Automated Software Engineering (2021) 28:12
https://doi.org/10.1007/s10515-021-00286-x

Information security implications of using NLP in IT outsourcing: a Diffusion of Innovation theory perspective

Baber Majid Bhatti[1] · **Sameera Mubarak**[1] · **Sev Nagalingam**[2]

Received: 31 December 2020 / Accepted: 24 June 2021 / Published online: 16 July 2021

Abstract

Information technology outsourcing (ITO) is a USD multi-trillion industry. There is growing competition among ITO service providers to improve their service deliveries. Natural language processing (NLP) is a technique, which can be leveraged to gain a competitive advantage in the ITO industry. This paper explores the information security implications of using NLP in ITO. First, it explores the use of NLP to enhance information security risk management (ISRM) in ITO. Then, it delves into the information security risks (ISRs) that may arise from the use of NLP in ITO. Finally, it proposes possible ISRM approaches to address those ISRs in ITO from the use of NLP. The study follows a qualitative approach using the case study method. Nine participants from three organisations (an ITO client, service provider and sub-contractor) engaged in an ITO relationship in the ICT industry were interviewed through a semi-structured questionnaire. The research findings were verified through a focus group. Case study scenarios are provided for a clear understanding of the findings. To the best of our knowledge, it is the first study to investigate the information security implications of the use of NLP in ITO.

Keywords Information security risk (ISR) · Information security risk management (ISRM) · Information technology outsourcing (ITO) · Natural language processing (NLP)

✉ Baber Majid Bhatti
baber.bhatti@mymail.unisa.edu.au

Sameera Mubarak
sameera.mubarak@unisa.edu.au

Sev Nagalingam
sev.nagalingam@unisa.edu.au

[1] UniSA STEM, University of South Australia, Adelaide, Australia

[2] UniSA Business, University of South Australia, Adelaide, Australia

1 Introduction

Businesses often entrust other organisations for the delivery of their Information Technology (IT) services. This practice, commonly referred to as IT Outsourcing (ITO), has gained significant popularity during recent years (Ensslin et al. 2020). ITO businesses have grown tremendously during the past two decades (Delen et al. 2019). The global ITO and business process outsourcing market was apprised at USD one trillion in 2016 (Snowden and Fersht 2016), and it crossed USD 1.5 trillion by 2019 (Lioliou and Willcocks 2019). Despite its growing trend, the failure rate of ITO is high, which indicates the presence of risks and the importance of managing those risks prudently (Dhillon et al. 2017). Information security is among the top three risks and is expected to remain among the high growth areas in ITO (Moiseev 2020).

ITO has become an established field of research. The earliest publications on ITO started coming in the early 1990 s. A multitude of topics in ITO has been covered since then. Examples of these topics include motivations, decision-making, measurement of success or failures and risk management in ITO. Although information security is among the top concerns in ITO practice, there is still a need for more focused knowledge on information security risk management (ISRM) in ITO (Dhillon et al. 2017; Moiseev 2020). This need is evidenced based on the fact that the fast-paced innovation in IT causes unprecedented information security risks (ISRs), previously not investigated (Ensslin et al. 2020; Plotkin and Tweardy 2018; Schneider and Sunyaev 2016). For example, studies have acknowledged that new ISRs result from the innovations in cloud computing (Wulf et al. 2019), machine learning (Bhatti et al. 2020; Pitropakis et al. 2019) and natural language processing (NLP) (Alshemali and Kalita 2020), but a comprehensive understanding of those ISRs is still required.

NLP is an evolving field of research, which has found wide applications in the industry because of its ability to automatically understand and analyse human language (Kang et al. 2020). Hence, there can be several useful application scenarios of NLP in ITO. For example, as the industry is striving to automate ITO service delivery, NLP can help to improve the efficiency of collaboration among the client and service provider teams or to identify vulnerabilities in the software specification documentation produced by service provider organisations for their clients (Kang et al. 2020; Zhang et al. 2019). Similarly, NLP can be used to ensure privacy-preservation in multi-party ITO relationships (Sadat et al. 2019). However, NLP comes with its own implications related to information security (Zhang et al. 2019). The investigation of those implications is swiftly gaining the attention of researchers as the use of NLP for improving ITO experience results in information security vulnerabilities that are not yet fully understood (Alshemali and Kalita 2020; Feyisetan et al. 2020; Sadat et al. 2019; Winter and Rinderle-Ma 2018).

This paper aims at researching the information security implications of the use of NLP in ITO. The following questions are explored in this study:

RQ1 How can NLP help to improve ISRM in ITO?

RQ2 What ISRs can occur from the use of NLP in ITO?
RQ3 How can ISRs from the use of NLP in ITO be managed?

This paper explores the scenarios where NLP can be leveraged to manage ISRM in ITO practice. This knowledge will contribute to the wider applications of NLP in the ITO industry. However, the application of NLP comes with its own challenges, which need to be understood, so that the practitioners can make well-informed strategic planning and operational decisions. Among those challenges, this paper investigates the ISRs resulting from the use of NLP in ITO. The study goes further to propose mitigation approaches to those challenges. To the best of our knowledge, it is the first attempt to investigate this topic.

The paper is organised as follows: Sect. 2 reviews the works related to this topic of research. Section 3 describes the methodology adopted by the study to explore the research questions. Section 4 presents the findings of the study. Section 5 discusses those findings, explains the limitations of this study and provides directions for future research. Section 6 concludes the paper.

2 Related work

This section presents a review of related works. Starting with the ITO lifecycle, it elaborates ISRs in ITO and then offers a perspective of Diffusion of Innovation (DoI) theory. Next, it discusses the use of technologies, focusing on NLP, in ITO and their ISRM implications.

2.1 ITO

Outsourcing is the arrangement where an organisation delegates the delivery of some of its business functions to another organisation and purchases it back as a service (Wang and Wang 2019). It is a widespread phenomenon and is commonly adopted by businesses today (Bhatti et al. 2020; Kabiraj and Sinha 2016). When an organisation entrusts IT services to other partner organisations, this engagement is called ITO. The customer organisation is called ITO client, and the organisation who delivers the IT services to the client is called ITO service provider. One client can breakdown the IT scope to multiple parts and outsource any combination of parts to distinct service providers. One service provider may also provide ITO services to one or multiple clients. Together, clients and service providers are called ITO parties. If required, clients or service providers may negotiate an exclusive relationship, for example, the client will not outsource the services to other providers simultaneously, or the providers will not deliver services to other clients.

2.1.1 Reasons for ITO

In recent decades, ITO has gained increasing popularity among businesses globally. Although cost savings is a major reason for a business to opt for ITO, it is not the

only one (Williamson 1991; Yuan et al. 2020). Businesses may outsource their IT even at costs higher than running the related work inhouse (Jorgensen 2010; Kabiraj and Sinha 2016). Organisations yearn for competitive advantage through outsourcing, which is based on several reasons, such as:

Focus ITO client organisations want to focus on their core capabilities and business activities. Hence they outsource their IT to reduce their efforts consumed towards managing IT services and infrastructure (Premuroso et al. 2012; Tarsh et al. 2016).

Efficiency ITO is an opportunity to seek cost and process efficiencies in delivering IT services. Clients are motivated to outsource their IT because they desire service providers to deliver services at a lower price compared to the cost of running those services either in-house or through previous suppliers. The desire for cost efficiencies is the most significant reason for businesses to go for ITO (Martinez-Noya et al. 2012; Tarsh et al. 2016). Nonetheless, ITO clients also look for improved quality and business processes. The improved efficiencies are measured through pre-defined key performance indicators (KPIs) (Premuroso et al. 2012; Słoniec and González Rodriguez 2018).

Skills and knowledge Through ITO, a client organisation gains the advantage of skills and knowledge of the resources from its service providers. Access to service providers' skills and expertise are quite significant reasons for a client organisation's decision to outsource (Na Sakolnakorn 2011; Słoniec and González Rodriguez 2018).

Technology The technologies change fast, and frequently updating the platforms is not always feasible for businesses due to the high cost of purchasing and maintaining their own infrastructure. Hence, partnering with other organisations becomes a compelling reason to outsource IT. Through ITO, the client and service provider organisations form an ecosystem leveraging the role of the service provider to maintain the state-of-the-art technology infrastructure (Słoniec and González Rodriguez 2018; Youssef 2019).

New products and markets By contracting ITO to the international suppliers, organisations sometimes pursue their desire to access other markets. Through ITO partnership, new products can be prepared and offered to customers in those markets (Premuroso et al. 2012; Tarsh et al. 2016).

