An Empirical Investigation of the Relationship Between Business Process Transparency and Business Process Attack

Alhanouf Aldayel[1], Dr. Ahmad Alturki[2]
College of Computer and Information Science
King Saud University, Riyadh, Saudi Arabia

***Abstract*—Business Process Management (BPM) is a management approach to discover, analyze, redesign, execute and monitor business processes. Implementing BPM concepts help and benefit organizations by increasing their productivity, achieving their strategies and operational excellence, and saving costs. Rosemann et al. identify business process transparency as one of the key values of BPM, and essential to achieving other BPM benefits. Business process transparency provides visibility about how operations/activities are conducted in a detailed way, sometimes with technical details, within an organization; which facilitates the identification of structural issues of the process model. A conducted content analysis of the literature shows that fraudsters have leveraged structural issues of the business process model to commit fraud. Such fraud can be labeled as a Business Process Attack (BPA). In analogy to information system security attack, BPA can be defined as the exploitation of a vulnerability in a business process model to commit fraudulent activities that influence the business negatively such as achieving invalid or unwanted results. This research aims to investigate the relationship between the degree of business process transparency and exposure to BPA. If the relationship is positive, appropriate security controls shall be implemented on the business process transparency to avoid BPA. The main research question is: What is the relationship between an organization's degree of business process transparency and exposure to BPA. A quantitative research method is employed to measure and understand the impact of business process transparency on BPA. An experiment is designed and conducted to assess the awareness of the existence of vulnerabilities in various process models and how to exploit them to commit BPA. Results show that there is a positive significant relationship between increased business process transparency and exposure to BPA. This research contributes towards understanding and highlights the negative impact of business process transparency, which motivates researchers to investigate this phenomenon and find appropriate solutions.**

Keywords*—Business Process Management (BPM); business process; transparency; business process attack; fraud

I. Introduction

Business Process Management (BPM) is “a body of methods, techniques and tools to discover, analyze, redesign, execute and monitor business processes " [1,p. 5]. A business process is a set of logically related activities performed to achieve the desired business outcome. Business processes are managed by BPM, which is an essential management guide for organizing and managing business processes using well-known methods, techniques, and tools to manage business processes [1]. BPM is applied by a defined sequence of activities known as the BPM lifecycle. It consists of six stages: process identification, process discovery, process analysis, process redesign, process implementation, and process monitoring and controlling [1].

The BPM approach is becoming widely adopted, and BPM research has become interested in analyzing the perceived effects of applying such an approach. BPM aims to achieve both strategic and operative organizational goals [2]. It helps organizations in increasing their productivity, achieving operational excellence, and saving costs [3].

Recent research by Rosemann et al. [4] introduced the value-driven BPM framework, which consists of seven values. The first six values are grouped as three pairs of opposing values that alleviate three classical business conflicts (efficiency–quality; agility–compliance; and integration–networking). The seventh value is transparency, which Rosemann et al. consider as the core value of BPM, and provides visibility into an organization's operations.

Transparency in BPM provides visibility regarding how operations are conducted and enhances decision-making processes in organizations[4]. In their work Rosman et. Al.

Mentioned that a process model repository can be published via various channels like an intranet. However, they did not mention publishing to external parties specifically. A study by Kohlbacher et al. [5] shows that higher transparency facilitates the identification of problems in a business process. Because process transparency entails the transparency of process weakness such as structural issues in the process model if there are any.

Structural issues can constitute an opportunity enabling fraudsters to commit fraudulent activities. A literature review shows several fraud cases that originate from the exploitation of different vulnerabilities in process models. For instance, the Swiss bank UBS had a loss of approximately two billion US dollars due to a structural issue of the process model [6]. In Europe, processes that include "forward-settling" exchange-traded funds (ETF) cash options do not issue confirmations until after settlement has taken place. Fraudsters use this vulnerability in the process to receive payment for a trade before the transaction is confirmed. While the cash cannot be simply retrieved, the seller may still show the cash on their books and possibly use it in further transactions. This allowed

for a recursive series of transactions, creating an ever-growing snowball. Such fraud cases can be considered as instances of business process attack (BPA).

In analogy to information system attack which is defined as the act of exploiting a vulnerability in a controlled system to damage or steal an organization's information or physical asset [7], researchers of the current study define BPA as 'the exploitation of a vulnerability in a business process model to commit fraudulent activities that influence the business negatively'. To avoid attacks ,organizations need to be aware of situations that lead to attacks which then secures themselves with appropriate security controls.

The current study aims to investigate the relationship between business process transparency and BPA. If the relationship is positive, appropriate security controls shall be implemented on the business process transparency to avoid BPA. The main research question is: What is the relationship between an organization's degree of business process transparency and exposure to BPA.

II. Literature Review

A. BPM Security

BPM security aims to provide sound guarantees regarding adherence to security, privacy, and regulatory compliance requirements. Security must be seamlessly integrated and applied to business processes at every stage of the BPM lifecycle. To achieve BPM security organizations, need to understand where and when security requirements are required. The security extended enterprise meta-model is used for this purpose. The model divides BPM security into three layers: the business layer, the application layer, and the infrastructure layer (Figure 1). The business layer defines the business processes and organizational structure to be followed. The application layer defines the security needed by the services and the data schemas required for the execution of the business processes. The infrastructure layer defines the security needed for the software and hardware to automate the execution of business processes[6].

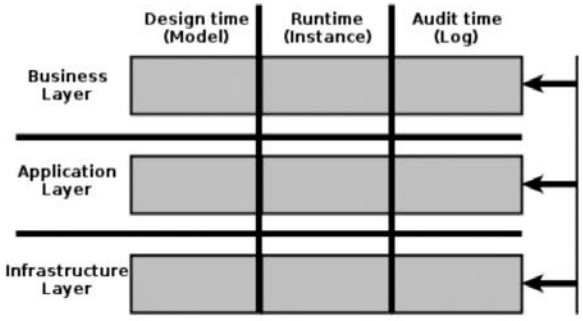

Fig. 1. Security Extended Enterprise Metamodel [6].

