition of a definite number of questions that will address only the risks and challenges of information security and the influence of internal control system. The questionnaires were only conducted once, which can also impact the construct validity. This was addressed, however, by validation of the results with respondents after information is analysed and conclusions are drawn.

3.4.4. Reliability

The limited number of experts and cases under study can impact the reliability of this research to a large extent. The results of this research cannot be ensured to be stable and consistent if repeated. Time also hinders the reliability of this research; due to technology and cyber threat developing at a fast rate, it cannot be assured that issues currently drawing the attention of experts will be the same, even in the nearest future.

Inclusion of the respondents in validation of the interpretation of the observation and questionnaire results should also address potential reliability issues.

Now that the approach for this research and the reasoning behind it are outlined, the results from case study observation and questionnaire are presented in the following two sections.

Chapter 4 - Case study observations

4.1. Financial industry overview

For the twenty years preceding 2006, the organizations and companies in the financial sector around the world were developing in many directions – providing more products, more communication channels and becoming more complex structurally. The development and spread of financial institution's scope of operations was related, as the world discovered later, to the development of vulnerabilities and risk impact. Currently, the banks focus on re-gaining the revenue and growth that was affected by regulations and other post-crisis risk reducing tools. (Oliver Wyman, 2015)

Swiss financial industry is considered one of the largest financial industries in the world, especially when taking into consideration its impact on gross domestic product (GDP). (Enoch & Segoviano, 2014) It has been one of the most important industries to Swiss economy in terms of its growth for the past twenty years; the statement being valid in spite of the millennial crises that took place in years 2000 - 2002 and 2008 onwards, which have slowed down the growth but did not reduce the industry's importance in national economy. (BAKBASEL, 2014) The slowing down of the development is possibly caused by numerous challenges that financial institutions in Switzerland are facing. One of the main challenges that Swiss banks face in particular is remaining compliant with transnational regulations and standards, in order to be a stable and safe partner in business for organizations from other countries. KPMG also highlights the importance of digitization, automation and outsourcing of processes in the bank's business model aiming at growth and development. (Rickert, 2015) The industry reports therefore seem to highlight the existence of the challenges faced by offshoring financial institutions caused by cyber threats and demanding regulatory requirements. I observed that off shoring plays a big role in the organisation under study – given the observation itself was conducted in major part at one of shared service centers. It was also noted that regulatory compliance and information security were often mentioned during decision making process or as the reason for running certain tasks (i.e. ensuring that applications do not contain any personal identifiable data).

4.1.1. Market position

Swiss banking sector constitutes of 275 banks, with a large group of foreign banks present in the country. This large number includes also asset management banks, private bankers and regional banks. (Swiss Bankers Association, 2018) The case under study is one of the two banks considered significantly bigger than others, however due to confidentiality reasons we cannot provide further details. I observed that the bank conducts its operations globally, providing various services to clients in different parts of the world. The bank has employees in bank locations and bank shared service centers. In addition to this, some of the internal services are provided by third party contractors. The biggest contractors are located in India and, as per observation, provide a large part of back office.

4.1.2. Case under study

History

The first antecedent of the case under study appeared on the market in 1862 causing the Bank to celebrate its 150th anniversary in 2012. However, the bank in its current form has existed on the market since 1998 when it was established as a result of two Swiss banks merging.

Ownership

The bank is a joint-stock company listed on both: Swiss and New York stock exchange. Shareholders equity reaches over 50 billion CHF with the largest institutional shareholders owning only ~4% of all issued shares.

Services

The institution provides services to private, corporate and institutional clients. The organization is also divided functionally: wealth management, personal & corporate banking, asset management, investment banking and corporate center. Wealth management serves wealthy customers globally, while Retail & Corporate serves retail, corporate and institutional clients in Switzerland with comprehensive financial services including bank and third party products. Retail, corporate and institutional clients are served in a multichannel approach. The Investment Bank provides all of the clients segments with expert advice, innovative solutions, execution and comprehensive access to the world's capital markets.

Organization

At the time of the observation the Bank employed over 13,000 of employees in Europe, Asia/Pacific and Americas. In comparison, Bank's financial report from 2014 reports the total number of employees reaching over 60 thousands across 50 different countries.

The most attention should, however be drawn to shared service center as processes related to outsourcing, information technology or information security are in the scope of their responsibility. Organizationally, shared service center is comprised of supporting core functions (including the above) and supporting non-core and legacy portfolio.

Shared service center operations are divided into technology, operations and corporate services and one Chief Officer is responsible for all three divisions. The Bank also assigned Chief Officers responsible for finance and risk. All three of the officers are supported by group legal counsel for ensuring Bank's regulatory compliance.

The observation on the premises of case under study, that was conducted for six months between April and October 2014, took place in a Project Management Office – team within shared service center, division technology. The core task of the team was to support every transition process from start to finish. This includes being responsible for defining the process of transition (performed by Transition Managers on the team), managing the process of transition (also performed by Transition Managers), defining vendor requirements and conducting audit against them (performed by Vendor Risk Assessment employees) as well as supporting the process with technical tasks such as: delivering IT hardware and software to the vendor, verification of data to ensure no personal information is transferred without proper controls in place, outsourcing such as anonymization or pseudonimization. The observation conducted from the position of that team allowed observation of transition process management including the controls being in place when processes related to IT systems and applications are outsourced. Additionally, being a part of the organization allowed observation of the approach to high level risk management including information security management. The real case observation was used not only to verify the real life scenarios against the literature review but also to better adapt the questionnaire form to respondents, who work in similar environments.

Outsourcing approach

The case operates three shared service centers (SSC) located in China, USA and Poland. It cooperates with two third-party outsourcing vendors located in India. At the time of the observation, the number of offshore and nearshore employees reached 20% of the total number of employees. Over 7000 employees of India companies were working for the Bank while 8000 employees were working at shared service centers. The company had a signed contract with Indian outsourcer (hereafter named: Indian Vendor I) (worth around \$250-300m, with initially 1,000 staff deployed), while another technology firm acquired the Indian service centre, becoming another vendor based in India (hereafter named: Indian Vendor II). Both of the vendors have top market information security certifications that assures certain levels of information security that were presented during the procurement process to the bank.

The quality enhancements the third party performed worked together with economic impact and were the main reasons why the Bank commenced a rapid outsourcing strategy in 2012. Based on legal, regulatory and/or competitive considerations the processes are outsourced to a third party provider or to a Shared Service Center.

4.1.3. Observation

Processes preceding decision to outsource a process

Thanks to shadowing Transition Managers and studying the corporate documentation it was observed that each decision that relates to outsourcing follows in-depth analysis and business case definition to ensure that the process can be outsourced in the first place. Each process to be outsourced is first raised as a business offshoring opportunity. The process is then analysed in terms of feasibility, potential savings and estimated cost of transition. Once opportunity is accepted by key stakeholders such as the process owners, IT and security management it is then transformed into initiative. The initiatives are managed by transition managers and start with an in-depth and detailed planning phase to confirm the estimations from opportunity analysis. The focus of these processes is to ensure successful planning and transition but also to ensure no confidential information is sent to unauthorized parties.

During the observation it was noted that although the transition process would often be delayed (as compared to original planning) or more complex to address than initially expected, no transition has been rolled back because of inappropriate processes selected for transition. The planning process was usually very detailed and difficult to manage due to the number of engaged stakeholders, for whom transition was not a business as usual task (process actors, information security subject matter experts, programme managers etc.). It was also noted, that many employees, especially the ones that were engaged in the process to be offshored were reluctant to provide any information, as they were conscious of losing their position in the company.

Processes preceding selection of the vendor

The Bank does not have a large selection of vendors, so the decision usually reflects the already outsourced processes and supports transition of similar processes or processes that use similar resources (i.e. technology or skills). At the time of observation, no new vendors were engaged and approximately the same share of processes have been outsourced by shadowed Transition Managers to both of the bank's vendors. As per discussions and meetings, the fact that only two specified vendors were engaged with the bank for back-office process offshoring made the decision much quicker and efficient. This was the case mainly because the relationship has been established, contact parties were defined on both sides, processing requirements were known to the vendor and the transition could focus purely on the specific process. The discussion around the number of vendors was the first hint on the number of vendors having impact on efficiency of any internal controls around offshoring processes.

Transition process

It was observed that following the decision making and planning process, transition managers commence the transition process by preparing required resources and ensuring all of them are ready at specified dates. Apart from staff trainings, transition managers had to provide technology and teams to be available to take over the process.

Most often the application and technology preparation would consume most of the transition process as it was again dependent on many stakeholders (technology team, security team and the application business owners who were asked to provide detailed information about the applications). It is worth

noting that the transition managers were never engaged in inspecting the applications and data stored and processed, because this responsibility was assigned to the client protection teams.

All the applications used in the process that is being offshored are reviewed in terms of containing and accessing data. The processes use systems hosted in the Bank's as well as vendor's infrastructure and they vary in terms of method of user interaction (thin client, fat client, terminal, web application) and in terms of stored, processed and accessed information. A major part of the application assessment is based on the application owner (author) self-populated questionnaire. This is the most time-efficient method, especially in a financial institution, where a high number of end-user computing applications occur. End User Computing is an umbrella term for all applications and systems created by business users. These can include Microsoft Excel workbooks and Microsoft Access databases and during the observations it became clear that most employees would create their own workbooks that would store or download data from different systems in order to make their work more efficient.

The currently outsourced processes include remote infrastructure management, IT helpdesk, financial reporting, software development, testing and risk management. These processes are based on confidential information related to Bank's financial information, strategic products, used technology and finally, vendors, employees and customers. By default, however, all personal data from which a person's identity can be derived (identifying data) should be anonymized or encrypted before given to the vendor for processing. Therefore if there is any presumption that personal data is stored or processed in an application, it will go through an anonymization process that is conducted in parallel to the transition process.

At the time of the observation, no clear internal controls were communicated to participants, aside from the business as usual process flow. Additionally, during that time no information security issues at this stage of the process were identified, but the process took longer than anticipated on multiple occasions.

Vendor risk management

Risk management approach

The Bank focuses on an operational risk control environment, as it develops core capabilities preventing financial crime, cyber threats and strengthening vendor management. Cyber risk is considered one of the most critical and constantly evolving risks carrying the potential results in data theft, disruption of service and cyber fraud (all with extreme impact on the organization). Bank is certified with ISO27001.

Cyber security is a topic being addressed by the Bank as the number of cyber attacks increases with every year. The five pillars of cyber security approach include: Data Confidentiality, Data Privacy, IT Security, Cyber Threat Management and Physical Security. The approach is tied with risk framework including a set of internal and external risk assessments, and therefore, periodic vendor risk assessments.

Vendor risk management

Vendor risk assessments are run against a standard checklist of requirements and usually are filled by the representative of the vendor. Rarely the assessments were held with regards to a particular process. At no stage of the assessment was the team actually reviewing the internal controls implemented at vendors' sites.

Additionally, as a part of the cyber security approach, internal cyber security controls related to third party vendors located in India require development to reflect evolving risks and the growing number of outsourced processes. Internal threats, current information security awareness levels and the large

number of processes outsourced are the main challenges of the information security. These challenges relate not only to the Bank's employees but all vendor employees who have access to Bank's information. Internal threat is understood as overuse or abuse of assigned access rights to possess confidential information and distribute to interested parties for the purpose of personal gains or to destroy important information. The employees awareness is limited to clear desk (nothing to be left on the desk after work) and clear screen (screens should be locked when unattended) policies.

Low security awareness levels may be exploited by hackers when collecting data on an organization or targeting social engineering or phishing attacks. Additionally, an unaware employee may unintentionally reveal the company's information,. For example, when sending unencrypted attachments or opening an email with malicious content. During the time of the observation however, none of the team members were subject to a phishing attack like that.

As a response the Bank established risk frameworks that are developed by internal teams for internal teams. The frameworks define the baseline of controls that should be in place and performed effectively, and include inter alia Operational Risk Framework. Cyber risks are defended proactively and responsively by teams assigned to first, second and third line of defence. Overarching teams such as technology risk or legal risk or operational risk, that are set cross-geographically will provide the control and management over existing processes.

As for compliance risks, each larger office location will have teams responsible for identifying regulations and regulatory changes that can potentially impact Bank's compliance. The teams feed information that gets translated onto existing risk frameworks when necessary. At the time of the observation the technology teams were responsible for reassuring that the technology related controls are in line with the requirements. It included both – functional and non-functional requirements, such as data reconciliation (functional) or application security (non-functional).

Data protection approach

Information security culture in the organisation

. There is a detailed definition of confidential information that is well known across the staff engaged in the anonymization and pseudonimisation process as well as across system owners. However, some employees that developed end-user computing systems such as MS Excel macro based workbooks or MS Access databases seemed to be unsure of the data their applications process. The Bank responded to that by various analysis tools that were run against each application to be offshored in order to identify potentially confidential information.

The Bank has global, regional and local teams responsible for information systems security and appointed Chief Information Security Officers across organisation. During the time of the observation the training for new joiners in terms of information security and incidents was limited, but a lot of focus was put on the information confidentiality. The training would explain clearly that all information processed is considered strictly confidential, unless published publicly by the Bank. However, low awareness was built around actions that should be taken in case incidents were identified. One could say there is definite potential for improvement around internal controls around training of new joiners. Incidents were not communicated to the staff, probably largely due to the fact most of the staff, especially those from internal services teams like PMO, would not have professional contact with external partners, be it customers or vendors directly.

As observed, incidents caused by data unavailability or confidentiality breach would be managed by the local teams and escalated to regional and global teams. Such reporting schemes were also defined for vendor related incidents in the documentation studied.

There were also few incidents reported by the media. At the time of the observation, one incident was caused by a former employee releasing confidential information to American authorities.

Another control that was observed and that heavily relates to data protection was access management control. It became apparent that the Bank is strongly focused not only on external unauthorized users accessing the confidential information, but also accessing information by internal staff. The access rights were therefore given on a 'need to know' basis and each user required management's and system owner's approval to access information. Additionally, confidential information processing systems required additional approval and risk assessments.

I observed two informational campaigns sent to all staff globally with regards to phishing awareness. It was also sighted that the majority of observation participants would delete such communication e-mails without looking. Additionally, on an everyday basis two popular controls were visible across the open space where employees were located – clear desk and clear screen policy. Clear desk policy was a term used for employees to remind them, that if they are away from their desks any hard copies or media with files should be placed out of site, in a key protected locker. Clear screen policy was a term used that means whenever an employee is not at their desk, their computer screen should be locked in order to prevent unauthorised access to the information stored on the computer. These policies were very strictly enforced by random checks and subsequent consequences (report to management and locked computer / locker until the employee in person picked up the unlocking code).

Information security culture at vendor's site

Although at the time of transition itself the vendor's employees approach towards information security was not verified, both vendors were obliged to train their staff with regards to data handling. Although no personal identifying information was shared with the vendor, their approach towards data handling was still considered important by transition managers. No vendor related incident was communicated at the time of the observation, but from the discussion it seemed like such incident would cause significant consequences to the relationship.

During the observation I also contacted the vendor on multiple occasions in order to obtain support for business processes –such as obtain access to certain information or fix network issues. I noted that all information would be provided only if I called from my assigned phone number. With certain level of confidence, it can be concluded that the vendor employees whom I approached had some consciousness about information security.

4.1.4. Conclusion

Although the organization is large and mature in local and global markets, there is always room for improvement. I observed that the awareness of employees with regards to information security rarely expands beyond clear desk and screen policies. However, the information existing in company's resources shows that information security risks are subject to consideration across various teams such as information systems security teams, IT risk teams, Project management office (for vendor risk assessment), Legal and Procurement. The developed risk management approach shows that the Bank takes the risks into account, also during processes such as business process transition. However, I have also learned that the responsibility for information security is highly dispersed - even when it comes to information security in offshoring.

The information obtained during the observation lead me to additional questions to be included in the questionnaire in addition to the questions coming from the literature review:

- The fact that the Bank uses services from two main providers triggered the question to survey the impact of the number of providers on information security risks;

- As the responsibility is dispersed between multiple teams the respondents were asked where the responsibility should be assigned;
- Low awareness of incidents across operational staff lead to a question whether cyber threats are actually a valid risk for banks;
- Questionnaire also asks about the importance of vendor risk assessments during the whole offshoring cycle, as per observation the Bank mainly focuses on risk assessment pre-transition and post transition periodic reviews;

Specialists were also asked whether low awareness among staff on information security risks impacts the overall information security management system efficiency.

The observation also allowed familiarization with organizational culture and organizational challenges that a large, international company may have when introducing new controls and frameworks.