Similarly, several other reasons behind ITO may exist depending on the business priorities or prevailing circumstances. For example, the COVID-19 pandemic, China-US trade-war and UK Brexit have inclined businesses to seek opportunities through ITO (Baldwin and Tomiura 2020; Moradlou et al. 2021; Quaglietta and Alvord 2020; Wang et al. 2020; Zalnieriute and Churches 2021).

2.1.2 ITO life cycle

Since this paper relates to the enhancement of ISRM in ITO, it is pertinent to describe the ITO lifecycle to understand and analyse the ISRs. Figure 1 presents the ITO life cycle adopted from ISO 37,500 (Bhatti et al. 2017; ISO 2014). Bhatti, Mubarak and Nagalingam (2017) extended the ISO 37,500 model to incorporate ISRM throughout the ITO life cycle. After a strategic decision to go for ITO is

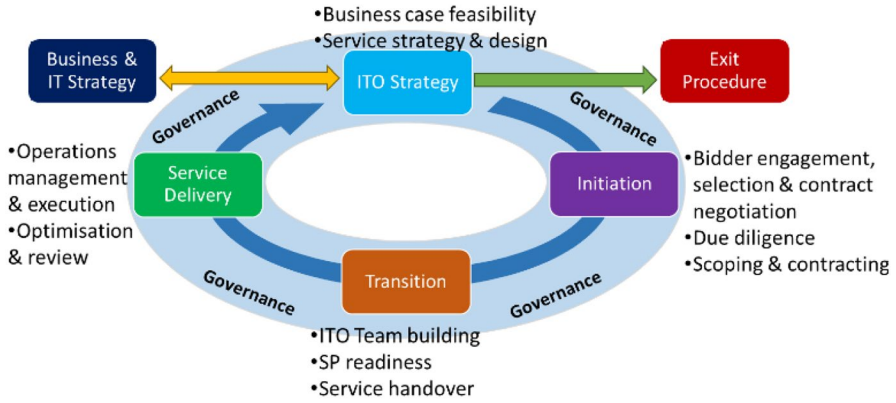

Fig. 1 ITO lifecycle

made, the ITO lifecycle begins. There are four phases in this model: ITO strategy, initiation, transition and service delivery, as described below:

ITO strategy is a consequence of business and ITO strategy and can impact the latter too. In this phase, the feasibility of the business case of ITO is assessed, whether it meets the needs and expectations. The finer decisions and assessment for ITO are carried out and the ITO strategy is formulated. The ITO strategy also includes the scoping of the services to be outsourced and the management of the remaining IT scope. The service strategy and design activities are also completed in this phase.

In the initiation phase, steps are taken toward engagement with the potential ITO service providers. The client compiles the detailed ITO requirements and expectations and publishes these documents. The clients may opt to float the requirements in the form of tenders, requesting responses in the form of bids. The clients, confident in their knowledge of their needs and expectations, publish detailed tenders, for example, Request for Proposals (RFP), or Request for Tenders (RFT). The clients who are less knowledgeable or confident in the understanding of their needs or expectations may split the service providers' engagement process into multiple stages. Therefore, they publish brief requirements, for example, Request for Information (RFI) or Expression of Interest to solicit detailed proposals from the potential service providers. The bids from interested parties (potential service providers) are evaluated, and the most suited bidders are shortlisted for contracting. After due diligence and finalising the scope of ITO, the contract is awarded to the selected service provider organisation. A client organisation may engage a single or multiple service provider organisations in an ITO relationship.

In the transition phase, the selected service providers build their teams to take over the outsourced scope from the client's teams. The outsourced IT services are then handed over by the client's personnel to the service provider's teams. The transition mainly focuses on service handover with no improvements or changes to service delivery scopes. The transition phase finishes with the milestone from where the client completely relinquishes its role in the delivery of outsourced services.

From there on, the service providers assume full responsibility for ITO service delivery.

In the service delivery (aka service operations) phase, the service providers run ITO service operations. The performance of ITO service delivery is measured against agreed KPIs. If requested by the client, the service providers may also undertake improvements through optimisations and review of the service performance. Within this phase, the client and service providers may agree to vary the scope, terms of the contract, or even terminate the ITO services, partially or fully, if deemed necessary. Throughout the ITO lifecycle, there is an omnipresent function of governance to oversee the smooth execution of ITO processes (ISO 2014).

2.2 ISRs in ITO

Although the competitive advantages are lucrative enough for the businesses to adopt ITO, the failure rate is high, and a variety of risks are involved (Dhillon et al. 2017; Moiseev 2020). Hence there is a need for understanding and managing those risks. A risk is defined as the likelihood of occurrence of an event, which has the potential to cause harm to business (Abdel-Basset et al. 2019). Information security is among the top three most significant categories of ITO risks (Truong et al. 2020). There are several ways the ISRs can be classified. For example, people, process and technology could be three categories (Dhillon et al. 2017; Lin 2010; Nassimbeni et al. 2012; Wulf et al. 2019):

People-oriented ISRs can include the lack of loyalty among the staff or capability of service providers' resources.

Process, legal or organisation-oriented ISRs come from practices, for example, lack of visibility into the services performed by the service providers' teams, lack of incompliance with the policies.

Technology-oriented ISRs may comprise examples from identity theft, information tampering, or unauthorised access to clients' resources.

The ITO orientation of an organisation can change its perception of ISRs (Dhillon et al. 2017). For example, trust that the service provider applies proper security controls, their ability to comply with the client's security policies, and the trust that they will not abuse the client's proprietary information or knowledge are the top-most ISRs from a client's perspective (González et al. 2016). However, information security competency of its own resources and the loss of knowledge due to staff turnover are among the top-most risks from a client's perspective (Dhillon et al. 2017; González et al. 2016).

2.3 Diffusion of Innovation (DoI) theory

The use of theory in research helps to understand a phenomenon and gain deeper insights into practice (Chou and Chou 2009). Several theories have been discussed in the ITO literature, for example, agency theory, resource-based view theory, transaction cost theory and DoI theory. This paper applies the DoI theory (Rogers 2003), and its brief description is provided here. According to DoI theory, five

characteristics justify an innovation's adoption in an organisation (Hanafizadeh and Ravasan 2017; Rogers 2003):

(i) Relative advantage of This characteristic represents the degree to which an innovation is perceived to benefit the organisation in comparison with previous Organisations tend to incline toward an innovation if its adoption is expected to bring a relative advantage.
(ii) It is the extent to which an innovation is consistent with the existing values, experiences, or business processes of the Compatible innovations have higher chances of acceptability.
(iii) It is the perceived degree of the ease of use of the The adoption of an innovation is negatively related to its complexity, i.e., ease of use and understanding.
(iv) It is the visibility of an innovation to The results or benefits of a few innovations are more visible than The observability of an innovation is positively related to its adoption.
(v) It refers to the testability of an innovation, i.e., the degree to which it can be tested on a limited The trialability helps to address the uncertainty about the adoption of an Hence, the trialability of an innovation is positively related to its diffusion.

Further details about the application of the DoI theory are provided in Sects. 3 and 5.

2.4 Natural language processing (NLP)

NLP is a technique for automatically understanding and analysing human language (Kang et al. 2020). With the advent of artificial intelligence (AI), NLP has found applications in diverse fields (Al-Hawari and Barham 2019; Kang et al. 2020). Examples of common functionalities of NLP are presented in Table 1, organised according to the sequence of appearance in typical usage.

2.5 NLP in information security and ITO

NLP is gaining the attention of experts in relation to its potential for enhancing information security. Following are the few instances where the application of NLP can be helpful:

2.5.1 Source code vulnerability analysis

The NLP model is trained on a collection of known vulnerable source codes. It is then applied to the given source code to identify the vulnerabilities (Russell et al. 2018).