Business process security must consider security each of the three layers. Each layer is divided into three stages according to the timepoint and entity where they act. Design time is concerned with process models, the runtime is concerned with process instances, and audit time is concerned with event logs. Both the application layer and infrastructure layer have been heavily investigated; however, the business layer is a relatively new and challenging area for research. Such research focuses on business process design time security; the security of the process model is investigated before the actual runtime of the business process instances[6].

1) BPM security requirements: To ensure the required level of security, organizations shall enforce certain security requirements. Current BPM security requirements focus on design and runtime, and can be classified into the following general types [6, 8]:

- Need-to-know: participants should access only the needed sensitive data to execute their tasks.
- Authorization: access control is needed to ensure that only authorized roles can execute activities within a process. This requirement is usually achieved with Role-Based Access Control RBAC.
- Usage control: to monitor conditions that must hold after the access to a resource e.g., the maximum number of access to a resource this requirement can be used to monitor the compliance to regulatory policies and data protection requirements.
- Separation of duty: constraints on process execution are needed to limit the abilities of participants to execute tasks, eventually reducing the risk of fraud e.g., some activities in a process cannot be executed by the same subject or by the same role.
- Binding of duty: In contrast, to the separation of duties, this requirement enforces some activities to be executed by the same subject or by the same role. This requirement helps to ensure the integrity of data.
- Isolation: Data must stay confidential during the execution of a process.

2) Gaps in Business Process Management (BPM) Security: To maintain Business Process management (BPM) security, organizations need to be aware of security threats, and appropriate security controls shall be implemented. Current business process security controls focus on the optimal assignment of subjects, roles, and activities in a Role-Based Access Control setting. In RBAC, each subject acting in a role should only have the minimal permissions necessary to execute the process, and all the assignments that lead to more rights should be prohibited. Such control is designed to prevent Business Process Attacks (BPA) by checking preciously defined security requirements during process execution[9, 10]. However, BPA can occur flowing the Standard Operating Procedures (SOP) and without any violation of security requirements. The attacks happen using existed vulnerability the business process model structure and become possible by only viewing the business process model. Most organizations do not pay attention to the secure sharing of business process models. And publish them through organizations' intranet. The models are published in an understandable and intuitive format to ensure that business processes are well accepted by the users[10]. organizations

shall pay more attention and only share process models to the intended audience, to reduce the possibility of exposure to BPA.

B. Transparency

The literature shows that there are many definitions of transparency. Some researchers define transparency using a descriptive approach, while others are using a normative approach. Oliver defines transparency using the descriptive approach using three elements: an observer, the object to be observed, and a way of observation. Moser takes a normative approach to define transparency: "to open up the working procedures not immediately visible to those not directly involved to demonstrate the good working of an institution" [11, p.258]. The normative approach does not only describe what transparency is but also what is needed for it to be achieved [11].

The variation in the definitions of transparency does not only come from the definition type but also from the context in which it is being used. For example, In the context of strategic alliances, Ackerman et al. define transparency as "sharing data regarding current order and production statuses as well as plans and forecasts with various supply chain partners" [12, p.4]. In the context of financial markets, Madhavan et al. define it as the "ability of market participants to observe information about the trading process" [12, p.4]. In the context of organizational governance, Potosky defines transparency as the “extent to which a communication medium facilitates a clear or unobstructed communication exchange” [12, p.4]. In the context of the electronic market, it is defined as the “degree of visibility and accessibility of information” [12, p.4].

There are some efforts to generalize the definition of transparency. For example, Davis defines transparency as “lifting the veil of secrecy” [11, p.258]. Hood defines it as “openness to public scrutiny” [13, p.5]. Such definitions are typically broader in scope; however, they do not specifically indicate all the elements of transparency. Schnackenberg et al. [12] have studied transparency definitions through the literature, concluding with a general definition of transparency: “Transparency is the perceived quality of intentionally shared information from a sender” [12, p.5]. Based on this definition, they suggest a conceptualization of transparency by examining the quality of information using three primary manners: disclosure, clarity, and accuracy.

Disclosure means: “the perception that relevant information is received in a timely manner” [12, p.9]. Disclosure implies that information must be openly shared for it to be considered transparent. Researchers see disclosure as a central dimension of transparency. Pirson et al., [12] for example, measure transparency as a stakeholder’s perception that firms openly share all relevant information. Perotti et al. [12] suggest that perceptions of transparency are built around a stakeholder’s ability to gather the necessary information about a firm. Williams [12]describes discloser in four processes: analysis, interpretation, documentation, and communication—in analysis, the target audience is identified; in interpretation, the relevant information for the audiences is determined; in documentation, the relevant information is documented; and in communication, information is distributed to internal and external audiences. Documentation and communication are associated with the open release of information, while analysis and interpretation are important to distinguish relevant from irrelevant information [12].

Clarity means “the perceived level of lucidity and comprehensibility of information received from a sender” [12, p.9]. The information must be understandable to be considered transparent. Complicated mathematical algorithms cannot be considered transparent even if highly disclosed. Daft and Lengel find that a major problem for transparency is a lack of informational clarity rather than a lack of data sharing (disclosure) [12]. Rawlins [14] argues that transparency is not only achieved by disclosure but also by increasing understandability. In this statement, Gower highlights that transparency implies an increase in the understanding of parties who are interested in the actions or decisions of an organization [14].

Accuracy means “the perception that information is correct to the extent possible given the relationship between sender and receiver” [12, p.10]. Information cannot be considered transparent if it is biased or incorrect. Bushman et al. suggest that information must be valid for it to be considered transparent [12].