Observation of the case study has helped in structuring and designing the questionnaire but also in understanding the results and viewpoints of respondents. The next chapter shows the questionnaire response analysis.

Chapter 5 - Survey Results

Using the information gathered during observation, the questionnaire for professionals in the field of financial industry, offshoring and information security has been developed. The purpose of the questionnaire was to identify the key risk and key success factors in business process offshoring by a Swiss financial institution to a vendor based offshore (as opposed to nearshore). The questions contained in the questionnaire also covered other aspects of offshoring such as its current state, predictions on development and organization's motivation to offshore processes. These questions were asked in order to identify potential differences in understanding of the matter and confirm relevance of information security management system's and internal control for offshoring risks (hence confirm practical relevance of this research to the industry).

The below analysis is the result of the framework method for analysis of qualitative data. Due to limited amount of data and the fact that the questionnaire is semi-structured, the data was analysed and interpreted manually with the support of atlas.ti software which is commonly used for qualitative data analysis. The framework method is relatively easy to follow as it lists exact steps for researchers to perform: starting with familiarisation with the obtained information, coding the obtained information, refining the themes and developing a working analytical framework. Researchers use this framework to group the codes, charting the information into the framework and finally interpreting the responses as they cover different aspects of the issue. The aim of this analysis was to identify the relationship between the concepts as well as other related concepts not tackled by the literature review previously in order to identify potential issues with information security management and propose solutions or success factors to address these issues. Let me remind you that the issues identified during the observation that may impact the effectiveness of information security internal controls included: low awareness, number of vendors, large number of stakeholders, lack of understanding of the concept of offshoring, timeliness of the offshoring process, conflicting aims in the process and passive vendor risk assessment methods. Aside from tackling these issues specifically – to understand the core underlying cause – the respondents were also asked to share their success stories and experiences from which we, the organisation at stake and other organisations could learn from. This approach makes this research highly practical as it adapts academic research methods to obtain as much practical knowledge as possible. It is also unique in terms of the scope

The survey was published online with the use of ZOHO Survey Online Survey tool. This tool was selected as it allowed publication of questions in a more graphic and easy to understand way but also requests the respondent to put answers in order.

Sections below present the summary of the answers obtained from respondents and insights drawn from them. The complete questionnaire is presented in Appendix I. The summary below has been divided into the following sections:

- structure of respondents – an introductory section that should introduce readers to the respondents providing better understanding of who they are and what experience has driven their respondents;
- practical relevance – as mentioned before the questionnaire contained questions about the respondent's views on the offshoring, its current state and development and their experience with challenges, therefore this question has been differentiated to present the respondent's views; the section confirms that respondents believe that while offshoring is becoming more popular, it is becoming increasingly challenging;

- identified challenges – the section that summarizes the challenges that financial institutions face when offshoring along with the possible causes behind those challenges. As per subject of this research the focus of the questions and therefore responses was put on information security, information security compliance and offshoring.;
- potential solutions to faced challenges – – as the aim of this research was to derive practical guidelines on how the financial institution can address the identified challenges in information security, compliance and offshoring, this section presents the potential solutions and insights from the respondents. This section, combined with other findings serves an important input to the guidelines presented in Chapter 6.

5.1. Background of respondents:

As the survey was published online, anyone with the link to the survey was able to see it and provide answers. The link was sent via LinkedIn or email to the initially selected 10 respondents and the attached message also advised that they were free to inform respondents of similar knowledge and experience to populate the survey. As mentioned earlier, to improve these results, the deadline was given with three weeks notice and everyone who obtained the link was reminded on the 5th and 10th day after sending the original e-mail and also two days before the deadline. All of the respondents were advised that if they prefer to share the information via interview or teleconference, there was a possibility to do that as well.

Additionally, the professors from TUDelft (Harry Bouwman) and academic experts in the field such as Tomi Dahlberg from University of Turku who was co-hosting a conference for Chief Information and Technology Officers at the time were also engaged in spreading the information and link to the questionnaire. As a result, 20 responses to the survey were obtained.

5.1.1. Demographics:

Based on the answers selected by respondents it can be concluded that specialists in information security & risk management, banking & financial institutions, as well as outsourcing & offshoring have provided their input to the survey. The specialists have gained their experience from different backgrounds: consulting companies, offshore service providers and, most importantly, banks. The respondents included inter alia:

- Swiss Bank Global Security Operations specialist with five years of experience;
- Senior Consultants from consulting firms (Deloitte, EY, KPMG) from Poland and Netherlands, all of whom at some stage served security advisory services to European banks, including Swiss banks.
- Senior Consultants from consulting firms (Deloitte, EY, KPMG) that at some stage in their career worked for at least one year with Swiss Bank's vendor
- Managers and Senior Managers who take senior management positions in security departments at European banks, including Swiss banks.
- Managers, Senior Managers and Directors - all of whom had experience of at least two years in a consulting company and at least five years in financial institution.

Inclusion of representatives of different professional backgrounds allowed better objectivity in the questionnaire, as views and opinions could be compared at a question level. While, of course, not all of the responses were uniform and not all of respondents had the same views, no particular dependency of the questions on the background was identified during the course of response analysis. Details are provided when particular sections of the questions are analysed below.

5.2. Practical relevance

In short, the questionnaire confirmed the practical relevance and usefulness of guidelines towards information security management for financial institutions engaged in offshoring. Respondents in their answers reflected on offshoring development, the increased risks in offshoring as well as potential improvements in information security management.

5.2.1. Offshoring development

While the majority of respondents agree that offshoring will continue to develop, their views differ with regards to pace of development – 66% percent (consulting and financial institution representatives) believe offshoring will develop at a faster pace while 33% (all sectors) believe it will develop at lower pace than to date. Their answers were supported with arguments such as increased talent mobility, globalization as well as local talent shortage. Increased talent mobility is the term that covers the movement of talented employees from one country to another but also from non-specialised organisations to more specialised (internal security function versus external teams that provide security services and focus on development of that service solely).

Respondents, who have had experience working at companies that were third party service providers to financial institutions, believe that the development slowdown can occur due to longer transition caused by complex regulatory requirements, technology complexity and focus on process automation. This appears to be a challenge considered at strategic level at those service providing companies, who – to grow – need access to organisations willing to offshore and to build scale – need transitions to be run smoothly.

Automation of processes and robotics were also mentioned by multiple respondents as factors that will potentially decrease the number of processes offshored, therefore reducing the pace of offshoring development. With the development of technology, companies do look into ways to conduct business processes with the use of machine learning and automated tools. Automation and robotics while widely introduced in the manufacturing, is not yet common across business processes – banks are lacking the technology and skill and with such high investment rates and uncertainty around return on investment this is not a preferred way to substitute offshoring at this stage. It is however important to keep that in mind when making offshoring decisions and initiatives. Such state is supported with recent industry reports, such as this one by McKinsey&Company on *The Transformative Power Of Automation in Banking*. (Berutti, Ross, & Weinberg, 2017) While automation was named as a risk for offshoring back in 2014, most recent literature presents views similar to McKinsey & Company.

If we possibly combine the two last notes, however, and focus on automation of transition, perhaps organisations will be able to have the the best of both worlds – offshoring and automation.

Some of the respondents also had the contradictory view – that offshoring will not continue to develop. The answer was justified by one of respondents with a visible trend of internalizing or nearshoring of business processes as a secure balance between associated costs and risk. The respondent explained that nearshoring carries lower risk of operations – less cultural difference and a more controllable environment, while not increasing the costs as much as conducting the processes within the organization. Nearshoring is therefore a balanced solutions that carries both – good and bad sides of both offshore and in-house processes. Another two respondents believe that the development of automation and robotics will be so great that the offshoring will be the less preferred solution for cost cutting.

All representatives agree that offshoring development will be impacted by global economics and politics. The geopolitical situation may impact the state of offshoring with events such as exit of the

United Kingdom from the European Union or changes in European Union – United States of America politics that may hamper or enforce restructure of the current offshoring practice. The economic growth of China and other countries considered to be located offshore can also increase the quality of services provided by those countries and therefore enhance the state of offshoring in terms of share of processes offshored by organisations in Europe. Some answers on this note were: “Politics (for example USA)”, “Political changes on labour in various countries (like USA)”, “Economic factors”, “Development of China, India and other countries”

The role of this research is not to argue with the respondents’ views on the development of offshoring and select the most true scenario, but to identify the different views in order to make the guidelines for financial institutions engaged in offshoring on information security management controls more appropriate i.e. include comparison of costs and return on investment between offshoring a process and automating the process.

5.2.2. Motivation for offshoring

The survey confirmed that the main motivation behind offshoring is cost-efficiency or even cost-reduction driven pressure on organisations. As the organisations, here – financial institutions, seek ways to run their business with lower costs than currently in order to increase growth. Majority of respondents listed cost efficiency as the main factor that motivates organisations to offshore. Cost efficiency was also one of the motivational aspects identified in available academic literature.

Another interesting point of view supporting further development of offshoring was raised by multiple respondents, who believe that processes offshored are higher quality (also in terms of provided information security) as vendor is more controllable than internal resources by contractual clauses or global security standards. This highlights the importance of three aspects when deciding to offshore:

- Verification of vendors’ skills and qualifications (to ensure quality of service), so that the process is, as expected, performed by employees who are skilled and qualified to deliver expected results;
- Contractual clauses compliance assurance, to ensure that the vendor organisation and vendor employees perform given responsibilities in line with the requirements stated in the contract;
- Detailed cost estimation (to ensure cost-efficiency) – including in the analysis, the factual costs of offshoring the process including the high transition costs that are increased.

The observation of case study in this field was rather limited, as the motivation for offshoring is established at a more strategic level and the observation was run on an operational level. However, even during that observation it was noted that indeed - the strategic goals of the organisation were often expressed in amounts to be saved. These goals were then cascaded onto business divisions and managers and finally employees. Also in the questionnaire the respondents mentioned that goals were often expressed in form of targets in reduced costs.

5.2.3. Risks in offshoring

Having confirmed the state of offshoring and its importance to business development for financial institutions, it is also important to identify the risk impacting factors – what causes certain risks and why. It was important for this project, because the most common internal control approach is the risk-based approach. This means that all internal control systems, including information security management system should address particular risks and focus on the ones of highest probability and impact.

Respondents listed the factors leading to the increase in risks associated with offshoring. The following were listed (in order of occurrence): regulatory changes, complex technology (technology in use,

complexity of technology, technology development), changing role of data, employees security awareness, number of vendors, client awareness, public opinion, lack of coordination and governance and senior management support, short product time to market, cost, communication, business complexity, hacking tools automation, threat actors skills developments, specific organization risk profile factors, employee market changes (contractors). We will elaborate on these topics in more detail below.

Regulatory changes

Regulatory changes generate risks of being noncompliant and at times can lead to obligatory termination of offshoring contract (vendor not able to provide services under new regulations) or bringing the business process back into the bank. Many respondents mentioned regulations from outside of Switzerland, such as General Data Protection Regulation issued by European Union due to its applicability to Swiss institutions. The regulations seem even more unrealistic, when an organisation operates and serves customers from various geographical locations with different requirements, definitions and approaches. At the time of the research, the search of academic sources for 'comparison of global data protection regulations' returned no results comparing the requirements, but a few works were found on the conflicting regulations in cyberspace dated as far back as 1999. (Lahaye & Lefebvre, 2017) (Reidenberg, 1999) This is possibly because the matter is rapidly developing and changing (i.e. number of countries including Switzerland are reviewing their regulations and plan to change their regulations in the near future) but also because each organisation will serve a different set of customers and different regulations will apply to each case separately. An example of differences that the case under observation noted was the difference in defining personal information. In Singapore personal identifiable information is the information that by itself or combined with other information that organisation has access to or may have access to allows identification of the individual at stake. In Switzerland, personal identifiable information is any information related to identified or identifiable individual – the regulation does not specify what other information can be taken into account to make information identifiable. This directly relates to anonymization of data: data processed in different processes may be anonymised (instead of using name, last name, personal identification number, the data subject is referred to by customer number) but there is another data within the organisation that has the capability of linking customer number with the name. In Switzerland, information presented per customer number may not be considered personal identifiable information, but in Singapore – it most certainly would. The risk of changing regulatory requirements raised by respondents is therefore even more complex to address for institutions operating globally. This highlights the importance of detailed compliance assessments prior to offshoring decisions but also constant cooperation between compliance departments with information security and transition managers. It is also worth noting that the risk of compliance is not addressed by global standards for information security such as ISO27001.

Complexity of technology environment

Additionally, it is often the case that a business decision process is to be offshored but complexity of information system will hinder successful, timely transition. In some cases complex IT infrastructure, differences in technology in use, use of cloud, lack of information on how data is stored and transfer could lead to more vulnerable offshoring. Complexity in technology may also impact compliance with data protection regulations for example when encryption or masking of confidential data cannot be ensured. Complex IT environments that are not reflected in up to date documentation make it more difficult for companies to determine where information is processed and where exchange of information occurs. This may impact both – compliance with regulatory requirements as well as timely offshoring processes. Complexity of technology environment also impacts other information security controls such as access management – lack of environment granularity may not enable proper

restrictions of user rights resulting in employees having access permissions to more volumes of data than they actually need.

Complex organizational structure

The importance of cooperation between different stakeholders of the process such as compliance departments, procurement departments, information security, IT and finally transition managers has been mentioned throughout this paper. The respondents also identified this risk of various departments being engaged in the process and the dispersion of goals and targets for each of them. Departments that are pressured with short product time to market will aim for quick and complete transition, while information security and compliance departments may slow down the process to ensure no oversight. Complex organizational structure may also mean dispersed business processes meaning the process that was to be offshored requires engagement of more teams and employees in the process understanding phase. Additionally, complex organizational structures may cause communication and responsibility issues, when throughout the course of transition issues arise but unclear responsibility for resolving one is assigned in the organization. During the course of observation it was noted that a number of offshoring program managers were contractors from external companies. Perhaps the turnover of contractors also has an impact on the complexity, but this could not be determined with such limited research. Respondents also mentioned “lack of coordination” for actions taken between different business areas of the organization, which could highlight the difficulties of disperse goals between teams and lack of overarching responsibility for all three areas.

Another note on the organization complexity mentioned by respondents was “changing role of data in the business process”. This implies that the respondents notice the risk that data used for one process can be used in another process causing issues when one of the processes is offshored together with appropriate data access. Also, often the data used in one process changes in scope due to new business requirements or internal business process reengineering exercises. Realistically however, some of the changes cannot be anticipated at the time of transition.

Low employee awareness

The risk arising from differences in security awareness between home institution and vendor staff was also mentioned as a factor impacting offshoring risks and it is another organizational factor. Due to different understanding of requirements and information security approach from the staff that operationally performs the process. The employees of both sides can therefore respond differently to social engineering techniques therefore impacting information security.

As noted during the observation, lack of employee awareness may impact the transition process itself, because employees without proper understanding of the situation may not be willing to share enough details with the transition manager.

This risk can potentially be addressed with improved communication not only of the information security campaign but also the offshoring engagement. Potential issues with vendor employees’ awareness can be addressed with contractual clauses, while the assessment of awareness to assure its alignment with financial institution should be included in the periodic risk assessment framework. As mentioned in the literature review, impact of low awareness on information security, along with other organizational factors and potential steps to improve the awareness have been studied by many researchers and discussed by industry leaders. This proves that the issue of low awareness is not financial industry or geographically specific, like this paper is. While the studies were not conducted in the financial sector specifically, many of them are said to be applicable across various industries.

Number of vendors

Number of vendors is another factor that impacts the offshoring risks and therefore taking this factor into consideration of internal controls may reduce the impact. The larger number of vendors will make the risk assessments, control over alignment with contractual clauses and additional requirements deployment to align with changing regulatory requirements more difficult.

Rising client awareness

Some of the respondents also pointed out that it is client's awareness of information security and protective behaviour, as well as public opinion that can increase potential risks of offshoring. One respondent confirmed that while undoubtedly there occur data breach incidents involving third party vendors, some of them may be caused by inappropriate customer behaviour. The risk of inappropriate user behaviour is rarely taken into account when offshoring – but perhaps it should be considered in order to provide additional internal controls on institution's or vendor's site. Additionally, there is another side to client awareness – clients are more aware of threats and their rights in terms of privacy. This awareness motivates them to request information from organisations on how their personal information is protected, what the security mechanisms are in use to ensure satisfactory protection and with whom information is shared. It seems that while individuals are sharing their information on social media, they may not be as willing to have that information shared by others.