Table 1 Functionalities of NLP

NLP functionality	Description	References
Classification	Identifying categories from the input content and segregating them into groups	Alshemali and Kalita (2020) and Feyisetan et al. (2020)
Machine translation	Translating input text or speech into another language, e.g., English to French	Kang et al. (2020)
Machine transformation	Transforming input text or speech into another form, e.g., speech to text	Alshemali and Kalita (2020) and Chowdhary (2020)
Question answering	Providing answers as outputs to input questions in human language (text or speech)	Alshemali and Kalita (2020)
Textual entailment	Predicting whether a hypothesis can be inferred from an input premise	Alshemali and Kalita (2020) and Feyisetan et al. (2020)
Tagging	Identifying tokens in the input and then classifying each token according to the grammar	Kang et al. (2020) and Winter and Rinderle-Ma (2018)
Parsing	Identifying tokens in the input and analysing the relationship between them	Alshemali and Kalita (2020) and Chowdhary (2020)
Dialogue generation	Interacting with human or machine users by understanding and analysing the input and generating responses	Chowdhary (2020)
Pattern matching	Correlating and matching similarities among distinct input messages	Chowdhary (2020) and Kang et al. (2020)
Sentiment analysis	Analysing the aggregate inputs and inferring the tone and sentiment of the source for generating the input messages	Kang et al. (2020)
Speech recognition	Understanding the meaning of what is being conveyed or identifying the source of input from its speech	Kang et al. (2020) and Sadat et al. (2019)

2.5.2 Detecting phishing attacks

NLP can be useful in the detection of certain types of information security attacks. For example, NLP techniques can be used to single out email messages containing phishing attacks (Buber et al. 2017).

2.5.3 Detecting denial-of-service attacks

Chambers et al. (2018) showed that using data from social media, NLP can be used to detect denial-of-service attacks.

2.5.4 Classifying malicious domain names

NLP has been shown to be effective in identifying malicious domains names from the internet (Buber et al. 2017).

2.5.5 Classifying malicious domain names

NLP has been shown to be effective in identifying malicious domains names from the internet (Buber et al. 2017).

The literature analysis reveals that the use of NLP for improving information security is gaining popularity but is still in the initial stages (Feyisetan et al. 2020). Hence, there is a need for identifying more scenarios where NLP can be helpful. This paper is among the earliest works to discuss NLP scenarios for helping information security in ITO. However, the use of NLP comes with several challenges, which need to be addressed (Chambers et al. 2018; Winter and Rinderle-Ma 2018). Information security vulnerabilities caused by the use of NLP are among the critical challenges, which are not sufficiently understood (Chambers et al. 2018; Feyisetan et al. 2020; Zhang et al. 2019).

3 Research Methodology

This section describes the methodology adopted for this study. It elaborates the approach, establishes the context by introducing three case organisations, elucidates the method of data collection and analysis, and explains the use of theory.

3.1 Approach

This paper explores the information security implications of using NLP in ITO. It required an in-depth investigation to answer the research questions posed in Sect. 1. Hence, a qualitative approach was selected (Creswell and Creswell 2018). A literature review was first conducted to get informed with the latest developments of NLP

in information security and ITO. For gaining first-hand knowledge about practitioners' experiences in the industry, a case study method was employed, with the organisation as the unit of analysis (Creswell and Creswell 2018; Yin 2014).

3.2 The case study

This study selected three organisations in the ICT industry to address the research questions. These organisations were engaged in an ITO relationship, as illustrated in Fig. 2. The real names of the organisations are anonymised in this study to preserve their identities.

The first organisation, CliTel, is the client organisation that provides telecommunication services to its subscribers in Australia. CliTel's offerings include voice, data and content-based services. It has a large telecommunication network and a complex IT infrastructure. To focus on its core business, CliTel outsourced its IT services to SerPro (the service provider organisation). Once CliTel took the business decision to go for ITO, it was reflected in the IT strategy of the organisation, and the ITO lifecycle kicked off. The finer decisions for ITO were carried out at the strategic planning stage of the ITO lifecycle, as shown in Fig. 1. These details included the scoping of which services to outsource and how the remaining IT scope would be managed.

CliTel considered the options of either (1) outsourcing distinct parts of ITO scope to multiple service providers or (2) outsourcing the entire ITO scope to one service provider organisation and then allowing them to engage with subcontractors for different systems if required. After deliberation on these options, CliTel decided to go ahead with the latter option in the ITO business case, i.e., to outsource the entire ITO scope to a single service provider organisation. Hence, steps were taken toward engagement with the potential ITO SPs.

CliTel prepared and published a Request for Proposals (RFP) document, detailed with ITO requirements and expectations. The bids from interested parties (potential SPs) were evaluated, and the most suited bidders were shortlisted. The contract for ITO service delivery was then awarded to SerPro, after negotiation.

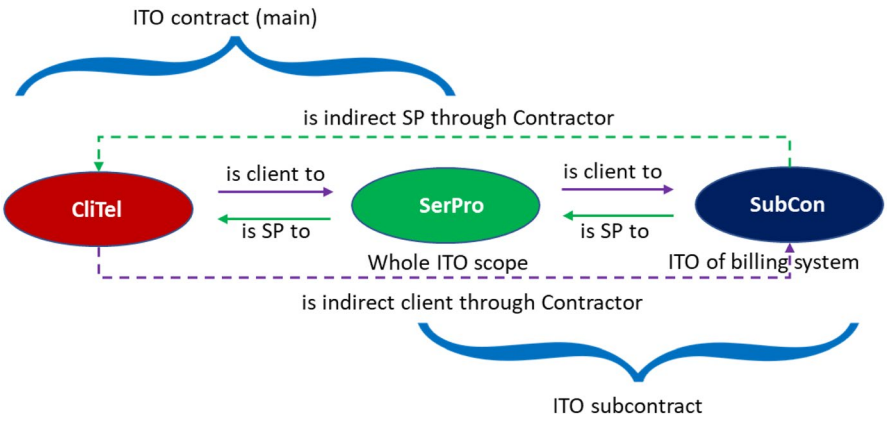

Fig. 2 ITO relationship of organisations

The second organisation, SerPro, is a large-scale multinational organisation, which provides specialised solutions and ITO services to clients in distinct industry verticals, including the telecom sector. SerPro leverages the latest technologies to provide competitive ITO services to its clients globally. They have their own service delivery platform (SDP), specialising in offering competitive services to SerPro's telecom clients globally. SerPro enjoys economies of scale through multi-tenancy, i.e., hosting multiple clients on their SDP. On the other hand, SerPro's telecom clients achieve a quick transformation of their business process through migration to SerPro's SDP as it already complies with the industry best practices.

After winning the ITO contract from CliTel, the team of SerPro took over the ITO scope from their new client through the transition phase of their ITO lifecycle, as shown in Fig. 1. The transition mainly focused on service handover without any improvements or changes to service delivery scopes. The commencement of service delivery (aka service operations) phase in the ITO lifecycle was the milestone from where CliTel completely relinquished its role in the delivery of outsourced services. From there on, the SerPro assumed full responsibility for ITO service delivery. A part of the ITO contract scope, SerPro undertook a project to migrate the service management scope of CliTel to their SDP. This project was called "Transformation" because the business process of CliTel would be re-engineered and achieve compliance with the industry best practices after migration to SerPro's SDP.

The third organisation, SubCon, is a medium-scale ITO service provider organisation, specialising in the customisation and running of telecom billing, enterprise resource planning (ERP) and customer relationship management (CRM) systems. CliTel's billing system is a customised solution tailored to their needs. Long before the ITO engagement with SerPro, this billing system was customised and deployed by SubCon for CliTel. Since then, SubCon had been running this billing system for CliTel. Considering the specialised role and good performance of SubCon and the satisfaction of CliTel, it was agreed in the ITO contract between CliTel and SerPro that the services of SubCon would be continued through a subcontract awarded by SerPro to SubCon. Hence, with the three parties' mutual agreement, CliTel terminated the direct contract with SubCon for operations management of the billing system, and SerPro outsourced the same scope to SubCon through a new subcontract. This subcontract was a back-to-back agreement between SerPro and SubCon for ITO service delivery of the billing system's scope as reflected in the main contract between CliTel and SerPro. Figure 2 shows the ITO relationship between these three organisations.

SerPro uses AI-based automation and NLP to improve the quality and efficiency of its ITO services. SerPro has also provided its NLP-based tools to CliTel and SubCon to facilitate ITO operations management. However, the use of these latest technologies in the business has information security implications, leading to various incidents and misunderstandings among the ITO partner organisations and some penalties owing to breach of contractual obligations. This research study investigates the information security implications from the use of NLP in this ITO setup.