1) Organizational transparency: Nowadays, transparency is an unambiguously positive concept. Without transparency, the actions of organizations cannot be monitored. To ensure organizations comply with the law and public interest, organizations need to be transparent [15]. Higher organizational transparency improves the image of an organization in the global market and toward the public [1]. Organizations benefit from organizational transparency by improved organizational efficiency and the effectiveness of the decision-making process [14]. It also plays an important role in facilitating business globalization. Transparency provides customers with the confidence they need when dealing with foreign companies that obey other countries’ laws. Moreover, providing information disclosure has a positive relationship with organizational performance. And is an enabler for observability, accountability, certainty, and better conduct[16].

Transparency is categorized into many types based on different perspectives. Based on the type of information in question, Heald divides transparency into event transparency and process transparency. Event transparency provides information about what organizations achieve in the form of inputs, outputs, and outcomes (i.e., organizational performance reports). Process transparency provides information about how organizations achieve this outcome (i.e. governmental transformation process) [17].

Bannister et al. [13] proposed a modified version of Heald's model to adapt it to computer-mediated transparency. The new E-transparency model consists of three categories: data transparency, process transparency, and decision/policy transparency. Similar to event transparency, data transparency is concerned with what organizations are doing. Facts and figures are used to provide data transparency. Process

transparency is concerned with how organizations are working. The steps of organizational processes should be clarified for them to make the process transparent. Decision/policy transparency is concerned with why organizations are doing their work in a specific way. An organization must justify its decisions to be decision transparent.

Heald also categorizes transparency according to its direction—upwards/downwards (a vertical dimension), and inwards/outwards (a horizontal dimension). The vertical dimension transparency goes through organizational hierarchy directions. In the downward direction, managers will be able to monitor their employees' actions. If the relation is symmetric, the upward direction will allow employees to view their managers' actions. The vertical dimension addresses an organization's internal transparency, whereas the horizontal dimension addresses an organization's external transparency. In an inward direction, an organization's internal actions can be seen from the outside. In an outward direction, the organization can see external actions. An organization is said to have full symmetric transparency when all dimensions are present at the same time [18].

2) BPM transparency: A key value of adopting Business process management (BPM) is providing an organization with business process transparency which provides visibility about how operations/activities are conducted in a detailed way[4]. Business process transparency is essential to achieve other BPM values such as agility, quality, networking, integration, efficiency, and compliance[4]. The use of computer systems to manage business processes empowers business process transparency and allows organizations to achieve high organizational transparency i.e. data transparency, process transparency, and decision/policy transparency [4].

3) Business Process Model Abstraction (BPMA): Business Process Model Abstraction (BPMA) is a technique applied to detailed process models to produce generalized versions of the process model[19]. Two main methods are used to apply BPMA: elimination and aggregation. Elimination omits some process model elements of the detailed version to generate the abstracted version. While aggregation groups related process elements of the detailed version to generate an abstracted version. Both methods hide certain activities of the abstracted version and hence reduce process transparency. BPMA shall assure that the resulted abstract process model is well-formed and maintains the original process semantics[20].

BPMA is conducted by applying a set of atomic abstractions are on the initial detailed model. An abstraction is a function that takes a process model as an input and produces a process model as an output. Based on selected criteria, each abstraction hides some process details and brings the model to a higher degree of abstraction. individual abstractions can be combined and afterward controlled to deliver the desired abstraction level[20]. Selecting abstraction criteria can be based on roles activity frequency or activity completion time, or structural aspects of a process model[19].

Moreover, abstraction criteria can be based on functional aspects such as sequential, block, and loop abstractions. Sequential abstraction replaces a sequence of tasks and events by one aggregated function[20]. In Block abstraction, a process fragment in the model enclosed between connecters is replaced with one function. The replaced fragment usually represents parallelism or a decision point in a process. In loop abstraction, Iterated tasks are replaced with a loop construct iterated for successful process completion. In a process model, the fragment to be repeated is enclosed into a loop construct.

C. Fraud

Fraud is defined as the art of deception for gain. Fraud is always intentional. According to Brenner, when someone commits fraud, four elements are present: the perpetrator communicates false statements to the victim, the perpetrator communicates what they know are false statements with the intent of defrauding the victim, the perpetrator's statements are false, and the victim is defrauded out of something of value [21].

According to the fraud triangle theory, fraud occurs in a situation where three components are present: opportunity, pressure, and rationalization. Opportunity refers to the opportunity for the perpetrator to commit fraud (i.e. the lack of internal controls creates an opportunity). Pressure refers to the motivation or driving force behind committing fraud (i.e. personal financial need could cause pressure). Rationalization refers to the fraudsters' justifications for the fraudulent activity using cognitive reasoning. Fraudsters rationalize fraud to consider their act acceptable [22].

1) Organizational fraud: In organizations, fraud can be categorized into two main categories. The first category is fraud committed by organizations regarding their financial reporting—i.e., when they use false financial reports to intentionally defraud investors and third parties to benefit the organization. An example of this category is financial statement fraud. Here, organizations intentionally misstate figures and make false disclosures in financial reports to deceive financial statement clients.

The second category is the fraud perpetrated against an organization that results in harm to the organization itself. An example of this category is employee fraud. This fraud includes the theft of cash or inventory, skimming revenues, and payroll fraud [23]. The fraud against the organization can be committed either internally by employees, or externally by someone who's externally related to the organizations such as suppliers, and other parties [24]. Both profit and non-profit organizations are susceptible to both categories of fraud [25].