Cybercrime

Development

On top of the above there is also broad cybercrime development, also mentioned by multiple respondents, that increases the risks of offshoring. Not only do the hackers improve their skills, but the technology development also allows automation of hacking tools. Such cybercrime methods progressing will impact the threat landscape of any company, also of a Swiss bank as well as the third party service provider. This is the reason why the company should review their threat profile on the basis of recent cyber incidents and address potential risks in the offshoring relationship.

Respondents confirmed that the probability of cyber attacks exploiting vulnerabilities at vendor's site or in vendor management process are very likely to happen, but they also believe that the success of such attack depends highly on internal controls. Overall success rate of such attacks is considered by respondents to be lower than the risk of cyber attack attempts.

In order to highlight the practical relevance of research focused on internal controls, the respondents were asked to determine what the most probable and most impacting consequences of executed cyber attacks are. The most probable attack would cause some compensation fees for a client or a regulatory body in case of noncompliance. Breach of client identifying information and institution's strategic or financial information is also probable.

Consequences

The problem of information security management in offshoring would not be an issue for financial institutions if lack of information security internal controls did not cause significant implications. Respondents confirmed that the compliance breach and other regulatory fees caused by information leaks can have noticeable impact on institution's operations. GDPR predicts high fees for noncompliant institutions, causing the rise in motivation and awareness among large companies as well as small enterprises.

Disastrous impact on the organization would be caused by interruption of the business operations (lack of ability to serve customers). Breach of financial or strategic information or ransomware related costs would be considered similar to regular expenses in terms of their value. Financial fees,

whether to impacted customers or the regulatory bodies were rated by respondents as noticeable but not impacting regular run of business.

5.2.4. Potential response to aforementioned risks

The first section of the questionnaire allowed establishment of the common ground – that offshoring is an ongoing trend and that it carries information security risks that are also on the rise. Respondents were also asked to voice their opinion whether information security management and system of internal controls could help in minimizing those risks.

All of the responses concluded that internal controls will support addressing risks raised from offshoring. The responses also listed key success factors that are concluded in Information security management subchapter of the questionnaire analysis.

5.2.5. Practical relevance summary

When related to risk categories identified in the academic literature from the previous chapter – we see that the factors impacting risks listed by respondents can also match the risk categories: whether operational, strategic and other. Similarly, these can be divided into identified information security system challenges: human, organizational and technological. It can therefore be concluded that recent experience from the market, regardless of the background, is in line with the literature findings presented in previous chapters.

Knowledge of the factors that hinder potential offshoring risks can be found useful when designing and building information security system, so that the factors can be addressed with adequate attention and result in reduced risk levels.

5.2.6. Information security management

Current state

Given the observation results and the respondents answers, it can be concluded that Swiss financial institutions engaged in international relationships have some information security management practice in place by now.

When asked for examples of current information security management controls at their organization, respondents tend to give generic answers: risk frameworks, internal audits, regularly conducted penetration testing, oversight over portable media usage.

From academic and industry literature we know that risk framework is a methodology that combines risk management processes that cover various areas of risks such as technology risks and information security risks. A consistent framework helps prioritising the risks that are critical to the organisation across those different areas and address them with the right amount of resources.

Internal audits are the periodic checks of effectiveness of introduced controls (although in less mature environments there may not be any controls, and the audit team decides whether there should or should not be any controls on basis of selected methodology, for example – COBIT) conducted by teams from within the structure.

Penetration testing is an exercise known to most technology and information security specialists that focuses on controlled vulnerability exploration and exploitation of computer system with the use of already known exploitation tools. Penetration testing on a computer system is often performed by

ethical hackers – hackers who hack organisations as a service helping them protect their infrastructure from technical risks.

Examples of how oversight over portable media usage can be maintained include limitation of access to use portable media (i.e. workstations with blocked CD drives and USB ports) or monitoring of file flow from workstations to USB ports.

Respondents were more detailed with their answers when they were asked about the biggest challenges.

Challenges

The respondents said that the identified areas that institutions struggle to improve include the contractual clauses design, reluctance to change, low levels of awareness (internally and at vendor’s organization), large number of vendors, vendor’s reluctance to higher security expectations.

Contractual clauses design

The importance of contractual clauses was already highlighted looking at the fact that processes performed by vendors should be performed at higher quality and contractual clauses constitute to one of the ways on how to achieve this.

Complexity in Information systems architecture and in vendor relationships (reflected as a large number of vendors engaged in performing offshore processes) were again mentioned as troublesome in addressing by information security management systems.

These are not the only organizational challenges in information management systems. The one that was raised multiple times across the questionnaire was the engagement of top management.

Scope of protection

For creation of useful and practical guidelines of information security management system, it was important to confirm the potential scope of information currently being protected in financial institutions. This question of the questionnaire aimed at identifying subjects for protection that are not given the attention they require, as per point of view of specialists from different backgrounds.

It was expected, and then confirmed in the questionnaire, that client information is protected most. This is mainly because of potential regulatory fees for noncompliance (if the client or their representative will raise an issue to a responsible regulator) but also because of potential loss of customer base (customer growth reduced due to unfavourable public opinion) and loss of reputation.

The heat map representing all responses from interviewees is presented in the diagram below. It can be easily noticed that security focus is also put on employees’ details, project documentation and product information. Employees’ details can be very sensitive, especially if they contain information on health insurance and family members. On the other hand, project documentation and product information can impact bank’s competitive advantage by giving out internal know-how and intellectual property.

	Minimal attention	Some attention	A lot of attention	Main focus
a) Client information				
b) Strategic information				
c) Products and systems used information				
d) Organizational & architectural charts				
e) Employees’ information				

f) Project documentation

g) Vendors, suppliers and contracts information

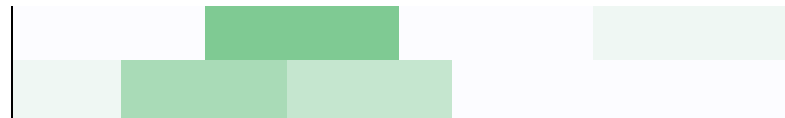


DIAGRAM 1 HEAT MAP SUMMARIZING RESPONDENTS' ANSWER TO THE QUESTION WHAT INFORMATION IS PROTECTED WITH WHAT LEVEL OF ATTENTION AT THE ORGANIZATION?

Responsibilities

The questionnaire asked respondents to reflect whose responsibility is it in the current state to ensure vendor's information security compliance with institution's requirements. The answers were highly divided, but the top three would be the vendor's IT department and information security departments from both parties.

Target state

In order to design applicable guidelines of practical relevance it was important to collect information of the desired, expected state of effective information security management system.

Key success factors

As mentioned before, respondents agreed that an internal controls system can support addressing risks that arise from offshoring (among other risks). Some respondents raised conditions in which the support will reach true results. The controls should be sensible in a way that they should address identified risks rather than assure compliance with the written policy or procedure. Such risks should be frequently reviewed and identified and the controls should be established and in place prior to relationship establishment between the vendor and institution.

Frequent review of vendor's compliance or continuous monitoring conducted by the institution or independent party can also be a crucial part in the controls around offshoring.

Multiple respondents believe that while internal controls can improve the security of offshoring, building awareness of threats and constant education will bring more benefits.

Having summarized the responses to deliver a simple ruleset of a successful internal control system, the following features were raised as the most important:

- Well established and standardized processes
- Clearly assigned responsibilities
- Assigned accountability
- Contractual clauses for different scenarios with specified leakage consequences
- In-depth review of vendor's practices (organization, awareness, mechanisms)
- Risk approach should balance benefits approach
- Top management engagement and commitment
- Understandable data classification

Respondents also claim that regulatory requirements and high noncompliance fees serve as motivation to both parties (institutions and vendors) to provide satisfactory levels of security.

When asked in a structured question – out of the ten suggested key factors, the winner was understandable objectives, supported by top management and reflected in compliance contractual clauses where possible.

Scope of protection

The respondents were also asked to provide answers as to what types of information should be protected with higher level of attention than they are currently. The respondents listed:

- Employees contact details – such as home address, family members, health insurance details; overall perception of the financial institution’s practices indicates imbalance between protection of customer data and customer’s data despite the fact that both groups have similar privacy rights
- Paper documents at branch offices – such as forms populated and signed by clients like written dispositions that can potentially contain sensitive personal and financial data; these are often overlooked in information security initiatives as they focus on IT systems and networks protections against cyber-attacks truth being that physically accessible information is often used in reconnaissance phase of an attack.
- Local payments export files (processed in local systems: SECOM, SIC) – SECOM is the Swiss system for financial assets settlements, SIC is the system for interbanking transactions; given the high levels of system security the files imported and exported from the system are often stored in directories or locations of decreased security.
- Big data sets – with large volume of data being processed it increases the risk of re-linking anonymized data records therefore compromising one of the protection methods.
- Technology development strategy and plans – although not protected by regulations, the information about strategic development of technology – whether it is acquisition of a system, migration or even upgrade can be found very important to potential fraudsters giving information of what systems are currently in use, what are the data structures or what are the current versions of underlying architecture. Such information provides hints about commonly known vulnerabilities.
- Web-facing applications and interfaces – currently all of the banks provide financial services online – through a web interface accessible publicly. These are usually well protected as they provide access to the client’s information. Banks however manage a large number of websites other than the main banking or transaction systems that are put aside in information security management initiatives.
- Use of cloud services – increasing user’s comfort and ease of use, but also impairing information security these tools are usually used by employees unaware of information security threats. Usage of such systems could occur at both ends: the financial institution and the vendor.
- Know-how and intellectual property – this information is usually valued because of competitive advantage i.e. certain tools or methods can be used to address particular financial problems. Know-how and intellectual property are very difficult to protect from internal threats – employees, present and past, sharing their knowledge with colleagues from competing companies or with new employer.
- Technology used for data sharing and data storage – information that may not seem critical to financial institution employees, may be crucial for cyber attackers. One of the respondents noted that it still happens that IT teams will seek answers to their issues online, often asking questions from their corporate e-mail associated accounts. Knowing the technology allows attackers identify vulnerabilities of the technology in use and exploit it in the attack vector.
- Audit findings – as they can contain crucial information on process-based or system configuration vulnerabilities, that similarly to the information on technology in use, can be helpful to conduct a successful cyberattack.

It was noted that the discrepancies between what is protected and what should be protected are the result of a lack of impact analysis or breach of certain data categories followed by adjustment of the security focus to the analyzed impact. The ideal information security management system should therefore repeatedly assess impact of data breach of data categories processed by the bank.

Such analysis will require the bank to first identify the data categories processed, identify the systems where and how the data is processed as well as data flows and finally assess probability and impact of data breach for each category. This approach will help the bank in addressing weak points in data processing, identify previously unprotected (or not protected enough) data and provide better protection for information that is critical not only to customers but also the company itself. The same issue was identified by European Union regulators who, by introduction of GDPR that requires organizations processing personal data to be able to identify processes, systems, flows and vendors that have any touch points with the data at stake.

It is important to note that while vendor representatives also voted that information security focus is put on customer data – the definition of customer data for third party vendor may be much broader than for a financial institution.

Responsibilities

When looking at current and preferred by customers assignment of responsibilities, minimal difference can be observed. The core of responsibility should still remain between vendor's IT department and information security departments in both fields. However, we did point out before that dispersion of responsibilities across departments in offshoring should be limited as it increases the associated information security risks. Higher engagement is however expected from vendor's legal department and from financial institution's PMO teams.

5.2.7. Conclusion

A large part of the questionnaire answers were in line with situations observed during the case study participatory observation, which means that despite different backgrounds the respondents identify similar challenges and risks that relate to compliance, security and offshoring in financial institutions. Taking into account all the insights and viewpoints of the respondents, the factors that impact the efficiency of internal controls, that are believed to play a great part in assurance of compliance and security, have been drawn. They are presented in the final chapter of this research below.

Chapter 6 - Summary & discussion

6.1. Summary

In this research we have analysed available academic research, industry reports as well as conducted empirical research in order to deliver a set of factors of information security controls that will reduce information security risk associated with offshoring. In order to present in short how this research reaches its conclusions, the initial research questions will be answered first.

The initial core concept relationship diagram is presented again below in order to bring back to light the focus of this research. In this research, we have discussed information security risks that arise from offshoring and may lead to data breach, information security challenges that are generated by these risks and data protection regulations. All of this has been done with the focus on financial institutions that seem to address the risks and challenges with information security management systems.

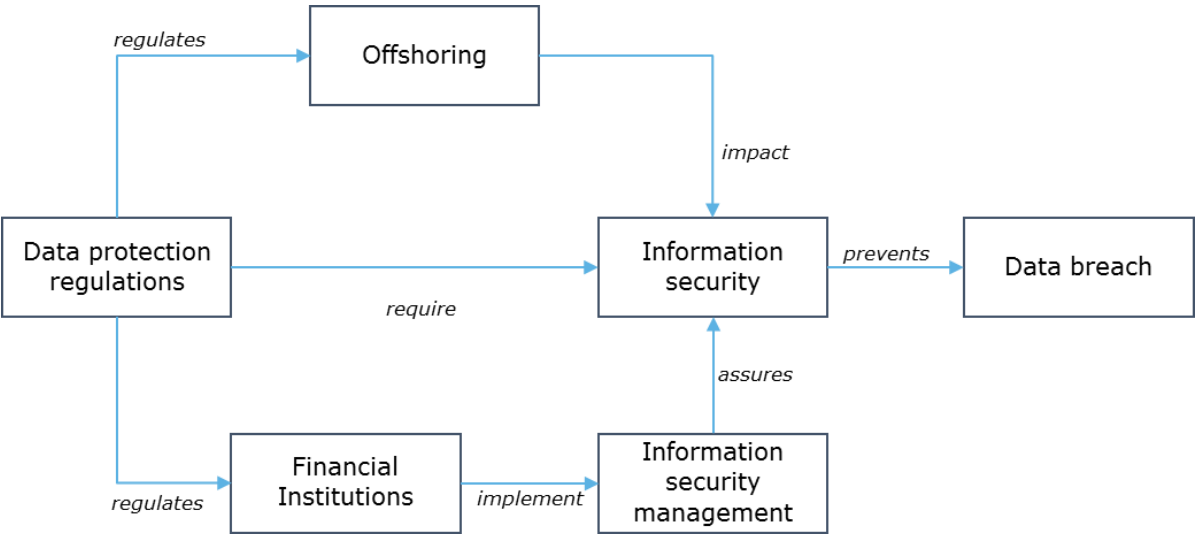


Figure 5 Core concepts and their relationship

Literature review brought more detail to these diagrams by introducing offshoring risk factors carried by organization, technology, stages of offshoring and different offshoring models. It also explained what offshoring risks can lead to (cyber attacks and internal threats), what consequences may be faced by financial institutions in case a risk is materialised (financial loss, reputational loss, noncompliance fees) and finally that it is not only regulations but also public expectations towards individuals' privacy that pose big requirements on financial institutions and their information security practice.