3.3 Research participants

Invitations to participate in this research study were initially sent to the management of CliTel and SerPro. On their advice, the invitations were extended to the management of SubCon. The extended coverage of participants from the ITO setup helped enrich the data collected for this research by increasing the variety of voices from three organisations (instead of one or two) and multiple organisational levels within those organisations (Myers and Newman 2007). The invitations comprised formal emails, ethics approval of the research, an endorsement from the management, an introduction to the research and a confidentiality statement. The employees from the three organisations, i.e., CliTel, SerPro and SubCon, participated in this study. The ITO orientation of each participant is shown in Fig. 3. Pseudonyms are used for naming the participants, whereby CT means the participant is an employee of CliTel, SP means the participants is an employee of SerPro, and SC means the participant is an employee of SubCon. Furthermore, FG means this person participated in the focus group conducted to verify the findings of this research. Figure 3 shows ITO orientation in a Venn diagram. The blue circle represents client orientation, the red circle represents service provider orientation, and the green circle represents the subcontractor orientation of a participant. ITO orientation signifies the type of organisation in which a participant worked during his or her career. The overlapping circles denote that a participant has experience of working in organisations with multiple ITO orientation. For example, SP6 is currently an employee of the service provider organisation but also worked in the past for another organisation with a client ITO orientation. The ITO orientation of the participants was distinguished for three reasons. (1) it helped enriching data collection by emphasising the relevant questions. (2) it helped to conduct an in-depth analysis and to understand participants' perspectives through the context of ITO orientation in their experience. (3) interviewing participants from a mix of ITO orientations, from different organisations within an ITO setup and at various organisational levels helped verify the research findings by establishing theory-based triangulation as well as improving the understanding of NLP adoption's perspectives from the lens of DoI theory (Creswell and Creswell 2018; Guion et al. 2011).

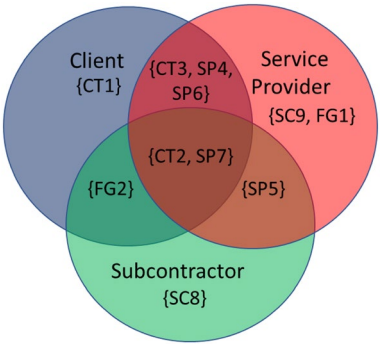

Fig. 3 ITO orientation of participants' experience

The participant selection criteria established in this study required each individual to have at least ten years of professional experience in the ICT industry with at least five years of experience related to ITO service delivery in any of the ITO orientations depicted in Fig. 3. Hence, eleven professionals were selected to participate in this study. The profiles of those participants are presented in Table 2. Three participants were interviewed from CliTel, four from SerPro and two from SubCon. They included professionals from management as well as technical backgrounds, possessing rich ITO experience and a variety of skillsets. There were no prior formal or personal relationships between the participants and the researchers of this study. Moreover, a focus group with two participants was conducted later to verify the findings.

3.4 Data collection method

The data were collected through in-depth semi-structured interviews (Creswell and Creswell 2018). Although the interviews were initially expected to be conducted in face-to-face sessions, they were conducted in online mode due to the COVID-19 restrictions in Australia at the time of data collection. The interviews followed an open-ended questionnaire so that the participants could freely discuss their opinions (Creswell and Creswell 2018; Yin 2014). The interviews were designed to explore the organisational and individual experiences of the participants on the scenarios using NLP to enhance ISRM in ITO (RQ1), the ISRs which can emerge from the use of NLP in delivering ITO services (RQ2) and how those ISRs can be managed (RQ3).

Since well-thought-out responses of the participants were required for this research, the interview questionnaire was shared with the participants in advance so that they could familiarise themselves with it for the best utilisation of interview time. Two pilot interviews were initially conducted to test the questionnaire for terminologies and language. For example, "technological perspectives" to improve the ISRM in ITO was not clear to a participant of a pilot interview. Hence, the question was paraphrased in the questionnaire. The amended questionnaire was then used to conduct the nine primary interviews with more understandable wordings for industry professionals (Kvale 2007). The interviews were audio-recorded and were verbatim transcribed into text.

The average duration of interviews was 1½ hours, although some interviews took longer to complete. The interview process was kept flexible. The researcher made reflexive decisions during the interview to adjust to the situation. Examples of such decisions include changing the sequence of questions to adapt to the discussion flow, skipping a question where the interviewer has already answered or spending more time on a question when the interviewer wants to provide more information. Hence, it was possible to customise each interview due to the interview questionnaire's openness and flexibility (Mason 2010).

Moreover, supplementary data were collected after the interviews through additional sources such as follow-up interviews or informal discussions. A diary was maintained to log such information, which was used during the analysis. The concerns raised or pieces of advice provided by the participants were also recorded. The

Table 2 Profiles of the participants

Participant (pseudonym)	Organisation	Job Role	Domain of expertise	Professional experience
CT1	CliTel	Director IT	IT Management, Systems and Infrastructure	21 years
CT2	CliTel	Specialist Network Operations and Security	Networking (Routing and Switching), Data Centre	14 years
CT3	CliTel	ICT Data Analyst	Network Operations, Data Analysis, Report Development	15 years
SP4	SerPro	ICT Business Analyst	Core Network Operations, ICT Business Analysis, Compliance and Audit	17 years
SP5	SerPro	Manager SMO	Software Development, IT Service Management	13 years
SP6	SerPro	Manager IT Service Delivery, IT Project Manager, Solution Architect	IT Service Delivery, Solution Architecture, ICT Business Analysis, IT Project Management	19 years
SP7	SerPro	Manager ICT Infrastructure	ICT Infrastructure, Data Centre, IT Security	16 years
SC8	SubCon	Manager IT Security	IT Security, IT Network Administration	11 years
SC9	SubCon	Team Lead IT Support	IT Support, IT Service Management, System Administration	14 years
FG1	Focus Group	Manager IT Service Delivery	IT Service Management, App Development, Data Analysis	16 years
FG2	Focus Group	Manager Systems Admin	Systems Administration, ICT Infrastructure	18 years

issues raised in one interview were discussed in the subsequent interviews to find suitable answers or explanations. It helped identify similarities or justify the difference of opinions among the participants' perspectives (Myers and Newman 2007).

3.5 Thematic analysis

A thematic analysis was performed on the collected data to develop an understanding of the underlying themes (Braun and Clarke 2013). The interviews were transcribed verbatim for the analysis. It helped the researchers to understand and interpret the data. The text data (interview transcripts) were coded and analysed using NVivo 12 tool. A reflexive thematic analysis was performed in six steps, following the guidelines from Braun et al. (2019).

1. Familiarisation with the data was obtained by reading through the data repeatedly as required. The first interaction of the researchers with the data was during the interview. The second interaction was during the transcription of audio files to text. Later, each interview transcript was reflected upon to understand the participant's perspective in his or her responses. Consequently, each participant's responses were discussed with a peer researcher to develop an in-depth familiarity.
2. Line-by-line coding was performed on the entire dataset. The NVivo software was used to generate codes manually, i.e., going line-by-line through the interview text.
3. Initial categories of data were then generated inductively by identifying broader patterns of meanings, which might be helpful in answering the research questions.
4. The categories were reviewed iteratively and refined into themes. Here, the theme meant a pattern of shared meaning connected to a central idea. This step was undertaken to ensure that the identified themes fitted well into a convincing explanation and answered the research questions. In this step, the themes were refined, aggregated, split or altogether discarded.
5. A detailed analysis of each theme was conducted. It was done by determining the story told by each theme, backed by data. The themes were then appropriately named and defined with explanations.
6. A write-up was prepared by narrating the analysis and quoting extracts from data, and contextualising the analysis. This write-up is presented in Sects. 4 and 5.

3.6 Use of theory

The use of theories in outsourcing research is important as it helps to comprehend and formulate theoretical foundations of the practice (Chou and Chou 2009). DoI theory (Rogers 2003) was used to understand the phenomena from a theoretical perspective. Since this theory explains the reasons for the adoption of innovation in organisations (Hanafizadeh and Ravasan 2017), its use was appropriate in this study because it helped to interpret the arguments provided by the participants in relation to adopting NLP in their ITO service delivery (RQ1).

A thorough understanding of the adoption scenarios of NLP for ISRM in ITO helped to further discover the ISRs of NLP in ITO (RQ2) and the possible mitigation approaches for those ISRs (RQ3). Furthermore, the DoI theory provided a theoretical foundation for conceiving the research questions in this study.

3.7 Verification

Verification of qualitative research means assuring the accuracy of findings from the viewpoints of researchers, participants and readers. The verification of qualitative research is conducted to improve its trustworthiness, credibility and authenticity (Creswell and Creswell 2018). The following strategies were applied to verify the findings in this research:

Participants from three organisations (CliTel, SerPro and SubCon) were interviewed to triangulate their differing perspectives on the same questionnaire. This helped to find the similarities of their responses and identify the areas of their disagreements. Hence, the collected viewpoints formed the basis of verification through data triangulation. Data triangulation was also performed by interviewing the participants from a variety of skill sets. Figure 4 presents the skill map of the participants across the organisations. It shows a range of skill sets and professional experiences of the participants. Hence, data triangulation was constructed into the data collection strategy.