2) BPM fraud: Organizations adopting a BPM approach are not excluded from being susceptible to organizational fraud. Fraud related to the business process is known as process-based fraud (PBF) and is enabled by deviations from standard operating procedures (SOP). It can be detected by analyzing deviations in throughput time such as duty sequences, wrong duty decisions, or wrong duty combinations. Process execution information is usually stored in an event log. This information includes events, originators, and time

stamps. Control flow analysis can be used to analyze process information patterns from event logs. Cases, where the fitness function is small, are considered as noise. This noise is identified as suspicious PBF.

Process-based fraud causes deviations from the process model. However, fraud cases can occur even during the normal flow of running processes. An example is a case of fraud in one of the leading finance companies in Sri Lanka. A fraud case was detected during an audit check. It was found that several returned checks for different clients in a specific branch were issued from the same checkbook owned by a marketing officer working in the branch. The marketing officer is responsible for initiating the contracts of returned checks. The marketing officer created personal agreements with clients whereby the client would pay in cash in advance to get a discount, and the marketing officer would subsequently invest the money for personal benefit and earn a return. In this case, the fraud did not cause the organization any financial loss; however, it could damage the reputation of the organization [26]. Additionally, the Swiss bank UBS had a loss of approximately two billion US dollars due to the use of "forward-settling" ETF cash positions [6].

In Europe, processes that include ETF do not issue confirmations until after settlement has taken place. This vulnerability in the process model can be exploited by a party to receive payment for a trade before the transaction is confirmed. While the cash cannot be simply retrieved, the seller may still show the cash on their books and possibly use it in further transactions. This will allow for a recursive series of transactions, creating an ever-growing snowball.

In both cases, the fraudster exploited a vulnerability in the process model to commit the fraud. In the case of the finance company, an absence of internal controls and policy in the case of checks returned enabled the fraudster to commit the fraud, while in the Swiss bank UBS, weak process design allowed the fraud to be committed. Eventually, the fraud in both cases affected the organizations negatively.

More fraud cases can happen without deviation in SOP, a case of a man in China clearly explain how weakness in the process structure enables fraudsters to commit such fraud. The man purchased one First class airline ticket, and used it to have a year of free meals! The man just used his ticket as a regular traveler to have a meal in the first-class lounge; however, instead of getting in the flight, he kept rescheduling his flight to another day. The man will show up on the rescheduled date in the lounge with a newly issued ticket, eat his meal, and reschedule his flight again! Airlines staff discovered that the man rescheduled the same ticket over three hundred times in a year. Moreover, when the airlines started investigating the fraud, the man simply canceled his ticket before the expiration date and had a full refund [27]. Such fraud cases involve more risk as they are harder to detect by organizations.

It is important to define a broader scope of process fraud that combines fraud that causes deviation in the SOP, as in PBF cases, and those that occur without causing such deviation. In both cases, the action of exploiting vulnerabilities to commit fraud is similar to an information system security attack. An attack is a deliberate act to exploit a vulnerability in a controlled system to damage or steal an organization's information or physical asset. Both process fraud and security attacks exploit a vulnerability and affect organizations negatively; however, the entities that are vulnerable to exploitation differ. In the case of fraud, the targeted entity is the business process, whereas, in an information security attack, it is the system. The author uses the term business process attack (BPA) to describe this act.

D. Transparency and Fraud

Transparency is nowadays an unambiguously positive concept. It ensures an organization's compliance with the law and the public interest. Higher transparency improves the image of the organization in the global market and toward the public [28]. Transparency helps organizations to improve the efficiency and effectiveness of their decision-making process [14]. It also plays an important role in facilitating business globalization by providing customers with the confidence they need when dealing with foreign companies that obey other countries' laws. Most of the published research within organizational transparency focus on its positive effects.

Rosemann et al. consider business process transparency as the core value of BPM, which provides visibility into an organization's operations [4]. Previous research shows that higher transparency facilitates the identification of problems in business processes to organizations. Such Identification help organization to optimize the weakened business processes. A study by Kohlbacher et al. [29] included 44 process-oriented firms; the results showed that process orientation leads to higher transparency, which enhances the identification of organizational problems and their causes. Malinova et al. [30] studied reasons for BPM adoption, finding that considerable numbers of organizations adopted the BPM approach mainly for identifying process weaknesses; they argue that without BPM practices, this would be more difficult or even impossible [29]. However easy identification of process weaknesses can facilitate fraud. According to Wells et al. [31], fraud is commonly committed by people who know the weaknesses and how to exploit them best.

Just as in the case of software programming, source code transparency in Open-Source software gives both attackers and defenders the analytic power to do something about known source code vulnerabilities, however, If the defender didn't improve security or eliminate vulnerabilities, Attackers will be able to use them in malicious attacks [32].In the same way, process transparency provides visibility to process weaknesses which constitute vulnerabilities that can be used to commit fraudulent activates. If organizations did nothing about discovered vulnerabilities, a fraud opportunity exists and is available to fraudsters. According to the fraud triangle theory, fraud occurs in a situation where three components are present: opportunity, pressure, and rationalization [22].

E. Related Work

Wehmeier et al. analyzed several published research studies on transparency, and find that more than half of them focus on its positive impact [14]. Research calls upon organizational transparency focused on its relationship with trust. Researchers find that increased transparency increase employees' trust in

their organizations [33]. Moreover, it helps in creating, maintaining, and repairing confidence and trust in an organization- stakeholder relationships [12]. In their work, Vössing et al. [34] find that organizations can enhance process performance by making process information accessible to their employees.

In the contrast to the widespread belief about its benefits, however, transparency is indeed a double-edged sword [35]. Fewer research studies the negative impact of transparency [14], research shows that increased transparency in buyer–supplier relationships may cause buyer's frustration. In the electronic marketplace, the increased transparency can harden the creation of a close buyer relationship. Because it facilitates the comparison of organizations' products with other competitor's products and causes organizations' products to be commoditized [35]. In the health care field [36], increased process transparency results in a decrease in trust in the health care system. Trust levels were higher among the group given no information about the procedures.