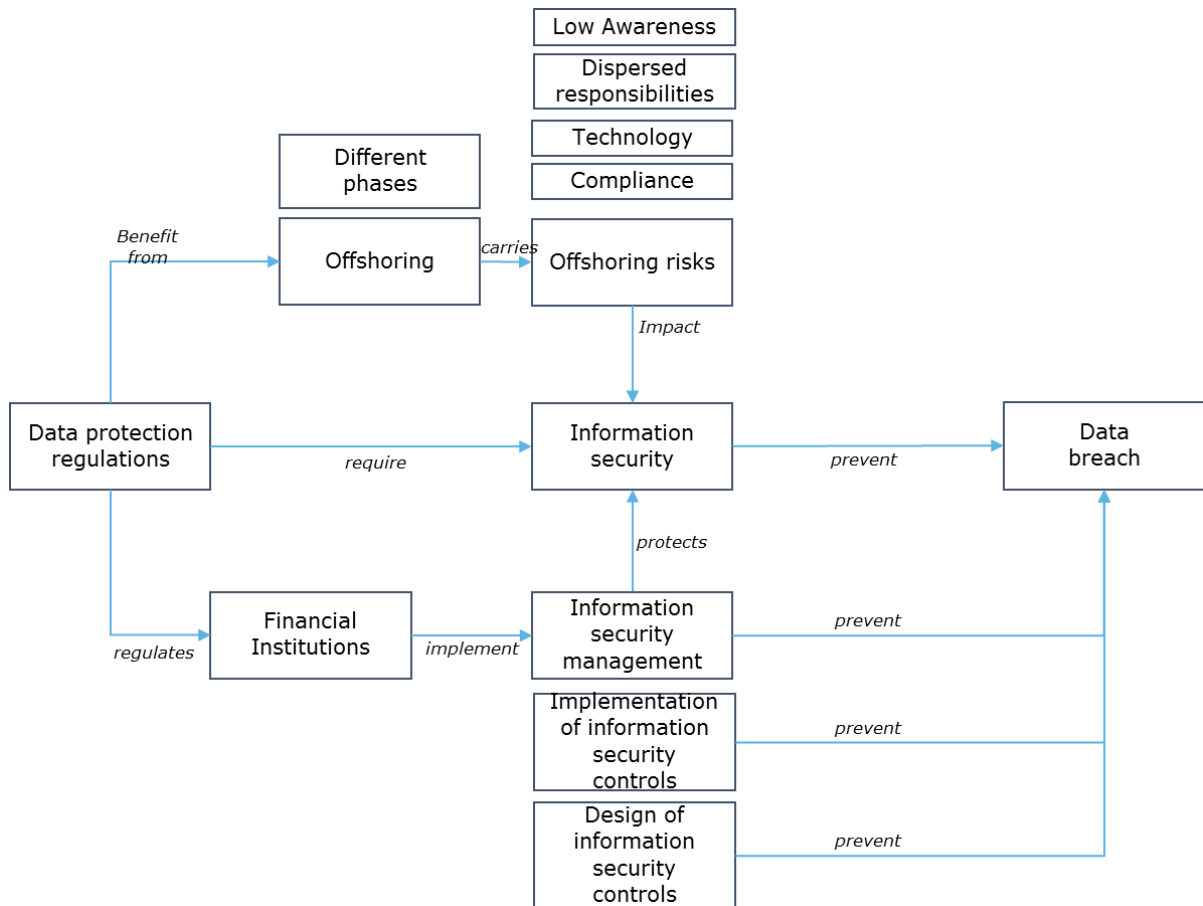
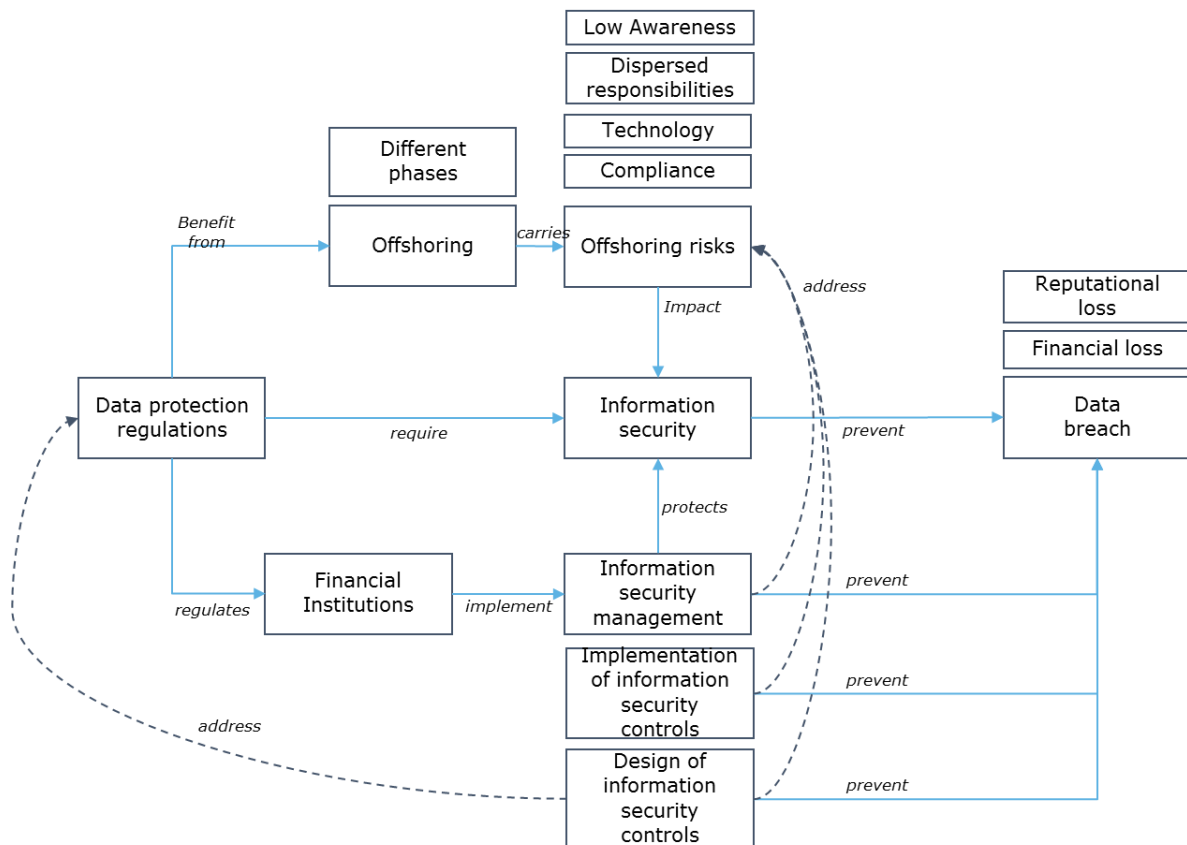


FIGURE 6 CONCEPT RELATIONSHIP REVISED

Having conducted the observation and analysis of questionnaire, even more detail can be brought to this diagram by showing what factors can improve information security management and therefore assure information security and, in consequence, reduce potential losses.



As per questionnaire results, information security controls are believed to have a true impact on information security risks, including risks faced by financial institutions engaged in offshoring.

6.1.1. What information security related risks do the Swiss financial institutions face when offshoring?

The risks that Swiss financial institutions face do not seem different from risks faced by other organisations. While strategic goal of financial institution is to grow, it can easily be seen that growth may be impacted by reputation or financial loss (among a broad spectrum of other factors). Reputation or financial loss may be caused by data leak that will cause compliance fees or reimbursement costs to the victims of data leak. Data leak can be caused by internal threats (sharing information on purpose), lack of employee awareness (unthoughtful upload of data to external network) and cyber attacks (including social engineering). These risks are the same for organisations that are engaged or not engaged in offshoring. However, if we look one level down: internal threat is increased as now data is available to employees and vendor employees. Lack of employee awareness can also occur on both sides – the organisation’s and the vendor’s. Finally, having the information spread across different organisations also broadens the surface that can potentially be attacked.

The requirements with regards to how to conduct offshoring engagements securely are rather limited. Literature review, observation and questionnaire all showed that there are much more requirements towards banks with regards to financial stability and reliability and only a small portion of the requirements addresses the risks of offshoring and information security (these are usually related). Swiss institutions that offer goods and services to EU citizens need to be compliant with General Data Protection Regulation as of 25th of May 2018. GDPR imposes three key requirements in terms of offshoring: (1) no responsibility can be passed over to service provider, (2) data may only be transferred to Secure Countries as assessed by European Commission, (3) data subjects must be aware and express consent of who (what other parties) will be processing their data. At the time of this

research Switzerland was considered a secure country, but India wasn't. For countries not listed as secure by European Commission, the processor should ensure other data protection mechanisms.

Other than that, Switzerland is currently in the process of reviewing its Data Protection Act that requires to ensure protection of privacy if data is transferred abroad, similarly to GDPR lists countries that are considered secure enough for data to be transferred but also clarifies, that even data processed in Switzerland and accessed from abroad is considered 'transferred'. At the time of research India was not on the country list.

6.1.2. What challenges do Swiss financial institutions face when implementing and maintaining the information security controls?

As per questionnaire results, information security controls are believed to have a true impact on information security risks, including risks faced by financial institutions engaged in offshoring. However, also per questionnaire results, it was noted that there are numerous challenges that financial institutions face in the process of design and implementation of controls.

This research has allowed identification of challenges and obstacles that come to surface when information security management controls are introduced or modified. These challenges include:

- multiple stakeholders – when setting requirements for the vendor and transition process itself, it is often difficult to manage the expectations and risks due to large number of actors in the process with each one taking partial responsibility for overall completion but also for their own goals (timing, budget, security, compliance);
- number of vendors – complex business environments with large number of service providers are considered by interviewees as challenges to deploy decent standard of information security across all data processed by the organisation and therefore its service providers;
- employees' reluctance to change – often employees, even senior management employees find the security requirements and configuration settings as disrupting the business or stopping growth and therefore are reluctant to change their behaviour on top of natural human reluctance to change;
- low awareness within the organisation – often employees do not realize what risks the organization and therefore the employees as well are facing and what errors may lead to data breach or what attack vectors the attacker may use in order to obtain confidential information; and
- control over vendor's behaviour and practices – setting requirements detailed enough for the vendor to leave little room for interpretation but also feasible for vendor to implement.

None of the respondents have mentioned time or budget to be a challenge when trying to provide information security in offshoring, but these two aspects were frequently mentioned by transition managers during case study observation. These challenges can definitely impact the efficiency of information security controls.

6.1.3. How to design information security controls that will contribute to information security risk (probability and impact) reduction in case of a Swiss financial institutions engaged in offshoring?

The summary below will provide the lessons as provided by the respondents and case study observation. Both can serve as guidance for the design of internal controls in vendor management. Detailed presentation of the insights gathered throughout this research divided into phases of vendor management process is attached in Appendix II.

All interviewees agreed in the questionnaire that efficient information security controls can have major impact on information security of the organization and therefore reduce information security risks in offshoring. Respondents' views on information security controls are following:

- Provide structure and baseline – the controls specify what processes and mechanisms should be in place and operating effectively to address identified risks;
- Provide instructions how to behave and act for employees – in most cases controls are well described and description includes information what risks is being addressed providing further explanation to employees with regards to what the mechanism or process serves;
- Ensure new systems, processes and relationships are designed to ensure security – a lot of controls have impact on security of entire system, for example: a control that states that every project should be assigned an information security risk specialist in order to identify and address the risks will reduce any risks associated with projects, regardless of the area the project is conducted within.

Having confirmed how the information security controls can reduce information security risks, it became clear during the research that if controls can overcome challenges of control design and implementation, they should reduce the information security risks even further i.e. more effectively .

General information security management system success factors

These factors seem to be generalizable for control implementation outside of offshoring process, and possibly also outside of the financial sector.

Organization

Throughout the research it was noted that in order for organisation to implement efficient controls they should be risk focused, include clear definition of responsibilities and be supported by senior management. Controls that do not address the risk may cause overinvestments while not bringing expected results, because they will not be addressing the risks that the organization faces. Additionally, lack of clearly assigned responsibilities showed in both phases of the research – observation and questionnaire, when it was noted that information security controls are often inefficient because there is not one team or employee that is held accountable. Finally, respondents clearly raised the issue of lack of support of top management for information security controls and limited communication of the events, both of which are believed to hinder the effectiveness of controls.

Focus of protection

Another surprising finding was that often some information assets are protected extremely well, to the point they may be considered over-invested, while others are not in the security focus at all, while our respondents believe they should be.

Success factors for financial institutions engaged in offshoring

The factors listed below relate to information security in offshoring specifically. Throughout the observation and analysis of questionnaires it became clear that preparation for offshoring can significantly reduce the risk of information security breach in go-live or post go-live phase of the process. A number of identified risks was due to lack of sufficient information gathered before the offshoring initiative. Additionally, unexpectedly, our respondents noted that often post-contract processes are not given enough resources to ensure that all vulnerabilities have been cleaned up. The third key conclusion relates to contracts. Especially when new processes are outsourced to the same vendor, often a template of a contract is used. Throughout the research it became clear that each information security control and requirement should be specifically defined in the contract requirements and agreed between the two sides of transaction. These three generic observations

would be the key points that should be taken into account when next planning information security management system controls for offshoring processes. At this high level of conclusion, these observations can be generalizable to other institutions and sectors, where information of various confidentiality levels is processed.

External research

A group of success factors identified during the course of this research can be concluded as detailed preparation and research. It was observed and then confirmed by the questionnaire that some time and cost issues, as well as information security efficiency issues arise during the process of offshoring because they have not been investigated and studied in enough detail prior to offshoring. We noted that while political and economic factors research will address not only information security challenges but also the broader problem of offshore centre locations, there are other aspects to be researched to address possible information security risks. These include upcoming regulatory changes (regulations that are under discussion or review) and compliance requirements and restrictions posed on specific service or location.

Internal research

Although study of external environment often takes place, even if in its most generic form, there is a lot of information that is available within the organisation, that may help with offshoring planning and more accurate risk identification. We already know that correct risk identification will lead to more efficient controls, therefore any additional piece of information may be very valuable to the process. It was noted that the planning phase should include steps such as identification of relevant IT assets and data sets that are used and processed in the process. That information may be further used to identify automation opportunities and ensure cost-efficiency (address the risk of large data volumes being processed for example). When discussing automation opportunities, blockchain technology should not be left out of consideration as with its high information security levels it may provide enough confidence to automate processes without impacting data integrity or confidentiality and therefore maintaining satisfactory compliance.

Vendor research

Another area to investigate is the vendor. Often it is very important to investigate in more detail than checking compliance against international standard, as no international standard or policy will ensure cultural and technology alignment with the main organization. It was noted that sometimes qualification of vendor employees does not match the standard of the company and this can be with contractual clauses requiring specific certificates to be granted to team members. Additionally, there is another a process that often takes place in process of mergers and acquisition, but is only seldom in offshoring and that could help addressing information security risks. By conducting due diligence discrepancies between technologies can be identified and either addressed before transferring the process or mitigated with additional layer of solutions.

Merged results

With information resulting from internal, external and vendor research, more detailed risks and even threat landscape can be determined this will help establishing whether the risks still outweigh the benefits of offshoring the particular process. More detailed risks can lead to more suitable controls and security mechanisms. Having identified potential issues and risks, it becomes easier to design controls that when in operation will prevent these risks from materialising. The next group of success factors shows how to ensure that controls are implemented.

Documentation

Although documentation usually just addresses the design of controls without reassuring implementation, not to mention successful and efficient implementation, documentation for offshoring can ensure successful implementation. We should consider documentation as a set of contractual clauses and low level information security requirements that the vendor will need to oblige by, but also by supporting documentation such as incident response planning. It was noted during the observation that while incident response plans and other similar procedures were carefully designed for the post-transition phase (when process is established at vendor's site) they often did not address issues related to the transition itself.

Organisation

It was already noted in the literature review that organisational factors can impact information security significantly. This should also be a part of overall planning and consideration when preparing the process to offshore. Overall top management support and communication have already been mentioned at the start of this summary, but there are other organisational aspects that can be addressed beforehand as well, for example: avoiding complete reliance on vendors and ensuring that the full time employee is engaged in the project and aware of risks and implemented controls. Additionally, the loyalty and engagement of the team should be ensured to a possible extent whether by internal contractual clauses or project preceding surveys and interviews with employees. Planning for organisational changes will address issues with unexpected turnover of staff.

Final steps

Finally, there are also factors that will help in achieving efficiency of controls that can be considered post transition phase. It is especially important that each process is analysed separately but also in conjunction with already outsourced processes in order to protect home organization from losing confidentiality over process know-how. Also, while companies tend to perform regular risk assessments it is important to point out that they should also work on improvement and review of the risk assessment methodology itself, by reviewing and updating risks and then testing controls against these risks.

The above should cover the information security management system controls on a generic level throughout the entire process of offshoring, but it is worth pointing out that both the observation and the questionnaire highlighted the importance of clean-up processes when the relationship with the vendor is terminated. As mentioned, the detailed description of all factors identified during this research is presented in Appendix II. These factors, as described in detail, will not necessarily be applicable to other institutions or sectors.

6.2. Conclusion

Before stepping into conclusion of the academic relevance of this research, let us conclude the considerations for transition managers or offshoring information security managers that come from the factors listed above.

The overall message for decision-making parties at Swiss financial institutions that engage in offshoring should be that information security management is a process that should be present across all phases of offshoring, from planning and decision to the final contract termination. While the go-live transition carries the most information security risks, these can be avoided by in depth planning and preparations. Preparations should also challenge the decision by investigating the data and technology at stake – preferably not only from the existing policies requirements but also from emerging threats and overall risk perspective.

The above considerations can be planned ahead in the timeframe and budget of the initiative. Additionally, some of the controls may be conducted continuously – such as verification of political, geopolitical and economic situations regardless of the current offshoring stage. For managers who wish to improve efficiency of the information security controls in offshoring it is advised to take the above factors into account.