Methodological triangulation was conducted after identifying themes from the data by holding a focus group which was attended by two participants. One participant was from CliTel, and the other participant was from SerPro. However, they are shown as a separate organisation in Fig. 4 because they were not previously engaged in the research. Hence, their perspectives formed the basis of verification through methodological triangulation verified the research finding.

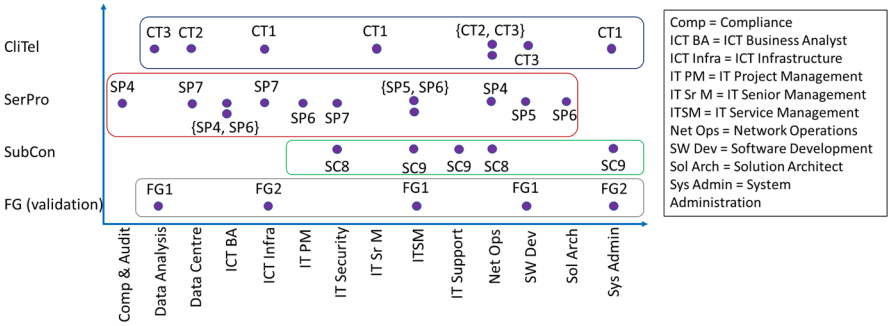

Fig. 4 Skills map of participants across the organisations

4 Findings and analysis

This section presents the findings obtained in this study by using the methodology described in Sect. 3 and the analyses of those findings. Section 4.1 provides the answer to RQ1, Sect. 4.2 answers the RQ2 and Sect. 4.3 addresses RQ3.

4.1 ISRM in ITO using NLP

Computers are not intrinsically introspective, i.e., they do not know what information they are holding and the processes they are executing. But the NLP is helping the computers to understand the useful information, and then they can follow the steps described in the documents they process (Kang et al. 2020). This capability can be used to improve the automatic understanding of ISRs in ITO and the management of those ISRs. Selected scenarios are presented in Fig. 5 and described below:

4.1.1 Identifying malicious code in shorter turnaround time

ITO clients use NLP to automatically detect malicious or aberrant parts in the code produced by service providers or their subcontractors. The clients utilise their NLP-based tools for this purpose. The tool breaks down the software code into smaller parts, and then NLP entails the correlation of those parts. This activity discloses the behaviour of various parts of the code, tagging the malicious code without the need to execute the code. It is pertinent to mention that without this NLP-based capability, finding malicious segments in code requires enormous time, effort and cost in testing and quality control.

Case study scenario:

CliTel acquired bespoke software from a third-party organisation, and this software is used to validate the scripts of billing solutions provided by SubCon. This check is an additional NLP-based measure to identify any malicious elements in the billing scripts automatically. CT2 expressed, “Bills processing is a very sensitive endeavour, and any malicious activity in this process can expose the sensitive information of customers into the wrong hands. Hence, this check, based on NLP, has added to our peace of mind .”

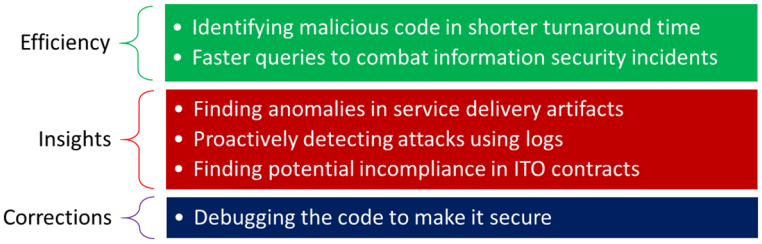

Fig. 5 NLP use-cases for ISRM in ITO service delivery

4.1.2 Debugging the code to make it secure

ITO service providers use trained NLP models to identify the deviations in software code from expected behaviour through parsing, pattern matching and semantic analysis. Once the aberrations are identified, the NLP model suggests cleaner versions of the code. Having cleaner code means fewer bugs and hence, a lesser chance of information security vulnerabilities that an adversary could exploit.

Case study scenario:

1. SP5 informed, "Our (SerPro's) QA team uses NLP tools to analyse the malbehaviour of CliTel's information systems to find bugs in the software or systems integration".
2. According to SP6, "Our (SerPro's) development teams use NLP to debug the issues with software code or its integration with other systems ".
3. FG2 confirmed, "We (SerPro) use NLP to advise the SubCon's team on debugging of their code".

4.1.3 Faster queries to combat information security incidents

From a game theory perspective, information security is a continual race of capability and faster measures between the ITO service providers and the adversaries. By leveraging NLP-based features, the security team of service providers and subcontractors can fix a vulnerability or combat a threat. They can swiftly query knowledgebase and information systems through machine translation, machine transformation, and query text generation without losing time to write complex commands or queries.

Case study scenario:

During information security incidents with CliTel's information systems on SDP, for the SerPro's team combating with information security incidents, time is of the essence, and the resources are always limited. SP7 advised, "Automatic query generation for systems and network elements through NLP, based on the natural language input from the operations team (a combination of voice and text), is handy in saving time and effort to write complex queries (during an incident)". In CT2's opinion, "Having NLP capable information Security systems also saves time in replicating queries to multiple devices or systems (during an incident)".

4.1.4 Finding anomalies in service delivery artifacts

In ITO service delivery, there are several artifacts produced and shared among the teams for further action or with the stakeholders for their information or advice. Any errors or anomalies in those artefacts can cause reworks, hamper the downstream

processes and may lead to breaches of service level agreements (SLA) with CliTel. Hence, SerPro and SubCon expend significant time, money and efforts to minimise the errors or anomalies in those artifacts through their service excellence and quality assurance functions.

Case study scenario:

SP4 identified service delivery scenarios on SDP, depicting the use of NLP to help find anomalies in the service delivery artifacts. Those scenarios presented in Table 3. The table organises the artifacts in a sequence as emphasised by the research participants.

4.1.5 Proactively detecting attacks using logs

Using logs and events' information, NLP helps in proactively detecting abnormal behaviour or attacks. It is done by applying classifiers to identify suspicious activities. Similarly, NLP helps in converging to the root-cause analysis of information security incidents by analysing the logs. Once the root cause is identified, the remedial actions are executed.

Case study scenario:

CT1 expressed satisfaction with SerPro's information security management capability by exclaiming, "We are happy that they (SerPro) have developed a tool that uses NLP to analyse the logs of SDP systems continuously. It is a proactive analysis using pattern matching and textual entailment features of NLP to identify potential information security threats." Hence, NLP is helping SerPro to stay vigilant and take corrective actions before the adverse effects of an information security threat can substantiate. When required, SerPro shares the information or advice for corrective action CliTel or SubCon teams.

Table 3 Anomaly detection scenarios in service delivery

Artifact	Anomaly detection scenario using NLP
Incident alerts	A common issue in incident alerts is false positives and false negatives. Using textual entailment feature, the NLP solves this issue by validating the correlation between the alert and the state of source entities
Trouble tickets (TTs)	A common issue is an inaccurate or incomplete description written by humans in TTs, leading to incorrect actions, delaying the restoration and hence, availability of disrupted services. The NLP instance validates the TTs by understanding the actual situation, establishing the context based on alarms from multiple entities. If required, it improves the integrity of information by generating accurate and complete text in TT
Work orders (WOs)	Adversarial activity on SDP or human error can cause a work order to comprise wrong authorisation or incorrect location for the corrective action. Wrong authorisation can give access to the adversary (confidentiality, integrity and availability threats). At the same time, incorrect location information can divert the dispatch of fault restoration teams to a wrong site, hence delaying the service restoration (availability threat). Using parsing, tagging and classification features, NLP segregates out the wrong WOs and is capable of rectifying the WO information without human intervention

4.1.6 Finding potential incompliance in ITO contracts

Ever-changing requirements from clients and regulatory authorities, varying circumstances and scope creep are among the most common issues in ITO. Ensuring compliance with the changes is a continual effort and an ongoing challenge. To address this challenge, the validity of the contracts, policies, SLAs and KPIs need to be continually assessed. NLP helps the clients and service providers in conducting this continual assessment of the artefacts. In case of imminent incompliance with the new regulations or business needs, the NLP raises flags indicating the need for a review of those artifacts. Without this role of NLP, it is a substantial and time-consuming effort for multinational ITO clients and service providers to assure compliance. The incompliance often leads to information security vulnerabilities or heavy penalties.