Based on the conducted content analysis of the literature, few number studies focused on the negative impact of increased transparency in BPM; there is a lack of empirical research studies to investigate the relationship between business process transparencies to Business Process attack (BPA). Research on BPM transparency has only discussed its positive impact in terms of decision making and enhancing business process models by understanding business process weaknesses [4, 5]. However, previous research has study the factors which increase the possibility of exposure to a. Process-based Fraud (PBF) - an instance of BPA.

Some characteristics of business process model design have been linked to the possibility of exposure to PBF. Possibility of exposure to PBF increases in business process models that were designed to allow for the skip of some task execution, or the skip of decision and proceed to the next task execution [37]. Moreover, PBF is more likely to occur when a process is allowed to be executed by an unauthorized resource, or when different authorities are given to the same originator. Moreover, the possibility of exposure to PBF has been linked to personal perpetrator behavior. Research findings show that PBF is more likely to occur by perpetrators who are known for their bad behaviors [37].This research studies process transparency as a factor that may increase the possibility of exposure to a BPA.

III. Hypothesis

An opportunity for BPA exists when vulnerabilities such as weak security controls are implemented in a business process. Low process transparency can hide the existence of such vulnerabilities because it provides fewer process details, Moreover, low process transparency limits people's understanding of process details, and hence increases people's trust in business processes [36]. This is because they assume that organizations are implementing high standards, even when they are not doing so [36]. Such an attitude may make people unaware of BPA opportunities because they are assuming high-security controls are implemented. To test this assumption, we need to assess people's understandability of a BPA opportunity, in relation to different levels of business process transparency. Two hypotheses are proposed:

H0: Increased business process transparency does not increase attackers' understandability of a BPA opportunity.

H1: Increased business process transparency increases attackers' understandability of a BPA opportunity.

IV. Experiment Design

For the aim of this study, a single factor experiment is suitable, because it allows investigating the effects of one factor on a common response variable. It also allows analyzing variations of a factor, the factor levels. The response variable, is then, determined by the participants, subjects, in relation to a specific factor level applied to a particular object [38].

The experiment in the current research is designed similarly to the one used in [38] to assess modularity's impact on process understanding. In the experiment, variations of a factor (process transparency degree): The factor levels (high-low) are analyzed. The response variable (level of BPA opportunity understanding) is determined by the participants in the experiment when they interact with different factor levels applied to a particular object (process model). The overall design of the experiment is depicted in Figure 2.

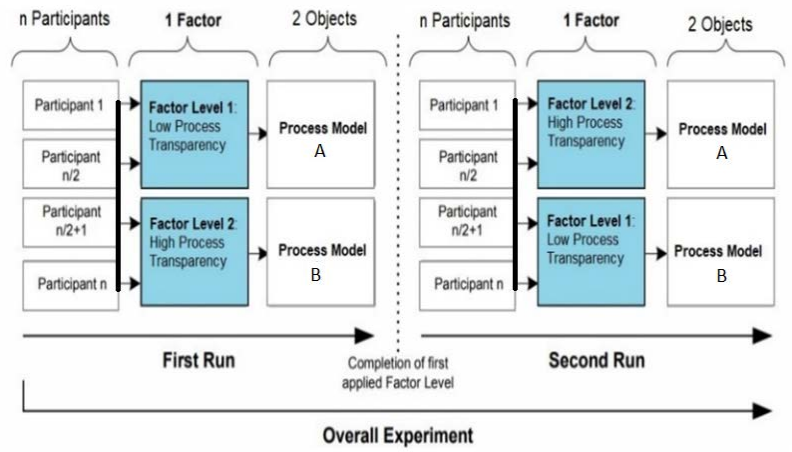

Fig. 2. Experiment Design [38].

V. Experimental Setup

A. Subjects

The subjects are the people who participate in this experiment. The participants are randomly assigned into two runs (previously explained in experimental design). In the first run, half the subjects will be shown two models: high transparency purchase-to-pay process model and low transparency Attend an event model. In the second run. The other half will be shown two different models low transparency purchase-to-pay process model and the high transparency Attend an event model. This way each participant will receive the two different processes (purchase-to-pay and attend an event) in two different transparency degrees (high transparency and low transparency).

B. Objects

The objects to be used in the experiment are different business process models designed with various structural issues. For each process model, two versions are designed with different process transparency levels. The first version is designed with low process transparency and shall include minimal details to understand the business process model. The second version shall be higher in business process transparency, and shall be modeled in detail to make the models more transparent and understandable. The business Process Model Abstraction (BPMA) technique is utilized to generate low transparency versions of the process model [19]. BPMA assures that the resulted process model is well-formed and maintains the original process semantics [20].

Two business processes are selected: purchase-to-pay, and Attend an event, because they are commonly susceptible to fraud. The original process models were re-designed to contain a vulnerability, which represents a common fraud. Figure 3 shows the vulnerable purchase-to-pay business process model. This process allows the staff of a company to request the purchase of goods needed by the company. The process is vulnerable to BPA because no internal controls exist to prevent billing schemes and check tampering. This allows the procurement officer to create fraudulent purchases of goods or services that do not exist, are overpriced, or unnecessary.2.

(Figure 4) shows the vulnerable attend an event process model. This process allows people to buy tickets to attend a specific event. The process is vulnerable to BPA because no checks are done on the attendee's age before entering the event. People over 18 years can illegally use a child's ticket to enter the event. The event organizer will be affected financially and lose money.

C. Factor and Factor Levels

The process transparency degree is the considered factor, with factor levels 'high' and 'low'.