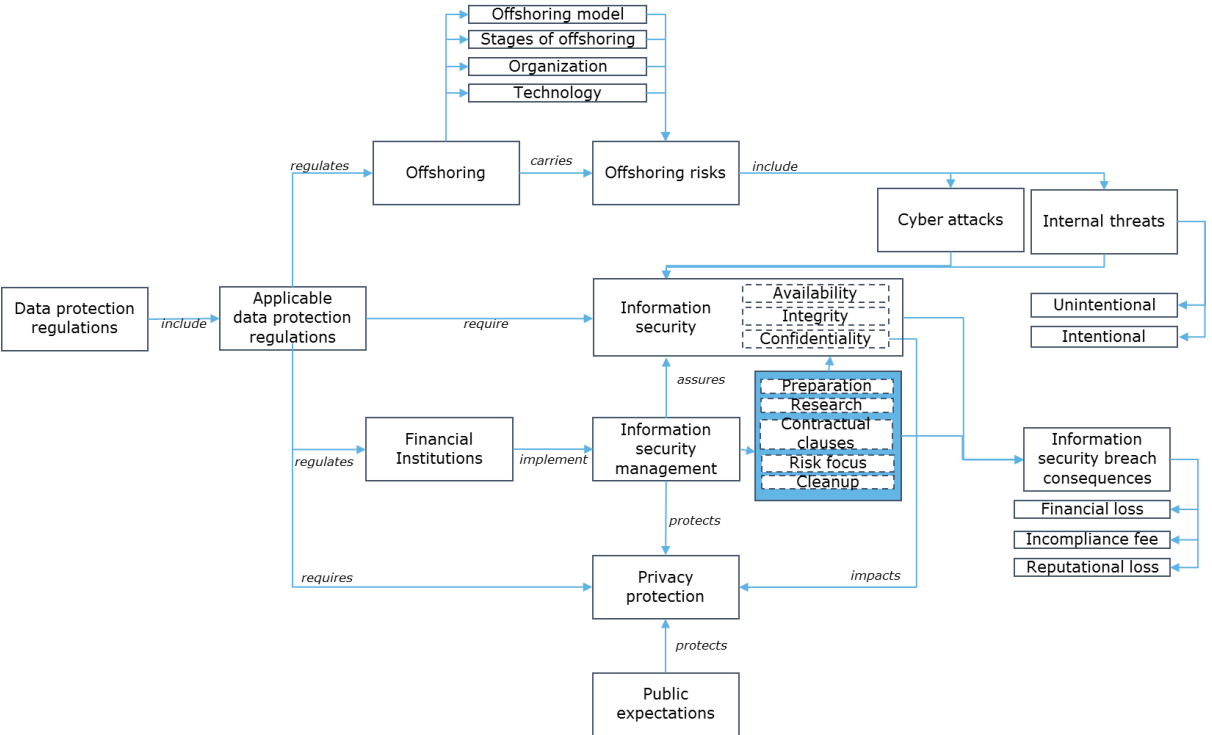
6.3. Academic relevance

The literature review in Chapter 2 presents a detailed analysis of literature review that supports the importance of this thesis to academia. The scope of this research is limited to information security in financial institutions that offshore their processes, because even though the concept is that specific the problem at stake still remains complex.

This research adds to the academic research by focusing on a specific industry and presenting it in the light of different requirements, existing processes and emerging threats. It presents information from case study observation of a large international financial institution – a view that is not often represented in research. Case study observations are also supported with knowledge and experience in the sector of specialists in offshoring, information security and financial institutions.

From Management of Technology perspective, this research provides more insights to project management by introducing the focus and important aspects of offshoring initiative management. Additionally it also tackles the challenges of international trade of services such as information security or regulatory compliance – consideration of which should be highlighted.

Now to structure how the answers to research questions adhere to the previously presented concept diagrams the below, very generic block was added to the revised diagram.



The diagram should also help understanding the practical and academic relevance of this research as they are described in separate paragraphs below.

6.4. Practical relevance

As for practical relevance of this research – as stated throughout the text – despite numerous industry publications on information security as well as presence of international standards on information security, no research supported study has been published to address challenges that offshoring financial institutions face. The summary of the factors relevant for an information security management system was prepared for financial institutions to be able to identify room for improvement in their well established and long operating information security management systems.

No currently available standards cover such level of detail regarding recommendation of proposed responsibilities that should be assigned, such as responsibility or an overarching body for information security, compliance and offshoring.

Also, this research gathers multiple views, and those views are not limited to narrow perspectives. This research shows the links of offshoring information security with other areas of process management such as automation and robotics, organisational culture and awareness building.

6.5. Rigor of research

The data collection that was designed on literature review and context study involved case study observation and mixed question questionnaire distributed among experts in the field of offshoring, financial institutions and information security. This allowed assessing the current state of the art of protecting information in offshoring by financial institutions but also exploring the views of experts on potential changes and increasing risks in order to assure practical relevance of this research. Different perspectives allowed identification of a full range of phenomenon of interest, but as this phenomenon is complex and consists of many concept relations, each of them could possibly be studied in more detail. The methods however allowed identification of answers to research questions.

Mixed method collection also allowed identifying relevant and salient themes – as the questionnaire was designed on the basis of the concepts already observed in the observation phase and the answers were also analysed by the person who had been involved in the observation (myself). Additionally, atlas.ti was used to analyse qualitative data coming from the questionnaires. The research questions defined at the beginning of this research framed this research in a way, that no other aspects of the context were subject to analysis. However, the overview and support of academic researchers – prof. Harry Bouwman and Dr Albert Plugge – has helped with framing this research and ensuring the identification of guidelines was not superfluous.

6.6. Limitations

It is important to note the limitations of this research. The research scope was very specific and narrow in terms of specialisation. It focused on the small part where three big concepts (information security, financial institution and offshoring) overlap. Therefore the academic literature available on this particular topic was highly limited. Contrary the topic was explored by industry in various reports.

This research is based on a single case study observation – a highly differentiated case study within certain geographical locations and specific scope of services. The observation of the case study also carried some limitations as some information in the global operating organization is strategically confidential but also the size of organization did not allow for identification of all controls in place and engagement with all stakeholders engaged in offshoring.

The questionnaire also faced some challenges such as the previously discussed low response.

All of these could be improved with a more in depth observation of different parts of the offshoring process and with less time restrictions on the data collection phase of the research.

6.7. Reflection

The market is seeking ways to improve their internal control systems alongside the technical protection in order to respond to growing cyber risks and regulatory requirements. This was the base assumption of this research, confirmation of which assures the practical relevance.

The subject of this research is very specific, not only does it tackle the area where three major research topics overlap, but it was also limited in terms of geographical location and specific relationship (financial institution - offshore vendor). The literature available on such a narrow topic is highly limited and this relates to academic literature as well as industry reports – which shows the uniqueness of this research in academia. During the course of research it became clear that no research yet has put enough of a detailed analysis on that space where offshoring, financial institutions and information security overlap, which is why the topic serves as a very interesting but also challenging basis for further research.

We learned that while there are standards related to information security, the international standards set a baseline that is not the same for every industry, in every country as all organisations have different profiles. There is room for a more specific analysis and results. Another interesting point that came to light during the course of this research is that while offshoring does increase the risks, for some of the respondents these risks are easier to manage as it is easier to control vendor performance with contract clauses and Service Level Agreements rather than the organisation's own environment.

With regards to future research implications – this research showed that while there is no one size fits all information security system management, there are certain obstacles and enhancers that occur across financial industry. Ideally, the next step would be to measure impact of each of these measures on efficiency of information security management system or focus on particular issue to establish how this obstacle can be addressed and the enhancer improved to obtain higher security levels in offshoring relationships.

Points of improvement could also be noted on the research methodology. It was noted during this research, that the views of respondents varied for some questions. The sample of respondents was too small to determine any scientific conclusions on this note. It would suggest that (a) more time should be allowed for gathering interviewee's responses and (2) timeframe when asking for respondent's views and predictions about the state of the future should be defined in future research.

Works Cited

- Accenture. (2015). *Accenture Technology Vision 2015: Digital Business Era: Stretch your boundaries*. Accenture.
- Aksin, O. Z., & Masini, A. (2008). Effective Strategies for Internal outsourcing and offshoring of business services: an empirical investigation. *Journal of Operation Management*, 239-256.
- Aleksandrova, D. (2014, December 23). *Rising external threats and regulations - top challenges for CISOs*. Retrieved from IT Governance: <http://www.itgovernance.co.uk/blog/rising-external-threats-and-regulations-top-challenges-for-cisos/>
- AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, 567-575.
- Alsaif, M., Aljaafari, N., & Khan, A. R. (2015). Information Security Management in Saudi Arabian Organizations. *Procedia Computer Science* (pp. 213-216). Elsevier.
- Amant, K. (2007). International outsourcing, personal data, and cyber terrorism: Approaches for oversight. *Cyber Warfare and Cyber Terrorism*, 112-119.
- Andress, J. (2014). Chapter 1: What is information security? In J. Andress, *The Basics of Information Security* (pp. 1-22). Oxford: Elsevier.
- Aron, R., Clemons, E. K., & Reddi, S. (2005). Just Right Outsourcing: Understanding and Managing Risk. *Journal of Management Information Systems*, 37-55.
- Ashended, D. (2008). Information Security management: A human challenge? *Information Security Technical Report*, 195-201.
- Atallah, M., Pantazopoulos, K. R., & Spafford, E. (2002). Secure outsourcing of scientific computations. *Advances in Computers*.
- Babin, R., & Nicholson, B. (2012). Corporate social responsibility in global IT outsourcing: A case study of inter-firm collaboration. *Pacific Asia Conference on Information Systems*. PACIS.
- BAKBASEL. (2014). *The economic significance of the Swiss financial sector - study on behalf of the Swiss Bankers Association SBA and the Swiss Insurance Association SIA*. BAK Basel Economics AG.
- Baldwin, L., Irani, Z., & Love, P. (2001). Outsourcing information systems: drawing lessons from a banking case study. *European Journal of Information Systems*, 15-24.
- Ball, K. (2010). Data protection in the outsourced call centre: an exploratory case study. *Human Resource Management Journal*, 294-310.
- Barako, D. (2008). Outsourcing practices of the Kenyan banking sector. *African Journal of Accounting, Economics, Finance and Banking Research*, 37-50.
- Bataev, A. (2015). Economic efficiency estimation for automated banking systems outsourcing. *Actual Problems of Economics*.
- BBC. (2015, May 26). *Number of identity theft victims 'rises by a third'* - BBC News. Retrieved from BBC News: <http://www.bbc.com/news/uk-32890979>

- Berutti, F., Ross, E., & Weinberg, A. (2017, November). *McKinsey & Company*. Retrieved from McKinsey & Company | Financial Services: <https://www.mckinsey.com/industries/financial-services/our-insights/the-transformative-power-of-automation-in-banking>
- Beutler, A. (2008). *Offshoring of Business Processes by Banks from Switzerland*. Diplomica Verlag GmbH.
- Birman, K. P. (2000). The Next-Generation Internet: Unsafe at Any Speed? 33(8).
- Boehm, F. (2015). A Comparison between US and EU data protection legislation for law enforcement. Brussels.
- Bott, J., & Milkau, U. (2015). Outsourcing risk: A separate operational risk category? *Journal of Operational Risk*.
- Box, D., & Pottas, D. (2013). Improving information security behaviour in the healthcare context. *Procedia Technology*, 1093-1103.
- Box, D., & Pottas, D. (2014). A model for information security compliant behaviour in the healthcare context. *Procedia Technology*, 1462-1470.
- Bygrave, L. A. (2014). *DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE*. Oxford: OUP.
- Colwill, C. (2006). Outsourcing: the Security Risk Management Challenge. *Proceedings of 4th Australian Information Security Management Conference*. Perth: Edith Cowan University.
- Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review*, 243-256.
- De Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, 162-176.
- Deloitte. (2014). *2014 Global Outsourcing and Insourcing Survey results*. Deloitte.
- Deloitte. (2016). *Deloitte's 2016 Global Outsourcing Survey*. : Deloitte Development LLC.
- Deloitte Development LCC. (2012). *Outsourcing, Today and tomorrow*. Deloitte Development LCC.
- DeWalt, K. M. (2002). *Participant observation : a guide for fieldworkers*. Walnut Creek: AltaMira Press.
- Dhillon, G., Syed, R., & Sa-Soares, F. d. (2016). Information security concerns in IT outsourcing: identifying (in) congruence between clients and vendors. *Information & Management*.
- Dinu, A.-M. (2015). The risks and benefits of outsourcing. *Knowledge Horizons. Economics.*, 103-104.
- Dolnicar, S., & Jordaan, Y. (2006). Protecting Consumer Privacy in the Company's Best Interest. *Australasian Marketing Journal*, 39-61.
- Drinkwater, D. (2014, June 20). *Bank bosses finally get the memo on cyber security - SC Magazine UK*. Retrieved from SC Magazine UK: <http://www.scmagazineuk.com/bank-bosses-finally-get-the-memo-on-cyber-security/article/356853/>
- Du, Y. (2014). Research on the information security of internet bank. *Applied Mechanics and Materials*, 1925-1929.

- Earp, J. B., & Payton, F. C. (2006). Information Privacy in the Service Sector: An Exploratory Study of Health Care and Banking Professionals. *Journal of Organizational Computing and Electronic Commerce*, 105-122.
- Ee, O., Abdul Halim, H., & Ramayah, T. (2013). The effects of partnership quality on business process outsourcing success in Malasia: Key users perspective. *Service Business*, 227-253.
- Eloff, J., & Eloff, M. (2003). Information Security Management - A New Paradigm. *IT research in developing countries: proceedings of SAICSIT 2003* (p. 130136). Pretoria: SAICSIT.
- Enoch, C., & Segoviano, M. (2014). *Switzerland: Financial System Stability Assessment*. International Monetary Fund.
- Ernst&Young. (2014). *Get ahead of cybercrime - EY's Global Information Security Survey 2014*. EYGM Limited.
- Fenn, C., Shooter, R., & Allan, K. (2002). IT Security outsourcing: how safe is your IT security? *Computer Law & Security Review*, 109-111.
- Fersht, P., & Snowdon, J. (2013). *State of the outsourcing industry 2013: Executive Findings*. Boston: HFS Research.
- Fragoso-Diaz, G. (2015). Perceptions of doing business in other countries: A logistic regression analysis of survey results. *International Journal of Supply Chain Management*, 52-62.
- Franke, J., & Wullenweber, K. (2006). The Impact of potential flexibility gains and losses on the intention to outsource business processes. *Proceedings of the 14th European Conference on Information Systems*. ECIS.
- Gabzhalilov, A. (2016, March 21). *The Market Mogul*. Retrieved from Outsourcing and Offshoring: <http://themarketmogul.com/outsourcing-offshoring/>
- Gellings, C., & Wuellenweber, K. (2007). Differences in Contracting: Anchoring Formal and Relational Norms within BPO Governance. *AMCIS 2007 Proceedings*. Association for Information Systems.
- Gewald, H., & Dibbern, J. (2009). Risks and benefits of business process outsourcing: A study of transaction services in the German banking industry. *Information & Management*, 249-257.
- Ghodeswar, B., & Vaidyanathan, J. (2008). Business process outsourcing: an approach to gain access to world-class capabilities. *Business Process Management Journal*, 23-38.
- Gonzalez, R., Llopis, J., & Gasco, J. (2013). Information technology outsourcing in financial services. *The Service Industries Journal*, 909-924.
- Goodman, S. E., & Ramer, R. (2007). Global Sourcing of IT Services and Information Security: Prudence before Playing. *Communications of the Association for Information Systems*, 812-823.
- Gorla, N. (2014). The impact of IT outsourcing on information systems success. *Information & Management*, 320-335.
- Gorla, N., & Lau, M. B. (2010). Will negative experiences impact future IT outsourcing? *Journal of Computer Information Systems*, 91-101.