Case study scenario:

SerPro's NLP tool is capable of parsing through contracts, standards and regulations and performing tagging, classification, text entailment and pattern matching. CT1 added, "SerPro has given access of this tool to us (CliTel) and SubCon so that we can also use it on ITO related matters. The NLP is used to raise potential incompliance or discrepancy between expected and actual ITO service delivery. This automated tool facilitates our legal, procurement and regulatory affairs departments".

4.2 ISRs in ITO from the use of NLP

Although NLP is very useful in managing ISRs in ITO, its use can result in information security vulnerabilities that can be exploited by adversaries (Zhang et al. 2019). These vulnerabilities have the potential to induce malfunctioning or anomalies in NLP models. Hence, ITO organisations need to understand the ISRM implications when they undertake NLP in their service delivery models. Those ISRs can be broadly categorised as follows:

4.2.1 Adversarial activities inducing confusion

In this category, the adversaries induce confusion by swapping or scrambling adjacent characters in an ITO artifact or legal document. Participant SP5 elaborated, "Such confusion can be induced by tampering with the content in TT, WO, contract document or scope change request". For example, swapping adjacent characters in a word, deleting letters from a few words, or replacing characters but keeping the visual form of the words. Participant SP6 mentioned, "Although such alterations may easily be ignored by a human reader but can distort the behaviour of the NLP model".

Case study scenario:

SP7 provided the following case study scenarios to illustrate this category of ISR, whereby the adversary can use NLP to change the meaning:

1. Change → chance: "when the incident is not resolved within 4 hours of detection, a *change* in the remedial action plan is allowed" can be morphed to "when the incident is not resolved within 4 h of detection, a *change* in the remedial action plan is allowed".
2. Order → older: "when a conflicting situation arises, the *order* of the above-mentioned rules will be applied" can be morphed to "when a conflicting situation arises, the *order* of the above-mentioned rules will be applied".
3. Elect → eject: "the software will *elect* the highest priority task first, from the execution queue" can be morphed to "the software will *elect* the highest priority task first, from the execution queue".

4.2.2 Adversarial activities attacking semantics

This type of adversarial activities usually targets to change the meaning of the text by replacing words or group of words. For example, it can be done by substituting the words in an ITO artifact with their synonyms, antonyms or even negating words, which change the meaning of the original text. The adversaries can even remove the stopping-words to change the semantics, which puts NLP in a confused state, impacting its service availability through misclassification.

Case study scenario:

SC9 shared a situation where the addition of the word "not" can land the service delivery operations to an entirely different interpretation of the contract: "A resource can be replaced if not performing to the required performance levels for a period of two weeks consistently" can give an altogether different meaning with the addition of just one word: "A resource can ***not*** be replaced if not performing to the required performance levels for a period of two weeks consistently".

4.2.3 Adversarial activities targeting sentences

The adversaries using this category of action alter the sentences to generate the attack on the NLP model in ITO. For example, an adversary can tamper with human-approved sentences by removing or even paraphrasing the segments in a TT or WO on the SDP (CT2). The alteration of the authorisation statement from a WO renders it meaningless as the working rights of fault-restoration teams of the service provider are not allowed access to the site, hence delaying the service restoration times (SC9).

Case study scenario:

Once, the incident management team of SerPro rushed in the late night to their data centre to fix an issue with the core router. However, they were denied entry to the data centre by the security guard because an adversary had altered the location ID in the WO to a telecom tower site in another city. The incident management team had to wait for around two hours to coordinate with the back-office and get the

location ID corrected. This elongated the service restoration time and hence caused an SLA breach (SP6).

4.2.4 Adversarial activities targeting the NLP model

The adversaries in this category attack the functionality or capabilities of the NLP model. The examples of NLP functionalities are presented in Table 1. Since Machine Learning (ML) and Deep Learning (DL) are the most popular choices for implementing NLP applications (Alshemali and Kalita 2020), the adversary may seek to formulate attacks similar to those on ML-based Automation (MLA) systems (Bhatti et al. 2020; Pitropakis et al. 2019; Qiu et al. 2019). Those attacks can be made as follows:

(i) *Data injection* The adversary does not have access to training data or the NLP model. They add new data to corrupt the training input of the NLP model.
(ii) *Data modification* The adversary has access to the training data but not the NLP model. They tamper with the original input training data of NLP.
(iii) *NLP model corruption* The adversary has access to the NLP model, and they corrupt its weights or internal architecture.
(iv) *White box attack* The adversary has complete knowledge of the NLP model, i.e., internal architecture, weights and the characteristics of training data. They use this knowledge to corrupt the NLP model.
(v) *Black box attack using characteristics of input training data* The adversary has access only to the characteristics of input training data, using which they train their own NLP model to give similar outputs. Then they use their NLP model to prepare corrupt inputs for the original NLP model. Those corrupt input can cause the original NLP model to misbehave, for example, misclassify the outputs.
(vi) *Black box attack using the functionality of MLA instance* The adversary has access only to the functionality of the working NLP model. Using the technique similar to that of the previous black box technique, they attack by generating the corrupt (input, output) set.
(vii) *Restrained black box* The adversary can only observe the working NLP model. Using this access, they compile the (input, output) dataset from the NLP model. Exploiting this dataset, they corrupt the NLP model as in the previous black box techniques.

Case study scenario:
Once the NLP model is corrupted, the adversary can impact any of the NLP functionalities described in Table 1. For example, (i) the TTs can be misclassified into wrong categories, (ii) the incident alerts can be inaccurately entailed to be considered false positives, or (iii) the WOs can be issued with incorrect details for ITO service delivery (SP6).

4.3 Managing ISRs from the use of NLP in ITO

The ISRs in ITO from the use of NLP needs to be managed. To this end, ISRM efforts have not yet achieved much success. However, the following directions can potentially provide mitigation to these ISRs:

4.3.1 Adversarial training

The NLP models can be trained on datasets comprising information about adversarial activities. Once it is done, the NLP model will be able to detect adversarial activities and can respond by not modifying its behaviour in response to adversarial activity. However, to make it happen, datasets on adversarial activities are required, which are not yet available.

Case study scenario:

SP4 voiced, "It is a real challenge to train the machine-learning-based NLP model to be able to identify adversarial activity during service operations. It is like a thief's chase by police where the winner is the one with better capabilities. Although we are striving to make it happen, it needs an industry-wide collaboration and institutionalisation, just like in the case of police".

4.3.2 Resilient NLP models

Another approach is to increase the resistance of NLP models to possible adversarial attacks. This approach requires modification of the NLP model to make structural changes, which add to its resilience. Accurate knowledge is required about the adversarial attacks for appropriate changes in NLP models, which is a challenge because such information is hard to foresee. Moreover, a heuristic approach is required to design the structural changes in the NLP model, which is not easy to implement.

Case study scenario:

SP6 said, "We are trying to implement resilient NLP models, but at the moment, we yet have to achieve the desired results".

4.3.3 Encapsulators

Encapsulators are the mechanisms used with NLP models to protect them from adversarial attacks. The advantage of using encapsulators is that no change is required in the structure or training of the NLP model. The concept is in the early stages, and more work is required to develop effective encapsulators to protect the NLP models by defending against or recovering from adversarial attacks.

Case study scenario:

SP6 said, "Encapsulators is low-hanging fruit (seems relatively easier to implement than the previous two approaches). However, it is a very recent concept and is currently under development. Once developed, this solution will be rigorously tested and then migrated to the operational platform".

5 Discussion

This section discusses the findings, highlights the limitations of this study and provides directions for future research.

5.1 NLP adoption for ISRM in ITO

The interviews with participants revealed that NLP has great potential for improving ISRM practices in ITO. This finding is consistent with the outcomes of the recent research on NLP (Alshemali and Kalita 2020; Kang et al. 2020; Mathews 2019). As presented in Fig. 5, the use of NLP in ITO assists ISRM in three dimensions. Firstly, it improves the efficiency of ISRM, as the ITO service providers develop the capability to identify malicious code in shorter turnaround times and generate faster queries to manage information security incidents. Secondly, the NLP helps ITO service providers and their clients developing deeper insights into their ISRs. They are able to discover anomalies in service delivery artifacts, proactively detect attacks using security and systems logs, and explore potential incompliance in their ITO contracts. Thirdly, the use of NLP in ITO facilitates the ISRM by being able to achieve corrections in the source code in faster, automated and robust ways.

The salient examples captured from the real-life ITO practices are presented in Sect. 4 of this paper. However, the scenarios presented in this paper are by no means exhaustive and more scenarios need to be explored for the benefit of ITO practice. These scenarios will also positively impact the feasibility of ITO businesses of the client, service provider and subcontractor organisations.