D. Response Variable

The response variable in this experiment is the level of BPA opportunity understanding that the respondents show with respect to the process models, both in their high-transparency and low-transparency versions. To measure the response variable, a specific set of questions are developed for each version to be answered by the participants. The percentage of correctly answered questions by a subject is used as a measure for the participant's level of understanding of BPA opportunity within a particular model. This approach is previously applied in studies to measure process model understandability [39-41].

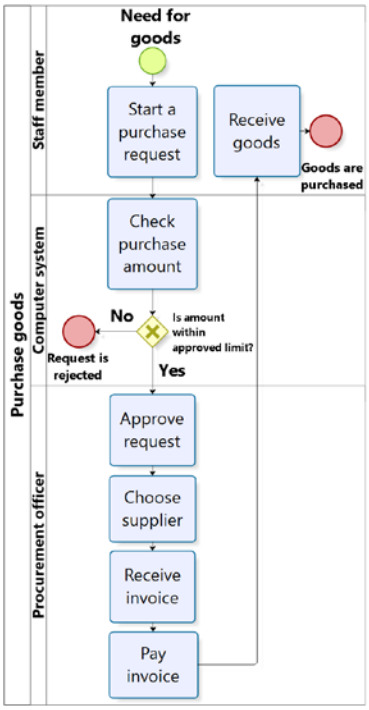

Fig. 3. Vulnerable Purchase-to-pay Process Model (High Transparency).

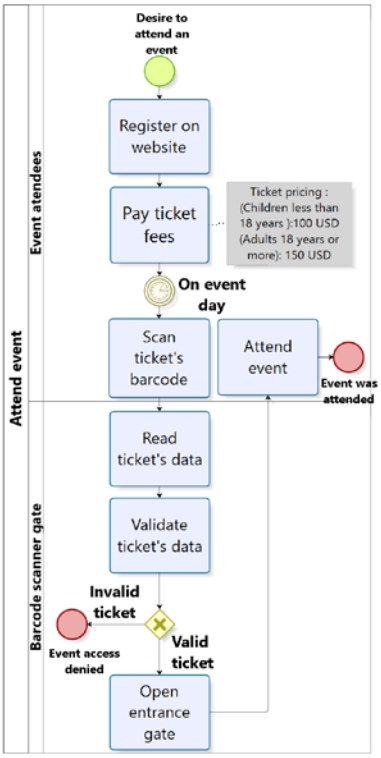

Fig. 4. Vulnerable Attend an Evet Process Model (High Transparency).

E. Instrumentation

The experiment was then carried out e using a surveying website. The participants use their personal computers or mobile phones to view the process models and answer the questions - about BPA opportunity- under each model. The researcher makes sure that the display of the process model fits both personal computer displays and mobile displays. Also, a note is added under each model to guide the participant on how to enlarge models by zooming – in case the model display is unreadable by the participant.

F. Data Collection Method

Various data collection methods are used to conduct research including interviews, experiments, and questionnaires [42]. The current study uses a structured questionnaire as a method for data collection utilizing participants' responses to a structured set of questions [42]. Questions in a questionnaire can be open or closed. Open questions allow respondents to answer on their own [43]. Open questions are used when a researched cannot predict what the responses might be [43]. On the other hand, closed questions allow respondents to choose an answer from a set of alternative answers, which makes answers to be more objective[43]. Questionnaires can be conducted in two ways: interview-based, and self-completed. This research makes use of a web-based self-completed questionnaire because, to reach a large sample, and maintain respondents' confidentiality [42]. The questions are going to be closed questions for more objective responses of respondent's awareness of exposure to BPA.

G. Questionnaire Design

There are two questionnaires used in this research- one for each run. Both questionnaires have the same structure, however, some model-specific questions may differ based on the process models selected in each run.

Each questionnaire is structured as follows: the first part contains a question on different business process models to assess respondent's knowledge about exposure to Business Process Attack (BPA). The second part will collect data about participants' previous experience in the field of BPM.

H. Questionnaire Validity and Reliability

To ensure the validity of the research method, the questionnaire used is built based on knowledge acquired by the researcher in the literature review. The questionnaire is also revived by the researcher's supervisor. And a pilot test has been undertaken. Moreover, guidelines of questionnaire design are taken into account to assure its validity. Five answers are provided for each question to reduce the chance of answering correctly by coincidence. Answers are positively formulated answers because negations distract respondent's attention.

The reliability of collected data is dependent on the integrity of provided answers. To encourage the respondents' honesty and integrity, the researcher uses a simple design and clear structured questionnaire and insures respondent's confidentiality. Moreover, filter questions are added to each model. A filter question is a question on some aspects of the model and is used to make sure the participant had read the model before answering the questions written based on the model. The questionnaire considers only the answers of the participants who answered filter questions correctly, which limits the chance for randomly answering the questionnaire.

I. Data Evaluation

After has been collected, the next step done is data evaluation. It involves tasks editing and coding. Editing is used to ensure that questionnaire results are checked for any potential errors or inconsistencies. Coding is used to define the values of different sets of responses. Coding is important to transform questionnaire results into a format that can be easily fed to analytical tools [27]. Correct Answers are coded as "1", and wrong answers are coded as "0".

J. Sampling Method

A sample is a subset of the population. A well-defined sample should have the same characteristics as the population, if not, then the research results will be wrong [27]. In our study, because Business Process Attack (BPA) assumes that attack can happen by anyone who interacts with process models. The target population can include all people, and the selected sample should represent people from different demographics. However, the participants' experience in process modeling can influence the questionnaire results [44]. Because participants' integrate their previous experience with process model content to construct new knowledge [45], which gives an advantage of an experienced user to gain more knowledge about a process model. To avoid such influence on participant experience, this variable should be randomized.

Another important consideration of sampling is to determine the sample size. The bigger the sample is the greater will be its accuracy [27]. Hair et al. [46], suggest that the minimum sample size is five respondents per variable to be analyzed. In this research, there are two variables in each run (high transparency, low transparency) which makes the minimum participants in each run 10 participants, and 20 participants for the overall experiment.