- Graeff, T. R., & Harmon, S. (2002). Collecting and using personal data: consumers' awareness and concerns. *Journal of Consumer Marketing*, 302-318.
- Graham, R. (1996). Outsourcing - The Major Legal Issues. *Information Security Technical Report*, 51-56.
- Grant Thornton. (2014). *Outsourcing: Driving efficiency and growth*. Grant Thornton International Business Report.
- Gupta, M., Ganguli, S., & Ponnampalani, A. (2015). *Factors affecting employee engagement in India: A study on offshoring of financial services*.
- Harangus, D. (2010). Banking industry in Digital Economy. *Proceedings of the 33rd International Convention*. MIPRO.
- Harker, P. (2012). *The Service Productivity and Quality Challenge*. Springer.
- Hathaway, O., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The Law of Cyber-Attack. *California Law Review*, Vol. 100, No.4, 817-885.
- Herath, T., & Kishore, R. (2009). Offshore Outsourcing: Risks, Challenges and Potential Solutions. *Information Systems Management*, 312-326.
- Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer Fear of Online Identity Theft: Scale Development and Validation. *Journal of Interactive Marketing*, 1-19.
- Hung, P., Chiu, D., Fung, W., Cheung, W., Wong, R., Choi, S., . . . Pun, J. C. (2005). Towards end-to-end privacy control in the outsourcing of marketing activities: A web service integration solution. *ACM International Conference Proceeding Series* (pp. 454 - 461). Scopus.
- Hung, P., Chiu, D., Fung, W., Cheung, W., Wong, R., Choi, S., . . . Pun, J. C. (2007). End-to-end privacy control in service outsourcing of human intensive processes: A multi-layered Web service integration approach. *Information Systems Frontiers*.
- Iqbal, Z., & Munir Dad, A. (2013). Outsourcing: A Review of Trends, Winners & Losers and Future Directions. *International Journal of Business and Social Science*, 91-107.
- Jie, H. (2008). Privacy in Internet Age—Comparison on internet privacy regulations between the United States and the European Union and its indication to internet privacy protection of China.
- Jimmy Gandhi, S., Sauser, B., & Gorod, A. (2012). Prioritization of outsourcing risks from a systemic perspective. *Strategic Outsourcing: An International Journal*.
- Jo, H., Kim, S., & Won, D. (2010). A Study on Comparative Analysis of the Information Security Management Systems. *Computational Science and Its Applications - ICCSA 2010* (pp. 510 - 519). Fukuoka: Springer.
- Johnson, J., & Lincke, S. (2014). A Comparison of International Information. *Interdisciplinary Journal of Information, Knowledge, and Management*, 89-116.
- Johnson, M. E., Goetz, E., & Pflieger, S. L. (2009). Security through Information Risk Management. *IEEE Security & Privacy*, 45-52.
- Jonsson, N., Moeller, O., & Lillieskold, J. (2007). Reasons for not Offshoring IT Services in Swedish Banks. *PICMET 2007 Proceedings* (pp. 1451-1455). Portland: PICMET.

- Kakabadse, A., & Kakabadse, N. (2005). Outsourcing: Current and Future Trends. *Thunderbird International Business Review*, 183-204.
- Kalakota, R., & Robinson, M. (2004). Offshore Outsourcing Business Models. In R. Kalakota, & M. Robinson, *Offshore outsourcing: Business Models, ROI and Best Practices* (pp. 23-48). Alpharetta: Mivar Press. Retrieved from Newsletter: <http://www.sterlinghoffman.com/newsletter/articles/article107.html#>
- Kalakota, R., & Robinson, M. (no date available). *Emerging Business Models in Offshore Outsourcing*. Retrieved from Newsletter: <http://www.sterlinghoffman.com/newsletter/articles/article107.html#>
- Kazmierczyk, J., & Macholak, P. (2014). Outsourcing in the Banking Sector (The Polish Banking Sector Case). *The IAFOR Journal of Politics, Economics and Law*.
- Kim, Y.-S., Lee, G., Shin, Y., Choi, Y., Park, J.-H., & Kim, J.-B. (2016). A Study on Control Item of ISMS in the Financial Industry. *International Journal of Security and its Application*, 123-134.
- Koech, L. C., Minja, D., Koyier, D., & Wachira, M. (2016). An assessment of factors affecting the performance of outsourced ATM service among commercial banks in Kenya. *Journal of Strategic Management*, 1-20.
- Kolah, A. (2015, February 27). *Urgent Action Is Required as Data Breaches hit Record Highs | Digital Marketing Magazine*. Retrieved from Digital Marketing Magazine: <http://digitalmarketingmagazine.co.uk/digital-marketing-data/urgent-action-is-required-as-data-breaches-hit-record-highs/1611>
- Krugman, P., & Wells, R. (2006). *Macroeconomics*. New York: Worth Publishers.
- Kull, A. (2011). Regulatory compliance to ensure information security: Financial supervision perspective. *10th European Conference on Information Warfare and Security 2011* (pp. 298-306). ECIW.
- Kumar, R. (2014). Cases on Universal Banking. In R. Kumar, *Strategies of Banks and Other Financial Institutions: Theories and Cases* (pp. 275 - 336). Elsevier.
- Kumar, R. (2014). Regulatory Environment of Financial Institutions. In R. Kumar, *Strategies of Banks and Other Financial Institutions: Theories and Cases* (pp. 31-60). Elsevier.
- Kumar, R. (2014). Strategies and Structures of Financial Institutions. In R. Kumar, *Strategies of Banks and Other Financial Institutions: Theories and Cases* (pp. 3-30). Elsevier.
- Lacity, M., & Willcocks, L. (2009). *The Practice of Outsourcing: From Information Systems to BPO and Offshoring*. Springer.
- Lahaye, C., & Lefebvre, P. (2017). EU Data Protection and the Conflict of Laws: The Usual "Bag of Tricks" or a Fight Against the Evasion of the Law? *Defense Counsel Journal*.
- Lainhart, J., & Ballister, C. M. (2016, May 12). *FCW*. Retrieved from Achieving holistic cybersecurity: <https://fcw.com/articles/2016/05/12/comment-holistic-cybersecurity.aspx>
- Leavitt, N. (2007, December 17). The Changing World of Outsourcing. *Computer*, pp. 13-16.
- Leavy, B. (2004). Outsourcing strategies: opportunities and risks. *Strategy & Leadership*, 20-25.

- LeBlanc, G., & Nguyen, N. (1988). Customers' Perceptions of Service Quality in Financial Institutions. *International Journal of Bank Marketing*, 7-18.
- LeBlanc, G., & Nguyen, N. (1996). Cues used by customers evaluating corporate image in service firms. *International Journal of Service Industry Management*, 44-56.
- Lewin, A. Y., & Peeters, C. (2006). Offshoring Work: Business Hype or the Onset of Fundamental Transformation? *Long Range Planning*, 221-239.
- Liang, H., Wang, J.-J., Xue, Y., & Cui, X. (2016). IT outsourcing research from 1992 to 2013: A literature review based on main path analysis. *Information & Management*, 227-251.
- Lin, N., Devinney, T. M., & Holcomb, T. R. (2016). Examining Managerial Preferences and Choices: The Role of Value Creation and Value Appropriation Drivers in Strategic Outsourcing. *Long Range Planning*, 706-722.
- MacKerron, G., Kumar, M., Benedikt, A., & Kumar, V. (2015). Performance management of suppliers in outsourcing project: Case analysis from the financial services industry. *Production planning and control*, 150-165.
- Madura, J. (2014). Role of Financial Markets and Institutions. In J. Madura, *Financial Markets and Institutions* (pp. 3-29). Stamford: Cengage Learning.
- Mahmoodzadeh, E., Jalalinia, S., & Yazdi, F. (2009). A business process outsourcing framework based on business process management and knowledge management. *Business Process Management Journal*, 845-864.
- Martin, S. (2014, November 10). *Banks to Spend \$8bn Upgrading Cybersecurity and IT Protection Over the Next 6 Years*. Retrieved from International Business Times UK: <http://www.ibtimes.co.uk/banks-spend-8bn-upgrading-cybersecurity-it-protection-over-next-6-years-1474073>
- Maughan, A., Wugmeister, M., & Titus, D. (2006, November 6). *Outsourcing to India: Dealing With Data Theft and Misuse*. Retrieved from Computerworld: <http://www.computerworld.com/article/2547959/it-management/outsourcing-to-india--dealing-with-data-theft-and-misuse.html>
- McLellan, K., & Beamish, P. (1994). The New Frontier for Information Technology Outsourcing: International Banking. *European Management Journal*, 210-215.
- McNeal, G. S. (2014, May 26). *Banks Challenged By Cybersecurity Threats, State Regulators Acting - Forbes*. Retrieved from Forbes: <http://www.forbes.com/sites/gregorymcneal/2014/05/26/banks-challenged-by-cybersecurity-threats-state-regulators-acting/>
- Mehta, A., Armenakis, A., Mehta, N., & Irani, F. (2006). Challenges and opportunities of business process outsourcing in India. *Journal of Labor Research*, 323-338.
- Merriam, S. B. (1998). *Qualitative Research and Case Study Applications In Education*. Jossey-Bass Publisher.
- Mukherjee, D., Gaur, A. S., & Datta, A. (2013). Creating value through offshore outsourcing: An integrative framework. *Journal of International Management*, 377-389.
- Mullin, R. (1996). Managing the outsourced enterprise. *Journal of Business Strategy*, 28-36.

- Nassimbeni, G., Sartor, M., & Dus, D. (2012). Security risks in service offshoring and outsourcing. *Industrial Management & Data Systems*, 405-440.
- Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management*, 123-134.
- Northcutt, S. (n.d.). *Security Controls*. Retrieved from SANS Technology Institute: <https://www.sans.edu/cyber-research/security-laboratory/article/security-controls>
- Ochri, I., Kotlarsky, J., & Willocks, L. P. (2013). *Advances in Global Sourcing - Models, Governance and Relationships*. London: Springer.
- Office of Data Protection Commissioner. (n.d.). *EU Directive 95-46-EC - Chapter 1*. Retrieved June 14, 2015, from Data Protection Commissioner - Ireland: <https://www.dataprotection.ie/docs/EU-Directive-95-46-EC-Chapter-1/92.htm>
- Oliver Wyman. (2015). *Managing complexity: the state of the financial services industry 2015*. Oliver Wyman.
- Oshri, I. (2011). *Offshoring Strategies: Evolving Captive Center Models*. MIT Press.
- Penter, K., Wreford, J., Pervan, G., & Davidson, F. (2013). Offshore BPO decisions and institutional influence on senior managers. Lecture Notes in Business Information processing.
- Ponemon Institute LLC. (2014). *2014 Cost of Data Breach Study: Global Analysis*. Traverse City: Ponemon Institute LLC.
- Professional Outsourcing Resources. (2014, June 6). *Professional Outsourcing Resources*. (Purple Cow Media) Retrieved October 19, 2014, from Banks to outsource back office?: <http://professionaloutsourcingmagazine.net/newsitems/banks-to-outsource-back-office>
- PwC. (2013, September). *Dodd-Frank Regulation S-ID SEC CFTC: PwC*. Retrieved from PwC: Audit and assurance, consulting and tax services: <http://www.pwc.com/us/en/financial-services/regulatory-services/publications/identity-theft-regulation.jhtml>
- PwC. (2014). *Financial Services sector analysis of PwC's 2014 Global Economic Crime Survey*. PwC.
- Ramingwong, S., & Sajeev, A. (2007). Offshore outsourcing: the risk of keeping mum. *Communications of the ACM*, 101-103.
- Reidenberg, J. (1999). Resolving Conflicting International Data Privacy. Fordham.
- Reisinger, D. (2015, February 12). *In shift, hackers want your identity, not just your credit card - CNET*. Retrieved from CNET: <http://www.cnet.com/news/in-shift-hackers-want-your-identity-not-just-your-credit-card/>
- Rickert, P. (2015, April 16). *Ten challenges to a successful future for Swiss private banks - Blog*. Retrieved from KPMG Switzerland Blog - Insights from our experts: <http://blog.kpmg.ch/ten-challenges-to-a-successful-future-for-swiss-private-banks/>
- Roses, L., Hoppen, N., Ballaz, B., & De Mello Freire, K. (2006). Quality evaluation in information systems outsourcing. *Information Systems and Collaboration: State of the Art and Perspectives - Best Papers of the 11th International Conference of the Association Information and Management* (pp. 268-280). AIM.

- Ruiter, J., & Warnier, M. (2011). Privacy Regulations for Cloud Computing: Compliance and Implementation in Theory and Practice. *Computers, Privacy and Data Protection: an Element of Choice*, 361-376.
- Sahgal, R., & Malhotra, V. (2005). Moving offshore: Key challenges and the importance of quality standards. *Making a difference: the impact of powerful research CONGRESS* (pp. 274-287). Amsterdam: ESOMAR.
- Savitz, E., & Toubba, K. (2011, June 6). *Forbes*. Retrieved from The Cybercrime Boom: It's A Good Time To Be A Hacker: <http://www.forbes.com/sites/ciocentral/2011/11/06/the-cybercrime-boom-its-a-good-time-to-be-a-hacker/>
- Saxena, K., & Bharadwaj, S. (2009). Managing Business process through outsourcing: A strategic partnering perspective. *Business Process Management Journal*, 687-715.
- Sharma, A., & Loh, P. (2009). Emerging Trends in Sourcing of business services. *Business Process Management Journal*, 149-165.
- Silva, T. C., Guerra, S. M., Tabak, B. M., & de Castro Miranda, R. C. (2016). Financial networks, bank efficiency and risk-taking. *Journal of Financial Stability*, 247-257.
- Skadden, Arps, State, Meagher & Flom LLP & Affiliates. (2014). *Outsourcing by Financial Services Companies: Impact of the OCC and FRB guidelines*. New York: Skadden.
- Sparrow, E. (2004). *A Guide to Global Sourcing*. Swindon: BCS.
- Strong, B., Cater-Steel, A., & Lane, M. (2014). Prudential risk management of IT sourcing strategies: A case study of an Australian bank. *20th Americas Conference on Information Systems*. AMCIS.
- Suryanarayan, M., & Sabyasachi, D. (2013). Information Technology Outsourcing Risks in Banks: A Study of Perception in the Indian banking industry. *Vilakshan: The XIMB Journal of Management*, 61-72.
- Swartz, N. (2004). Offshoring Privacy. *Information Management Journal*, 24-26.
- Swiss Bankers Association. (2018, May). *SwissBanking - Facts & Figures*. Retrieved from Swissbanking: http://www.swissbanking.org/en/facts_figures.htm
- Symantec. (2016). *Internet Security Threat Report Vol.21*.
- Tan, D. R. (1999). Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and European Union . *21 Loy. L.A. Int'l & Comp. L. Rev.* 661.
- Tas, J., & Sunder, S. (2004). Financial services business process outsourcing. *Communications of the ACM*, 50-52.
- Tayauova, G. (2012). Advantages and disadvantages of outsourcing: analysis of outsourcing practices of Kazakhstan banks. *Procedia - Social and Behavioral Sciences*, 188-195.
- TechNavio. (2016). *Global Back Office Outsourcing Market in the Financial Services Sector 2016-2020*. TechNavio.
- TechNavio. (2016). *Global Document Outsourcing Market 2016 - 2020*.
- TechNavio. (2016). *GLOBAL OUTSOURCING MARKET IN BFSI SECTOR 2016-2020*. TechNavio.

- Tovino, S. (2017). *The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons*. Las Vegas, Nevada, USA.
- Vaxevainou, A., & Konstantopoulos, N. (2014). Basic Principles the Philosophy of Outsourcing. *Procedia - Social and Behavioral Sciences* (pp. 567 - 571). Madrid, Spain: Procedia.
- Verizon. (2014). *2014 Data Breach Investigations Report*. Verizon.
- von Rosing, M., Doucet, G., Jansson, G. O., von Scheel, G., Soffel, F., Bach, B., . . . Waters, J. (2015). Business Process Outsourcing. In H. v.-W. Mark von Rosing, *The Complete Business Process Handbook* (pp. 657-670). Elsevier.
- von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, 371-376.
- von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers&Security*, 97-102.
- Walder Wyss. (2015, June 14). *dataprotection.ch - Walder Wyss Ltd*. Retrieved from Walder Wyss Ltd.: <http://www.dataprotection.ch/en/legal-framework.asp>
- Wenge, O., Lampe, U., Muller, A., & Schaarschmidt, R. (2014). Data privacy in cloud computing - An empritical study in financial industry. *20th Americas Conference on Information Systems*. AMCIS.
- Werlinger, R., Hawkey, K., & Beznosov, K. (2008). An Integrated view of human, organizational and technological challenges of IT security management. *17*(1).
- Willcocks, L. (2014, December 4). *Professional Outsourcing Resources*. Retrieved from Professional Outsourcing Resources: Digital Dilemmas: Six Challenges For Outsourcing: <http://www.professionalloutsourcingmagazine.net/insight/digital-dilemmas-six-challenges-for-outsourcing>
- Wong, R. (2013). *Data Security Breaches and Privacy in EU*. London: Springer.
- Wu, L., & Park, D. (2009). Dynamic outsourcing through process modularization. *Business Process Management Journal*, 225-244.
- Wu, Y., Lau, T., Atkin, D. J., & Lin, C. (2011). A comparative study of online privacy regulations in the U.S. and China. *Telecommunications Policy*, 603-616.
- Yépez, A., & Dixon, D. (2016, January 21). *RSA Conference*. Retrieved from Cybercrime and Threats are growing in 2016: <https://www.rsaconference.com/blogs/cybercrime-and-threats-are-growing-in-2016>

Appendix I: Questionnaire – questions and answers summary

1.1 Online version



Information security in offshoring

Introduction

Dear All,

The increasing number of cyber-attacks give sleepless nights to many. Public opinion and regulators require more information protection than ever, while hacking tools continue to develop and spread rapidly. The issue becomes more complex if one looks at the extensive vendor networks that are the result of outsourcing and offshoring development that took place over last decades. Increasing cyber risks can have huge impact on relationships between organizations and their vendors also limiting the cost-cutting capabilities. However, little is known on what is actually done in this domain, therefore professor Harry Bouwman and TUDelft, a renowned Technical University in the Netherlands, have started an explorative research focused on investigating good practices and guidelines for design and implementation of internal control system that will reduce the risks of cyber-crime (data breach in particular) affecting financial institutions engaged in offshoring. The aim therefore is to identify features and focus of internal controls that will address the information security risks identified in offshoring, while being efficient in implementation.