NLP is being adopted to address the current shortage of information security professionals by automating ITO service delivery tasks (Janssens 2019; Kang et al. 2020). This automation is mostly based on ML or DL, which are areas of AI (Alshemali and Kalita 2020). These automation techniques are emerging fast. Hence, the NLP scenarios banking on these techniques is expected to embrace evolution, giving rise to new ISRs. Further research is required to explore those new ISRs in ITO from the use of NLP.

5.2 New ISRs from the use of NLP in ITO

The industry is now starting to understand the ISRs in ITO from the use of NLP. New ISRs are also emerging, which are not yet sufficiently explored. The implications of those ISRs need to be investigated in the light of regulations, standards, industry type, demographics and cultural attributes. For example, the issues concerning privacy are surfacing when organisations are increasingly relying on NLP (Feyisetan et al. 2020). Businesses need to be aware of their information security obligations before considering the use of NLP in their ITO, where failing to meet those obligations may result in heavy penalties (Kang et al. 2020; Mathews 2019).

As new ISRs are discovered from the use of NLP, ideas to manage those ISRs need to be proposed (Buber et al. 2017; Shropshire 2018). Sound knowledge of the

possible adversarial activities targeting the machine-learning-based NLP models of ITO service providers is essentially required before the organisations can come up with their ISRM strategies. At present, the efforts in the industry to manage ISRs from the use of NLP in ITO have not yet achieved much success. However, the ISRM approaches have been proposed but are yet in the early stages. To the best of our knowledge, there is no study that has investigated the use of NLP for improving ISRM in ITO. Future studies are encouraged to explore new ISRs and their implications and propose ISRM strategies in this area as the current knowledge is limited.

The approaches to manage ISRs from the use of NLP in ITO can be broadly classified into three categories. (1) organisations can train their NLP models to detect adversarial activities. (2) ITO service providers can build resilient NLP models, which have more resistance to adversarial attacks, or can restore to their reliable state after an adversarial activity takes place. (3) ITO service providers can implement encapsulator solutions to protect their NLP models from external adversarial attacks.

NLP is beneficial to ITO businesses for international collaboration among client and service provider teams (Kang et al. 2020). NLP has enabled the engagement of organisations in ITO relationship independent of the languages of their skilled resources. It is reasonable to expect new ISRs to emerge from this application of NLP in ITO. Those ISRs need to be explored, and their mitigation strategies need to be investigated.

5.3 DoI theory perspective

As described in Sect. 2.3, the DoI theory helps to understand the adoption of innovation in an organisation (Hanafizadeh and Ravasan 2017; Rogers 2003). The five attributes of this theory are applied to the adoption of NLP for the enhancement of ISRM in ITO client and service provider organisations as follows:

(i) *Relative advantage* The adoption of NLP in ITO bestows competitive advantage to an organisation for ISRM, as described in Sect. 4.1.
(ii) *Compatibility* NLP models are usually trained to improve the efficiency of the existing business processes. Hence, the compatibility attribute of the DoI theory is addressed.
(iii) *Ease of use* One reason for the popularity of NLP for ISRM in ITO is the convenience which it brings by automating the analysis of content in various forms.
(iv) *Visibility* The use of NLP by a service provider adds to its capability from an ITO client perspective. Hence, the service provider is seen as more capable of delivering ITO services, thus increasing the peer pressure on competitor service provider organisations.
(v) *Trialability* An ITO client can test the reliability of the NLP capability of their service provider by executing simple test cases.

By reviewing the five attributes of the DoI theory on the use of NLP for improving ISRM in ITO, it is inferred that this practice is expected to gain popularity in

future. Hence, more research is required to explore the ways NLP can help improving ISRM in ITO and understand the ISRs emerging from the use of NLP.

5.4 Limitations and future directions

The limitations of this study are as follows. First, this investigated a single ITO relationship between the three organisations. Future studies can remove this limitation by examining more ITO setups. Then, this study interviewed nine participants and conducted a focus group with another two participants. Hence the knowledge gained is limited to their experiences and expressed opinions. Lastly, ISRM in ITO and the use of NLP are rapidly evolving areas. Although this study strives to address a focused topic of convergence of these areas, comprehensive coverage by future studies is still required.

This research investigates new ISR scenarios emerging from the use of NLP in ITO. Further research is needed to rank various ISRs that ITO services can be subjected to while using the NLP in ITO. Moreover, researchers can conduct in-depth investigations to explore the degree of harm associated with each ISR. It may be interesting to see how those rankings and the degree of harm change from industry to industry (for example, telecommunications, banking or healthcare), in the perspective of ITO orientations (client, service provider or subcontractor), and for different ITO models (for example, offshoring, co-souring or managed services).

6 Conclusions

This paper investigates the use of NLP to enhance ISRM in ITO. A qualitative approach is followed, using the case study method to examine the ITO practices at three organisations in an ITO relationship: CliTel (client), SerPro (service provider) and SubCon (subcontractor). The data was collected through nine semi-structured interviews based on an open-ended questionnaire. DoI theory was applied to conceive the research questions for this study and to understand the adoption of NLP for ISRM in ITO. The first research question examined the scenarios of NLP, helping to improve ISRM in ITO. Specific issues from ITO service delivery are described where NLP provides the solution. The second research question investigated the ISRs resulting from the use of NLP in ITO. The ISRs are elucidated with examples. The third research question explored the strategies to manage the ISRs resulting from the use of NLP in ITO. Those ISRM strategies are concepts at this stage and need to be verified by future studies. However, these research findings were verified using a focus group. Further research is recommended to explore more ISRs emerging from the use of NLP in ITO, investigate their implications and propose their ISRM strategies.

Funding All authors certify that they have no affiliations with or involvement in any organisation or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript.

Declarations

Conflict of interest The authors have no conflict of interest to declare that are relevant to the content of this article.

References

Abdel-Basset, M., Gunasekaran, M., Mohamed, M., Chilamkurti, N.: A framework for risk assessment, management and evaluation: Economic tool for quantifying risks in supply chain. Future Gener. Comput. Syst. **90**, 489–502 (2019)

Al-Hawari, F., Barham, H.: A machine learning based help desk system for IT service management' J. King Saud Univ. Comput. Inf. Sci. 17. (2019) (**Article in Press**)

Alshemali, B., Kalita, J.: Improving the reliability of deep neural networks in NLP: a review. Knowl. Based Syst. **191**, 105210 (2020)

Baldwin, R., Tomiura, E.: Thinking ahead about the trade impact of COVID-19. In: Economics in the Time of COVID-19, pp. 59–71. Centre for Economic Policy Research (CEPR) Press, London, UK, (2020)

Bhatti, B.M., Mubarak, S., Nagalingam, S.: A framework for information security risk management in IT outsourcing. In: Australasian Conference on Information Systems (ACIS) (2017)

Bhatti, B.M., Mubarak, S., Nagalingam, S.: Information security implications of machine-learning-based automation in ITO service delivery—an agency theory perspective. In: International Conference on Neural Information Processing, pp. 487–498. Springer (2020)

Braun, V., Clarke, V.: Successful Qualitative Research: A Practical Guide for Beginners. SAGE Publications, Inc., Thousand Oaks (2013)

Braun, V., Clarke, V., Hayfield, N., Terry, G.: Thematic Analysis, pp. 843–860. Springer, Singapore (2019)

Buber, E., Diri, B., Sahingoz, O.K.: NLP based phishing attack detection from URLs. In: International Conference on Intelligent Systems Design and Applications, pp. 608–618. Springer (2017)

Chambers, N., Fry, B., McMasters, J.: Detecting denial-of-service attacks from social media text: applying nlp to computer security. In: Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, pp. 1626–1635 (2018)

Chou, D.C., Chou, A.Y.: Information systems outsourcing life cycle and risks analysis. Comput. Stand. Interfaces **31**(5), 1036–1043 (2009)

Chowdhary, K.R.: Natural language processing. In: Fundamentals of Artificial Intelligence, pp. 603–649. Springer, New Delhi. https://doi.org/10.1007/978-81-322-3972-7_19 (2020)

Creswell, J.W., Creswell, J.D.: Research Sesign: Qualitative, Quantitative, and Mixed Methods Approaches, 5h edn. SAGE Publications, Inc., Thousand Oaks (2018)

Delen, G.P.A.J., Peters, R.J., Verhoef, C., Van Vlijmen, S.F.M.: Foundations for measuring IT-outsourcing success and failure. J. Syst. Softw. **156**, 113–125 (2019)