In this research, the participants will be 200 people randomly assigned into the two experiment runs (previously explained in experimental design). In the first run, half the subjects (100 people) were shown two models: high transparency purchase-to-pay process model and low transparency Attend event model. The great number of participants will increase the accuracy of the experiment results.

K. Data Analysis Method

Data analysis is the interpretation of collected data using different analytical tools. According to the requirements of the management is called analysis. Several tools are used for statistical analysis (such as SPSS and Microsoft Excel). The research makes use T-test to assess the significance of the difference between participants' knowledge in each run of the experiment. The result is demonstrated and interpreted based on knowledge acquired by the researchers [27].

VI. Results

To distill the experiment results, a comparison is conducted between participants' performance for each model in terms of the number of correct answers. This helps us to understand if

more transparency will increase people's understandability of exposure to BPA. The percentage of correct answers for each model variant is calculated; as shown in table 1; the result for the high transparency version is analysed in comparison to the low transparency version for each process model.

TABLE I. AVERAGE PERCENTAGES OF CORRECT ANSWERS FOR EACH MODEL VARIANT

Process model / Transparency degree	Low transparency	High transparency
“Purchase-to-Pay”	38%	44%
“Attend an Event “	43%	51%

A. Purchase-to-Pay Process Model Results

Looking at the results reported in table-1, we can see that when participants are given the low transparency version of the "purchase-to-pay" process model they had correctly answered 38% of the questions about BPA opportunity. This percentage increases to 44% for the participant who had been given the high transparency version of the "purchase-to-pay" process model. To test if this increase is statically significant, a T-test is used.

To use the T-test, two assumptions must be met: data should be normally distributed, and the two samples should have equal variance. first data are explored for each model variant. First, we check if data is normally distributed. Data is normally distributed when the standardized skewness and standardized kurtosis should be within the range of -2 to +2 for each model variant. For the "purchase-to-pay" process model, the actual results of skewness are (1.24, .89), and the results of kurtosis are (-.84, -1.24) for the low transparency model version, and the high transparency model version respectively. Since all values of skewness and kurtosis are within the range of -2 to +2, we can assume that percentage of correct answers for the "purchase-to-pay" process model is normally distributed. Second, the two samples should be tested using F-tests to ensure they have equal variance. Applying F-test with 95% confidence shows that standard deviations of the samples for each of the models are the same. Table 2 shows the results of applying of F-test on purchase-to-pay low transparency business process model and high transparency business process model version.

TABLE II. F-TEST (PURCHASE-TO -PAY BUSINESS PROCESS MODEL)

	Purchase-to-pay high transparency	Purchase-to-pay low transparency
Mean	0.44	0.38
Variance	0.08	0.08
Observations	100.00	100.00
Df	99.00	99.00
F	1.03	
P(F<=f) one-tail	0.44	
F Critical one-tail	1.39	

As T-test assumptions are met for the "purchase-to-pay" process model, we can apply T-test results which generate a P-value for the comparison between process model variants. A P-value lower than 0.05 is considered significant. The T-test results with (P=.13). P-value suggests there is no difference between the high transparency version of the process model and the low transparency version in terms of the average percentage of correctly answered questions on exposure to BPA. We can conclude that the increase in the number of correct answers between the low transparency version of the "purchase-to-pay" process model and the higher transparency one is statically significant.

B. Attend an Event Process Model Results

Looking at the results reported in table-1 above, we can see that when participants are given the low transparency version of the "attend an event" process model they had correctly answered 43% of the questions about BPA opportunity. This percentage increases to 51% for the participant who had been given the high transparency version of the "attend an event" process model. To test if this increase is statically significant, a T-test will be used.

To use the T-test, two assumptions must be met: data should be normally distributed, and the two samples should have equal variance. first data are explored for each model variant. First, we will check if data is normally distributed. Data is normally distributed when the standardized skewness and standardized kurtosis should be within the range of -2 to +2 for each model variant. For the "attend an event" process model, the actual results of skewness are (.45,.1), and the results of kurtosis are (-.48, -1.11) for the low transparency model version, and the high transparency model version respectively. Since all values of skewness and kurtosis are within the range of -2 to +2, we can assume that percentage of correct answers for the "attend an event" process model is normally distributed. Second, the two samples should be tested using F-tests to ensure they have equal variance. Applying F-test with 95% confidence shows that standard deviations of the samples for each of the models are the same. Table 3 shows the results of applying of F-test on the "attend an event" low transparency business process model and high transparency business process model version.

TABLE III. F-TEST (ATTEND AN EVENT BUSINESS PROCESS MODEL)

	Attend an event high transparency	Attend an event low transparency
Mean	0.51	0.43
Variance	0.10	0.08
Observations	100.00	100.00
Df	99.00	99.00
F	1.28	
P(F<=f) one-tail	0.11	
F Critical one-tail	1.39	

As T-test assumptions are met for the "attend an event" process model, we can apply T-test results which generate a P-value for the comparison between process model variants. A P-value lower than 0.05 is considered significant. The T-test results with (P=.06). P-value suggests there is no difference between the high transparency version of the process model and the low transparency version in terms of the average percentage of correctly answered questions on exposure to BPA. We can conclude that the increase in the number of correct answers between the low transparency version of the "attend an event" process model and the higher transparency one is statically significant.

VII. Testing Hypothesis

A. H0: Increased Business Process Transparency does not Increase Attackers' understandability of a BPA Opportunity

To test this hypothesis, we need to assess the P values in regard to the two process models used in the experiment. If the P-value is significant (<=.05) then H0 will be accepted, otherwise, when the P-value is greater than (.05) the H0 will be rejected. Looking at the P values reported in the previous section (5.3), P values are (.13,.06) both "purchase-to-pay" model and "attend an event" process model respectively. we can conclude that H0 is rejected.