Following in-depth literature review, we would like to contrast the gathered information with real-life views and opinions. We believe gathering information from different sources where the difference comes from employment background, employment experience and specialization. This is where on behalf of TUDelft I would like to ask you for information you have gained throughout your experience.

The data gathered in this questionnaire is to serve as supporting information for definition of guidelines that can be used when designing and implementing internal controls that will address information security management system gaps in terms of information security risks in offshoring relationship. The questionnaire should not take more than 15 minutes, although it does consist of 28 questions. You will find some open questions and where free text is allowed, I would like to encourage you to provide all details you feel comfortable sharing.

Upon completion of this research, you have the option to be informed of its results and receive summary of the final results. Please select corresponding answer at the end of the questionnaire.

Once again, thank you for your time.

If you are interested in conducting an interview, rather than populating the questionnaire, please contact me at a.m.lecka@tudelft.nl.

Also, at any time you can close the survey and return to answering at your convenient time.

Next

Powered by  Survey
Create unlimited online surveys for free



Information security in offshoring

Background data

First Name (optional)

Last Name (optional)

Country (optional)

Experience (specialization)

- Information security & risk management Outsourcing & offshoring Banking & financial institutions

Experience (sector):

- Banking & financial institution Consulting Offshore service provider

[Previous](#)

[Next](#)

Powered by Zoho Survey

Create unlimited online surveys for free

Information security in offshoring

Offshoring

First section of the questionnaire serves introductory purposes for increased understanding of the background and context of the answers in further parts of the questionnaire.

Offshoring should be understood as a long term relationship between main location of the company and an external vendor located in a remote location based on a contract obliging the vendor to perform and manage transferred business processes or corporate activities on behalf of the company and for the company.

1. Having seen the definition of offshoring, I would like to know what you think of future developments. Do you believe, that offshoring will continue to develop?

- a) Yes, even at faster pace.
 - b) Yes, but at slower pace.
 - c) No, because of information security risks
 - d) No, because... (provide your reasons)
 - e) I don't feel comfortable answering this question.
-

Provide your reasons or additional comments:

2. Please, define the order of the following aspects of development starting with the development that has the most impact on offshoring development to the one with the least impact?

- Technology development
 - Cyber-crime development
 - Data protection regulations development
-

Other developments that have impacted growth in offshoring:

Comments:

3. What advancements in particular do you believe have increased the risks of information security in offshoring relationships?

Let us now think about how financial institutions respond to current state of offshoring and information security risks.

4. Is the budget for offshoring at financial institutions increasing (at your organization), stable or decreasing compared to previous year?


- a) Increasing
- b) Decreasing
- c) More-or-less stable

5. What is the target in savings to be reached by offshoring more processes?

6. Do you know any data protection regulations that are applicable to financial institutions in Switzerland? Please list the ones you are aware of.

[Previous](#)

[Next](#)

Powered by  **SurveyMonkey**
Create unlimited online surveys for free

Information security in offshoring

Data protection and information security

As we have covered the current state of offshoring and its context I would like you to help me investigate what is the current state of data protection and information security. We stay focused on a Swiss financial institution offshoring their business processes to India.

Data protection should be understood a set of regulations, laws, standards and best practices that relate to personal data gathering and processing.

Information security is a concept much wider than data protection, less regulated and its importance is delivered because of potential strategic impact, rather than public expectation of privacy.

7. What is the focus on protection for the given types of information at your organization (the organization you have consulted)?



	Minimal attention	Some attention	A lot of attention	Main focus
a) Client information	1	2	3	4
b) Strategic information	1	2	3	4
c) Products and systems used information	1	2	3	4
d) Organizational & architectural charts	1	2	3	4
e) Employees' information	1	2	3	4
f) Project documentation	1	2	3	4
g) Vendors, suppliers and contracts information	1	2	3	4

8. What kind of information does your organization or the organization you have consulted NOT protect while you believe it should?

9. Despite the large focus that financial organizations put into information security and data protection, hackers do not waste time and develop their skills continuously. Did you hear about any cyber-attacks that affected financial institutions (preferably in Switzerland) in the past year? Please list those that you are aware of.

10. How high would you rate the probability information security incident caused by vendor or vendor management process vulnerabilities occurring at your organization?

	1 - Unlikely	2 - Low	3 - Most likely	4 - Almost certain
Unsuccessful	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Successful	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

11. Please rate the probability and the impact associated with the following potential results of cyber attacks:

	Probability	Impact
a) Disruption of business (lack of ability to serve clients)	<input type="text"/>	<input type="text"/>
b) Disruption of business (lack of ability to perform operational tasks) ...	<input type="text"/>	<input type="text"/>
c) Data breach of financial institutions' strategic and financial data	<input type="text"/>	<input type="text"/>
d) Data breach of client identifying data	<input type="text"/>	<input type="text"/>
e) Financial payments required to decrypt hacked data	<input type="text"/>	<input type="text"/>
f) Financial payments to cover non-compliance fees	<input type="text"/>	<input type="text"/>
g) Financial reimbursements to data breach victims	<input type="text"/>	<input type="text"/>

Previous
Next

Powered by **FormSurvey**
 Create unlimited online surveys for free

Information security in offshoring

Information security management

12. Put in order the most common (most probable) reactions of financial institutions to increasing number of cyber attacks?

- a) Organizational changes
 - b) Investments (consulting companies)
 - c) Investments (IT solutions, technology)
 - d) Investments (new employees)
-

Other & Comment:

13a. Please rank the numbers next to departments from 1 (in largest part) to 8 (in smallest part) whose responsibility it is to assure satisfying vendor's information security levels:

- Vendor - Legal department
- Vendor - IT department
- Vendor - Information security department
- Vendor - Customer relations
- Financial institution - Legal department
- Financial institution - IT department
- Financial institution - Information security
- Financial institution - Risk management
- Financial institution - PMO team
- Financial institution - Procurement
- Financial institution - Contract owner

Comment:


13b. Please rank the numbers next to departments from 1 (in largest part) to 8 (in smallest part) whose responsibility it should be to assure satisfying vendor's information security levels:

- ▼ Vendor - Legal department
- ▼ Vendor - IT department
- ▼ Vendor - Information security department
- ▼ Vendor - Customer relations
- ▼ Financial institution - Legal department
- ▼ Financial institution - IT department
- ▼ Financial institution - Information security
- ▼ Financial institution - Risk management
- ▼ Financial institution - PMO team
- ▼ Financial institution - Procurement
- ▼ Financial institution - Contract owner

Comment:

[Previous](#)


[Next](#)

Powered by  **SurveyMonkey**
Create unlimited online surveys for free

Information security in offshoring

Information security internal control system

14. What are the examples of internal controls (implemented reactive or preventive processes) addressing information security issues in offshoring and / or vendor management established at your organization? If you are answering from vendor's perspective: what are the examples of client's requirements addressing information security issues in offshoring?

15. What are the key features of a successful (strong, followed and obliged, established, efficient) information security management system in relation to offshoring and vendor related information security risks? 

	Insignificant	Little important	Important	Critical
Supported by top management	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Documented	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Documented in a well-structured documentation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Distributed to all parties	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Needs to cover all information assets	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Well and repeatedly communicated	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Reviewed regularly	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Present generally understandable objectives	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Where possible, compliance should be required by contractual clauses	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Consistent with other organizational communication	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Other factors:


16. What budget is your organization willing to spend on increasing information security?

17. Is the budget growing from year to year?

- a) Increasing
- b) Decreasing
- c) More-or-less remains stable

Previous

Next

Powered by  Survey
Create unlimited online surveys for free




Information security in offshoring

Data protection in offshoring

18. What phase of offshoring relate to the biggest information security risk? Please rank the following:

- Decision to outsource
- Selection of the business process to be outsourced
- Selection of the vendor
- Transition preparations
- Transition
- Go-live
- Vendor management

19. Given the timeline of outsourcing transition process below (and in the hint view - click on question mark next to this question), please mark the moments where risk assessment(s) should take place (take places) 

	Decision to outsource	Selection of business process to be outsourced	Selection of the vendor	Transition preparations	Transition	Go-live	Vendor management
Risk assessment phase:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>


20. The timeline (phases) above was created on basis of literature review and personal experiences. It may not reflect the process that you are familiar too with or the one established at your organization. Would you modify the timeline to reflect the process at your organization more realistically?

21. What are the key elements of an outsourcing risk management process before engaging in a relationship and afterwards?

22. What are the most applicable information security challenges that financial institutions face when offshoring:

	No occurrence	Some occurrence	A lot of occurrence	Notorious occurrence
a) Vendor's information security management system	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
b) Vendor's organizational culture towards information security	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
c) Vendor's attitude	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
d) Lack of effective vendor assessment possibilities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
e) Lack of vendor's competences	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
f) Lack of supporting technology	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
g) Systems / IT architecture difficult to manage and control	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
h) Large number of vendors	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
i) Lack of personnel awareness at financial institution	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
j) Lack of personnel awareness at vendor's location	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
k) Overall unwillingness towards change in the organizational culture	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
l) Unstructured relationship between financial institution and vendor	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
m) Lack of or vague information security clauses in contracts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
n) Well established relationship with additional requirements being difficult to impose	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

[Previous](#)
[Next](#)

Powered by  Survey
 Create unlimited online surveys for free

Information security in offshoring

Last page

23. On a scale of 1 to 4 please rate the level of information security awareness across employees in financial institutions?



Would you say it needs improvement?

- Yes, it needs improvement
 - No, the level of awareness is satisfactory and does not need improvement
-

24. On a scale of 1 to 4 please rate the level of information security awareness across employees at vendor's organizations in India?



Would you say it needs improvement?

- Yes, it needs improvement
 - No, the level of awareness is satisfactory and does not need improvement
-

25. Do you believe that if the number of offshore vendors increases the more efforts should be put into maintaining the information security level?

- Yes
 - No
-

The final questions relate to your personal experiences in designing and implementing internal controls or other mechanisms that aimed at increasing information security in offshoring relationships.


26. What is needed to make offshoring more secure in terms of protecting sensitive information?

27. Can internal controls reduce the information security risk in offshoring relationships?

Thank you for the time and thought you have put into this survey. Please do leave your e-mail contact if you would like to receive information on the survey results.

If you have any questions do not hesitate to contact me at a.m.lecka@tudelft.nl

[Previous](#) [Submit](#)

Powered by  Survey
Create unlimited online surveys for free

1.2 Offline version

Dear All,

The increasing number of cyber-attacks give sleepless nights to many. Public opinion and regulators require more information protection than ever, while hacking tools continue to develop and spread rapidly. The issue becomes more complex if one looks at the extensive vendor networks that are the result of outsourcing and offshoring development that took place over last decades. Increasing cyber risks can have huge impact on relationships between organizations and their vendors also limiting the cost-cutting capabilities. However, little is known on what is actually done in this domain, therefore professor Harry Bouwman and TUDelft, a renowned Technical University in the Netherlands, have started an explorative research focused on investigating good practices and guidelines for design and implementation of internal control system that will reduce the risks of cyber-crime (data breach in particular) affecting financial institutions engaged in offshoring. The focus therefore is to identify features and focus of internal controls that will address the information security risks identified in offshoring, while being efficient in implementation.

Following in-depth literature review, we would like to contrast the gathered information with real-life views and opinions. We believe gathering information from different sources where the difference comes from employment background, employment experience and specialization. This is where on behalf of TUDelft I would like to encourage you to provide all details you feel comfortable sharing.

The data gathered in this questionnaire is to serve as supporting information for definition of guidelines that can be used when designing and implementing internal controls that will address information security management system gaps in terms of information security risks in offshoring relationship. The questionnaire should not take more than 15 minutes, although it does consist of 28 questions. You will find some open questions and where free text is allowed, I would like to encourage you to provide all details you feel comfortable sharing.

Upon completion of this research, you have the option to be informed of its results and receive summary of the final results. Please select corresponding answer at the end of the questionnaire.

Once again, thank you for your time.

If you are interested in conducting an interview, rather than populating the questionnaire, please contact me at a.m.lecka@tudelft.nl.

Also, at any time you can close the survey and return to answering at your convenient time.

1.3 Questionnaire

Name and last name (optional):

Experience specialization (select all that apply):

- Information security & risk management
- Outsourcing
- Banking

Experience sector (select all that apply):

- Financial institution
- Consulting
- Offshore services provider

Offshoring:

First section of the questionnaire serves introductory purposes for increased understanding of the background and context of the answers in further parts of the questionnaire.

Offshoring should be understood as a long term relationship between main location of the company and an external vendor located in a remote location based on a contract obliging the vendor to perform and manage transferred business processes or corporate activities on behalf of the company and for the company.

1. Having seen the definition of offshoring, I would like to know what you think of future developments. Do you believe, that offshoring will continue to develop?
 - a) Yes, even at faster pace.
 - b) Yes, but at slower pace.
 - c) No, because of information security risks
 - d) No, because... (provide your reasons)
 - e) I don't feel comfortable answering this question.
2. Please, define the order of the following aspects of development starting with the development that has the most impact on offshoring development to the one with the least impact?

Please put in the number next to the listed aspect: 1 – most impact, 4 – least impact

Technology development

Cyber-crime development

Data protection regulations development

Other (please add)

Comment (optional):

.....
.....
.....

3. What advancements in particular do you believe have increased the risks of information security in offshoring relationships?

.....
.....
.....
.....

Let us now think about how financial institutions respond to current state of offshoring and information security risks.

4. Is the budget for offshoring at financial institutions increasing (at your organization), stable or decreasing compared to previous year? With what % is the budget in- or decreasing?

- a) Increasing (% change)
- b) Decreasing..... (% change)
- c) More-or-less stable

5. What is the target in savings to be reached by offshoring more processes?

.....

6. Do you know any data protection regulations that are applicable to financial institutions in Switzerland? Please list the ones you are aware of:

.....
.....
.....
.....

Data protection and information security:

As we have covered the current state of offshoring and its context I would like you to help me investigate what is the current state of data protection and information security. We stay focused on a Swiss financial institution offshoring their business processes to India.

Data protection should be understood a set of regulations, laws, standards and best practices that relate to personal data gathering and processing.

Information security is a concept much wider than data protection, less regulated and its importance is delivered because of potential strategic impact, rather than public expectation of privacy.

7. What is the focus on protection for the given types of information at your organization (the organization you have consulted)?

Select (one) level of attention given to information security for the given types of information.

Minimal attention
Some attention
A lot of attention
Main focus

- d) Client information
- e) Strategic information
- f) Products and systems used information
- g) Organizational & architectural charts
- h) Employees' information
- i) Project documentation
- j) Vendors, suppliers and contracts information

8. What kind of information does your organization or the organization you have consulted NOT protect while you believe it should?

.....

9. Despite the large focus that financial organizations put into information security and data protection, hackers do not waste time and develop their skills continuously. Did you hear about any cyber-attacks that affected financial institutions (preferably in Switzerland) in the past year? Please list those that you are aware of.

.....

.....

.....

.....

10. How high would you rate the probability information security incident caused by vendor or vendor management process vulnerabilities occurring at your organization?