Dhillon, G., Syed, R., de Sá-Soares, F.: Information security concerns in IT outsourcing: identifying (in) congruence between clients and vendors. Inf. Manag. **54**(4), 452–464 (2017)

Ensslin, L., Mussi, C.C., Dutra, A., Ensslin, S.R., Demetrio, S.N.: Management support model for information technology outsourcing. J. Glob. Inf. Manag. (JGIM) **28**(3), 123–147 (2020)

Feyisetan, O., Ghanavati, S., Thaine, P.: Workshop on privacy in NLP. In: 13th International Conference on Web Search and Data Mining, ACM, pp. 903–904 (2020)

González, R., Gascó, J., Llopis, J.: Information systems outsourcing reasons and risks: review and evolution. J. Glob. Inf. Technol. Manag. **19**(4), 223–249 (2016)

Guion, L.A., Diehl, D.C., McDonald, D.: Triangulation: establishing the validity of qualitative studies. EDIS **2011**(8), 3 (2011)

Hanafizadeh, P., Ravasan, A.Z.: An investigation into the factors influencing the outsourcing decision of e-banking services. A multi-perspective framework. J. Glob. Oper. Strat. Sour. **10**(1), 67–87 (2017)
ISO: ISO 37500:2014 Guidance on outsourcing. International Organization for Standardization, Geneva, Switzerland (2014)
Janssens, D.: Natural language processing in requirements elicitation and requirements analysis: a systematic literature review. Department of Information and Computing Sciences, Utrecht University (2019)
Jorgensen, C.: Offshore supplier relations: knowledge integration among small businesses. Strat. Outsourc. Int. J. **3**(3), 192–210 (2010)
Kabiraj, T., Sinha, U.B.: Strategic outsourcing with technology transfer under price competition. Int. Rev. Econ. Finance **44**, 281–290 (2016)
Kang, Y., Cai, Z., Tan, C.-W., Huang, Q., Liu, H.: Natural language processing (NLP) in management research: a literature review. J. Manag. Anal. **7**(2), 1–34 (2020)
Kvale, S.: Doing Interviews: The SAGE Qualitative Research Kit. SAGE Publications, Inc., London (2007)
Lin, Y.M.: Data leakage in ICT outsourcing: risks and countermeasures. J. Inf. Commun. Technol. **9**, 87–109 (2010)
Lioliou, E., Willcocks, L.P.: Exploring outsourcing, governance, and discourse. In: Global Outsourcing Discourse: Exploring Modes of IT Governance, pp. 1–19. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-74045-4_1 (2019)
Martinez-Noya, A., Garcia-Canal, E., Guillen, M.: International R&D service outsourcing by technology-intensive firms: Whether and where? J. Int. Manag. **18**(1), 18–37 (2012)
Mason, M.: Sample size and saturation in PhD studies using qualitative interviews. Forum Qual. Soc. Res. **11**, 3 (2010)
Mathews, S.M.: Explainable artificial intelligence applications in NLP, biomedical, and malware classification: a literature review. In: Arai, K., Bhatia, R., Kapoor, S. (eds.) Intelligent Computing, pp. 1269–1292. Springer (2019)
Moiseev, A.: How Outsourcing Creates Cybersecurity Budget, Expertise Options. Channel Futures, channelfutures.com. viewed 21 February 2020 (2020)
Moradlou, H., Fratocchi, L., Skipworth, H., Ghadge, A.: Post-Brexit back-shoring strategies: What UK manufacturing companies could learn from the past? Prod. Plan. Control. https://doi.org/10.1080/09537287.2020.1863500 (2021)
Myers, M.D., Newman, M.: The qualitative interview in IS research: examining the craft. Inf. Organ. **17**(1), 2–26 (2007)
Na Sakolnakorn, T.: The good aspects of managing an organization with an outsourcing and subcontracting strategy. Int. J. Manag. Inf. Syst. **15**(3), 11–17 (2011)
Nassimbeni, G., Sartor, M., Dus, D.: Security risks in service offshoring and outsourcing. Ind. Manag. Data Syst. **112**(3), 405–440 (2012)
Pitropakis, N., Panaousis, E., Giannetsos, T., Anastasiadis, E., Loukas, G.: A taxonomy and survey of attacks against machine learning. Comput. Sci. Rev. **34**, 100199 (2019)
Plotkin, D., Tweardy, R.J.: Global Outsourcing survey Deloitte, Online report (2018)
Premuroso, R.F., Skantz, T.R., Bhattacharya, S.: Disclosure of outsourcing in the annual report: causes and market returns effects. Int. J. Account. Inf. Syst. **13**(4), 382–402 (2012)
Qiu, S., Liu, Q., Zhou, S., Wu, C.: Review of artificial intelligence adversarial attack and defense technologies. Appl. Sci. **9**(5), 909(2019)
Quaglietta, J., Alvord, D.: Coronavirus Impact on Service Delivery Continuity, Employees and Customers. Gartner Information Technology Research. viewed 12 March 2020 (2020)
Rogers, E.M.: Diffusion of Innovations, 5th edn. Free Press, New York (2003)
Russell, R., Kim, L., Hamilton, L., Lazovich, T., Harer, J., Ozdemir, O., Ellingwood, P., McConley, M.: Automated vulnerability detection in source code using deep representation learning. In: 17th International Conference on Machine Learning and Applications, IEEE, pp. 757–762 (2018)
Sadat, M.N., Aziz, M.M.A., Mohammed, N., Pakhomov, S., Liu, H., Jiang, X.: A privacy-preserving distributed filtering framework for NLP artifacts. BMC Med. Inf. Decis. Mak. **19**, 1 (2019)
Schneider, S., Sunyaev, A.: Determinant factors of cloud-sourcing decisions: reflecting on the IT outsourcing literature in the era of cloud computing. J Inf Technol **31**(1), 1–31 (2016)
Shropshire, J.: Natural language processing as a weapon. In: Proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy, AIS Electronic Library (AISeL) (2018)

Słoniec, J., González Rodriguez, R.: Reasons of using IT outsourcing (ITO)—polish-Spanish cross-cultural analysis. Found. Manag. **10**(1), 113–122 (2018)
Snowden, J., Fersht, P.: The HFS market index–IT services and BPO market size and forecast 2016–2020. HFS Research, Boston (2016)
Tarsh, S., Tweardy, R., Smith, J., Plotkin, D., D & Kinsella, D.: Global Outsourcing Survey. Deloitte, Online report (2016)
Truong, T.C., Diep, Q.B., Zelinka, I.: Artificial intelligence in the cyber domain: offense and defense. Symmetry **12**(3), 410 (2020)
Wang, C.J., Ng, C.Y., Brook, R.H.: Response to COVID-19 in Taiwan. JAMA **323**(14), 1341 (2020)
Wang, M.-M., Wang, J.-J.: How vendor capabilities impact IT outsourcing performance. J. Enterp. Inf. Manag. **32**(2), 325–344 (2019)
Williamson, O.: Comparative economic organization: the analysis of discrete. Adm. Sci. Q. **36**(2), 269 (1991)
Winter, K., Rinderle-Ma, S.: Detecting constraints and their relations from regulatory documents using nlp techniques. In: OTM Confederated International Conferences "On the Move to Meaningful Internet Systems", pp. 261–278. Springer (2018)
Wulf, F., Strahringer, S., Westner, M.: Information security risks, benefits, and mitigation measures in cloud sourcing. In: 21st Conference on Business Informatics, IEEE, pp. 258–267 (2019)
Yin, R.K.: Case Study Research: Design and Methods, 5th edn. SAGE Publications, Inc., Thousand Oaks (2014)
Youssef, A.E.: A framework for cloud security risk management based on the business objectives of organisations. Int. J. Adv. Comput. Sci. Appl. **10**(12), 186–194 (2019)
Yuan, Y., Chu, Z., Lai, F., Wu, H.: The impact of transaction attributes on logistics outsourcing success: a moderated mediation model. Int. J. Prod. Econ. **219**, 54–65 (2020)
Zalnieriute, M., Churches, G.: Rejecting the Transatlantic outsourcing of data protection in the face of unrestrained surveillance. Camb. Law J. **80**(1), 8–11 (2021)
Zhang, N., Mi, X., Feng, X., Wang, X., Tian, Y., & Qian, F.: Dangerous skills: Understanding and mitigating security risks of voice-controlled third-party functions on virtual personal assistant systems. In: Symposium on Security and Privacy, IEEE, pp. 1381–1396 (2019)