1 – Unlikely 2 - Low 3 – Most likely 4 – Almost certain

Unsuccessful

Successful

11. Please rate the probability and the impact associated with the following potential results of cyber attacks:

Use the following probability rating:

1 – Unlikely 2 - Low 3 – Most likely 4 – Almost certain

Use the following impact rating:

1 – Insignificant 2 - Noticeable 3 – Regular 4 – Disastrous

	Probability	Impact
a) Disruption of business (lack of ability to serve clients) ...		
b) Disruption of business (lack of ability to perform operational tasks) ...		
c) Data breach of financial institutions' strategic and financial data ...		
d) Data breach of client identifying data		
e) Financial payments required to decrypt hacked data		
f) Financial payments to cover incompliance fees		
g) Financial reimbursements to data breach victims		

Information security management:

12. Put in order the most common (most probable) reactions of financial institutions to increasing number of cyber attacks?

- Organizational changes
- Investments (consulting companies)
- Investments (IT solutions, technology)
- Investments (new employees)
- Other:

13. Please rank the numbers next to departments from 1 (in largest part) to 8 (in smallest part) whose responsibility it is and whose responsibility it should be to assure satisfying vendor's information security levels:

It is

It should be

Vendor

Legal

IT
Information security
Customer relations
(other)
.....

Financial institution

Legal
IT
Information security
Risk management
PMO
Procurement
(other)
.....

14. What are the examples of internal controls (implemented reactive or preventive processes) addressing information security issues in offshoring and / or vendor management established at your organization? If you are answering from vendor's perspective: what are the examples of client's requirements addressing information security issues in offshoring?

.....
.....
.....
.....

15. What are the key features of a successful (strong, followed and obliged, established, efficient) information security management system in relation to offshoring and vendor related information security risks?

1 – Insignificant 2 – Little important 3 - Important 4 - Critical

Supported by top management
Documented
Documented in a well-structured documentation

Distributed to all parties

Needs to cover all information assets

Well and repeatedly communicated

Reviewed regularly

Present generally understandable objectives

Where possible, compliance should be required by contractual clauses

Consistent with other organizational communication

(list your own)

(list your own)

(list your own)

(list your own)

(list your own)

16. What budget is your organization willing to spend on increasing information security?

.....

.....

.....

.....

.....

.....

17. Is the budget growing from year to year? What is the rate of change?

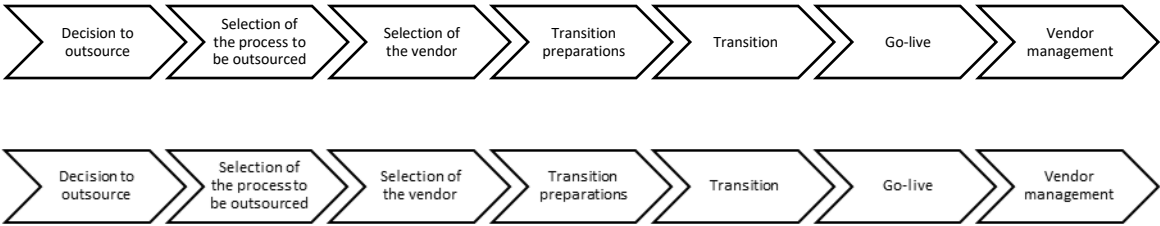
- k) Increasing (rate of change)
- l) Decreasing..... (rate of change)
- m) More-or-less remains stable

Data protection in outsourcing:

18. What phase of offshoring relate to the biggest information security risk? Please rank the following:

- Decision to outsource
- Decision to select the business process
- Decision to select the vendor
- Transition preparations
- Transition
- Go-live
- Vendor management

19. Given the timeline of outsourcing transition process below, please mark the moments where risk assessment(s) should take place (take places)



[At this point my thesis shows literature research on motivation to outsource, as this is too far away from the core topics of the thesis I do not include questions why do financial institutions outsource here]

20. The timeline above was created on basis of literature review and personal experiences. It may not reflect the process that you are familiar too with or the one established at your organization. Would you modify the timeline to reflect the process at your organization more realistically?

.....

.....

.....

.....

21. What are the key elements of an outsourcing risk management process before engaging in a relationship and afterwards?

.....

.....

.....

22. What are the most applicable information security challenges that financial institutions face when offshoring:

	No occurrence	Some occurrence	A lot of occurrence	Notorious occurrence
a) Vendor's information security management system				
b) Vendor's organizational culture towards information security				
c) Vendor's attitude				
d) Lack of effective vendor assessment possibilities				
e) Lack of vendor's competences				
f) Lack of supporting technology				
g) Systems / IT architecture difficult to manage and control				
h) Large number of vendors				
i) Lack of personnel awareness at financial institution				
j) Lack of personnel awareness at vendor's location				
k) Overall unwillingness towards change in the organizational culture				
l) Unstructured relationship between financial institution and vendor				
m) Lack of or vague information security clauses in contracts				
n) Well established relationship with additional requirements being difficult to impose				

23. On a scale of 1 to 4 please rate the level of information security awareness across employees in financial institutions? Would you say it needs improvement?

1 – Very low

2 - Low

3 – Medium

4 - High

Needs improvement

Satisfactory, therefore does not need improvement

24. On a scale of 1 to 4 please rate the level of information security awareness across employees at vendors' locations in India? Would you say it needs improvement?

1 – Very low

2 - Low

3 – Medium

4 - High

Needs improvement

Satisfactory, therefore does not need improvement

25. Do you believe that if the number of offshore vendors increases the more efforts should be put into maintaining the information security level?

[YES/NO]

The final questions relate to your personal experiences in designing and implementing internal controls or other mechanisms that aimed at increasing information security in offshoring relationships.

26. What is needed to make offshoring more secure in terms of protecting sensitive information?

.....
.....
.....
.....

27. Can internal controls reduce the information security risk in offshoring relationships?

.....
.....
.....
.....

28. What is your most successful story in increasing the information security level in offshoring relationships?

.....
.....
.....
.....

Appendix II

The overarching factors of information security controls design that will improve their effectiveness and therefore contribute to information security risk reduction in the case of Swiss financial institution engaged in offshoring are:

Risk focused controls

The design of controls must take into account relevant risks. Design of controls focused on international standards compliance that are generic enough to be applicable to all industries across the globe will not result in sufficient controls. The risk approach is the true issue of why no research, no matter how detailed, can deliver a bulletproof set of controls for financial institutions. There is no solution that fits all and this is why information security risks should be conducted prior to decision to outsource and periodically reviewed for all existing relationships with vendors.

Clearly assigned responsibilities

Controls that require overview or decision making should include assignment of responsibility. This has been proven in the observation and in the questionnaire that the responsibility assignment is particularly important when the control relates to multiple areas of expertise. Information security risks in offshoring processes are highly expected to carry controls that relate to multiple areas such as: compliance, procurement, information security, IT, offshoring and project management.

The reminder of the factors can be split across different phases of the process of offshoring. The stages as listed below were first identified in the case observation and later confirmed with the respondents who were encouraged to suggest changes or improvements to this model.



Decision to offshore

Research on economic and political prospects

Prior each decision to offshore, and for financial institutions already engaged in offshoring – on regular basis, the economic and political prospects need to be analyzed in order to identify potential obstacles that although not yet visible, may become valid in the near future. Information on referenda held in countries related to organization’s operations that will relate to availability of talent on the home institution’s market and vendor’s market can be found useful in offshoring planning to ensure that the impacted talent or taxes will not impact the offshoring costs and success.

Research potential regulatory changes

Apart from studying existing regulations and requirements that relate to offshoring and information security, financial institutions should also take into account any plans for new regulations. The case under study had established a crossfunctional compliance team that discusses any anticipated regulatory changes in order to determine their impact and applicability even long before the regulations come to place. The challenge was to build engagement across different stakeholders and encourage in-depth analysis of the requirements with various strategic goals across individuals.

Study compliance requirements

In global organizations, it is difficult to monitor requirements of all jurisdictions and define all applicable regulations without in depth familiarity of the business. Outsourcing this task to law office may also require a lot of efforts from within the organization as external entities may not have the knowledge sufficient to determine applicability. On basis on a previously mentioned example – it is important to identify differences in requirements and design the approach on how to tackle these.

Communication and senior management support

It is important for the process and associated controls to be clearly communicated to all participants of the process in order to obtain their understanding rather than face reluctance to change. Respondents have mentioned that aside to communication of the controls and requirements, support of senior management in the process of enforcing these controls is also very important.

Selection of business process to be offshored

Selection of the process to be offshored has been mentioned by interviewees. Although the selection of business process to be offshored fell outside the scope of observation (these decisions are highly confidential due to impact on current employees), some of conclusions on actions to be undertaken in this phase may be drawn from survey results. They are presented below.

Define what information is used in the process

In order to determine the applicability of regulations to the process and its transition across the borders, it is important to understand what kind of information is used in the process. Such activity will also help with next step (identify supporting IT assets). This stage can also help addressing the risk of low protection over know-how. In case the information used in the process reveals intellectual property of the organization, scope of offshoring should be revised in order to ensure that know-how remains within the home organization. Should the entire process require to be offshored, the risk of know-how protection can be addressed with non-competition contractual clauses.

Identify supporting IT assets

In order to avoid surprises at transition phase and in order to reduce risks associated with offshoring it is crucial to identify IT assets that support the process in the phase of deciding on the process to be offshored. Discovery of IT assets in use and their links with personal information will allow better preparation of data or systems segments that need to be offshored. At the same time identification of supporting architecture will allow identification of legacy or outdated systems and therefore prepare for complications during transition. It seems like preparation for complexity of IT architecture may reduce the offshoring risks during later stages of the transition process.

Test against potential for automation

One of technology trends for financial institutions as found in industry reports and in survey answers was automation and robotics. It may therefore be worthwhile to conduct analysis if it would not be more cost and time efficient to automate the process rather than offshore it to third party vendor. As mentioned in the main text of this thesis when discussing automation opportunities, blockchain technology should not be left out of consideration as with its high information security levels it may provide enough confidence to automate processes without impacting data integrity or confidentiality and therefore maintaining satisfactory compliance.

Ensure cost-efficiency

Having the information gathered from controls above, it may be seemingly trivial task – to ensure the anticipated cost efficiency. Respondents did say that the transition costs can expand and therefore it is important to compare these against the expected savings in the long-term.

Turnover assessment

When preparing the process to be offshored it may be worth to analyse the anticipated turnover of contractors engaged in offshoring, vendors – if plans are to move processes between vendors and employees as turnover of staff may add to complexity of the transition.

All of the above are factors that may be worth considering on top of the existing business decision-making processes in place such as existence of personal identifiable information (client identifying information), in order to ensure better internal compliance with the requirements but also to design appropriate security mechanisms addressing process-specific information security risks.

Selection of the vendor

Having made the decision on the process to be offshored, the decision on the vendor who should overtake the process should be made soon after. The vendor capability may also impact the decision on the process to be offshored.

Verify vendor's qualifications

Testing qualifications of vendor employees may even be more difficult than testing the employees of the organisation itself, so perhaps this verification should be maintained at control and management level rather than individual employees. During the observation it was noted that some of requirements, such as individual certifications may be included in contractual clauses. However, the certifications or degrees do not ensure neither technical skills or information security consciousness of the vendor employees, so this is why the qualifications should be tested with regards to the particular process at stake and associated risks.

Due diligence of vendor's technology

As the process is supported by certain IT assets it may be important factor of the transition costs and success. It therefore makes it important to verify the alignment of vendor's technology for particular process. It has been said by the interviewees that contractual requirements may not be enough to ensure the supporting IT systems capability and, more importantly, security. Interviewees highlighted that cooperation between business process owners, vendor IT staff and bank security specialists may be critical to establish the minimum but realistic requirements for the technology.

Pay attention to number of vendors

Although it may seem beneficial to engage vendor specializing in certain process for each of the different areas, respondents actually confirmed that number of vendors may impact the information security risks by increasing them. Large numbers of vendors introduce unnecessary complexity to the environment but also make it more difficult to review and manage vendors' compliance with contractual clauses. Large number of vendors, out of which uses different technology may also make it difficult to establish a baseline of security that will be applicable to all of them. When deciding on the vendor it is therefore important to remember that lower number of vendors is better for information security.

Assessment of information security awareness

On top of technical qualifications, respondents as well as literature highlighted the importance of vendors' employees' awareness on information security in managing information security risks in

offshoring. Before the vendor is selected it is important to identify the controls they have in place to ensure employees' awareness. Also, it is worth noting here that while international standards set the baseline for certain practices, they will not ensure the same level of awareness as they do not describe the best practice in such detail. Review of training materials to ensure alignment of awareness program may be more valuable to the transition process.

Assess threat landscape

Having identified the IT assets it is important what will potentially motivate cyber attacks and what attack vectors are most probable, remembering that hacking decisions are also made on basis of cost and benefit analysis. Assessment of threat landscape can help identifying additional controls that should be in place to protect information confidentiality. During the time of observation, no further threat landscape with relation to particular offshoring initiative was conducted, as it was believed that once performed risk assessment will be valid throughout the entire process. One aspect of threat landscape was specifically mentioned by the interviewees and it was to identify information exchange points in order to provide better security for them.

Transition preparations

The next phase of the process is the preparation for transition itself – one of the highest rated phases of transition in terms of information security risks. Respondents mentioned numerous factors that can decide on the success of transition that can be addressed by controls improvements in this phase.

Detailed incident response plans

Results of the survey clearly stated that incidents response plans should not only cover the processes “at rest” i.e. before transition and after “go-live” but also, if not especially, the transition process at self and stabilization. There is a large number of academic and industry publications on what the incident response plan should be and what information it should contain, therefore this point just highlights the importance of broadening the scope. Incident plans should also address the risk of business process disruptions caused by issues with transition process.

Prepare contractual clauses

Highly important part of the process is to prepare adequate contractual clauses. While standard contractual clauses have become popular over the past few years, the development of risks and the need for detailed guidelines implies that contractual clauses are actually adjusted to each process and associated threat landscape. The contractual clauses should define responsibilities for incident management planning and cooperation, the right to audit but also introduce controls that will ensure compliance such as non-compliance fees.

Organization

Out of the organizational controls that may impact the success of transition there were two key findings on how to address the information security risks.

Full time employee on the project

The interviewees responded that ensuring presence and engagement of a full time employee on the project may have beneficial impact on the transition. The turnover of contractors has been raised as one of the risks for information security during the process and to address this risk is to ensure a full time employed project manager or SME who will be aware of the issues and challenges of the process as well as the plan for transition.

Assignment of responsibilities

Based on the observation as well as the survey responses, the confusion in transition often is caused by large number of engaged specialists in the process. A solution to minimize the confusion and

therefore improve the probability of successful transition is assignment of responsibilities to stakeholders and establish decision-making bodies for various types of issues. The responsibilities in the process itself should also be assigned to employees at both sides – the home institution as well as vendor in order to better align expectations with feasibility.

Transition

Although this phase has been claimed to be the second most prone to information security risks, no particular control improvements to be deployed in this phase have been identified.

Go-live

Undoubtedly voted by the questionnaire respondents as the phase that carries most information security risk. While everything has been planned in the transition preparations – this phase can only be improved by implementation of monitoring of control performance

Continuous monitoring

Currently available technology allows analysis of data and behavioural patterns and statistics with capabilities that allow identification of issues before they have any impact of the process. Implementation of real life monitoring may help identifying an incident before it is serious enough to cause data breach.

Vendor management

The stabilisation phase is the stage that carries high risks of information security. The process is considered established and the risks associated with go-live diminish. Often the offshoring initiative teams are dissolved. However, the data breaches that do come to the surface thanks to media happen even in long term established offshore relationships.

Holistic offshoring management

In order to maintain information security risks at acceptable levels it is not enough to offshore each process securely. Offshoring new processes may have impact on security of processes already offshored – for example by providing additional information that the vendor did not have before. This is the reason why the offshoring should be managed in a holistic overview and not initiative by initiative. The holistic management however does not end with definition of the initiative handling process, but rather implies periodic holistic risks assessments and reviews.

Continuous development and improvement

On top of the holistic offshoring management and periodic vendor risk assessments the respondents have identified a factor that actually does appear in the ISO27001 as well, it being continuous development and improvement of implemented controls. In such fast developing environment of cyber security it is crucial to develop internal controls in order to respond to arising threats.

Contract termination

Clean-up procedures

Upon contract termination, especially after a long and established relationship – it is difficult, as per observation and respondents answers, to identify all the information ever transferred to the vendor. While the vendors are often obliged by contractual clauses to delete or transfer back the information gathered throughout the offshoring relationship, it is often omitted that clean up procedures should cover much more in terms of scope: user accounts in the systems, any links to the databases, physical and hard copies of information. It is important to maintain track of information passed throughout the process in order to be able to request the information and access to information upon contract termination.