B. H1: Increased Business Process Transparency Increases Attackers' understandability of a BPA Opportunity

This hypothesis is the alternative hypothesis of H0 "Increased business process transparency does not increase attackers' understandability of a BPA opportunity." the H1 is accepted when H0 is rejected in vise versa. Since H0 is rejected, we can conclude that H1 is accepted. And we can say that increased business process transparency does increase attackers' understandability of a BPA opportunity.

VIII. Discussion

In general transparency in BPM is a positive value. Transparency is categorized according to its direction. The vertical dimension addresses an organization's internal transparency, whereas the horizontal dimension addresses an organization's external transparency.

Internal process transparency provides visibility about how operations/activities are conducted in a detailed way[4]. Internal Process transparency is essential to achieve other BPM values such as agility, quality, networking, integration, efficiency, and compliance[4]. External process transparency can improve customer relationships. However, transparency is indeed a double-edged sword [35].

Studies show that higher transparency facilitates the identification of problems in a business process. Such identification of process weaknesses can facilitate fraud. According to Wells et al. [31], fraud is commonly committed by people who know the weaknesses and how to exploit them best.

Just as in the case of software programming, source code transparency in Open-Source software gives both attackers and defenders the analytic power to do something about known source code vulnerabilities, however, If the defender didn't improve security or eliminate vulnerabilities, Attackers will be able to use them in malicious attacks [32].In the same way, process transparency provides visibility to process weaknesses which constitute vulnerabilities that can be used to commit fraudulent activates. If organizations did nothing about discovered vulnerabilities, a fraud opportunity exists and is available to fraudsters.

This research aims to investigate the relationship between the degree of business process transparency and exposure to BPA. A single factor experiment is implemented to assess modularity's impact on process understanding. It also allows analyzing variations of a factor (process transparency degree): The factor levels (high-low). Where the response variable (level of BPA opportunity understanding) is determined by the participants in the experiment when they interact with different factor levels applied to a particular object (process model).

Findings suggest that increased business process transparency can constitute an opportunity to commit fraud. The opportunity exists when people understand different vulnerabilities in process models, and who to exploit them the best to commit fraud.

To avoid attacks, organizations need to be aware of situations lead to attack to secure themselves with appropriate security controls.

IX. Conclusion

The research main question is:" What is the relationship between an organization's degree of business process transparency and exposure to BPA?". To Answer the research main question, an experiment was conducted using two process models with different variants "high transparency "and "low transparency. Results show that the high transparency of a process model increases participants' understandability of exposure to BPA. And hence increases the risk of being attacked by BPA.

To achieve the benefits of BPM transparency while avoiding the risk of being attacked by BPA, the researcher recommends the following: Organizations need to follow the BPM security model described in the literature review section and ensure that all their processes are free of structural process vulnerabilities during business process design time. Additionally, suspicious process executions should be detected and prevented by using runtime controls and analyzing event logs. Organizations shall enforce well-known BPM security requirements such as (need-to-know, authorization, usage control, separation of duty, and Isolation when needed. BPM security requirements cover regulatory requirements and privacy and data protection requirements. By doing so the organization reduce vulnerabilities in the process model and hence lowers the risk of being susceptible to BPA. Organizations shall also consider business process model privacy and only share process model design to its intended audience. Moreover, the process model shall be saved in a secure location and not shared or saved out of the organization. In certain cases, when it is needed to share the process models with external parties, process models should be considered as

confidential data and Non-Discourse Agreements (NDA) shall be used.

X. LIMITATIONS

There are some limitations to this research project. The first limitation is in the number of business processes models used during the experiment. Only four process models were considered. The researcher kept the number small to encourage participants to complete the survey and make sure all processes are understood by the participants. For the same reason, the chosen processes were simple, common, business process models. The second limitation is in the research sample. The population was not limited to a specific type or specific characteristics for attackers. There could be other factors that affect the results, however to our best of knowledge, no prior research identifies a special characteristic of business process attackers and anyone can attack a business process.

XI. FUTURE WORK

Future research can be conducted to assess the effect of attackers' experience in BPM and business process model understandability on transparent business process model exposure to BPA. Moreover, In regards to the process mining research area, anomaly detection is not very frequently researched [47]. Future research can focus on using Business Intelligence (BI) for vulnerability detections during design time.

REFERENCES

[1] Dumas, M., Fundamentals of business process management. 1st ed. 2013, New York: Springer.

[2] Meerkamm, S., The Concept of Process Management in Theory and Practice – A Qualitative Analysis. 2010: Springer.

[3] Van Der Aalst, W.M., Business process management: a comprehensive survey. ISRN Software Engineering, 2013. 2013.

[4] Franz, P., M. Kirchmer, and M. Rosemann, Value-driven business process management—impact and benefits. 2011.

[5] Kohlbacher, M. The perceived effects of business process management. in Science and Technology for Humanity (TIC-STH), 2009 IEEE Toronto International Conference. 2009. IEEE.

[6] Müller, G. and R. Accorsi, Why are business processes not secure?, in Number Theory and Cryptography. 2013, Springer. p. 240-254.

[7] Whitman, M.E. and H.J. Mattord, Principles of information security. 2011: Cengage Learning.

[8] Arsac, W., et al. Security validation tool for business processes. in Proceedings of the 16th ACM symposium on Access control models and technologies. 2011. ACM.

[9] Gritzalis, D., et al. Insider threat: enhancing BPM through social media. in New Technologies, Mobility and Security (NTMS), 2014 6th International Conference on. 2014. IEEE.

[10] Brucker, A.D., et al. SecureBPMN: Modeling and enforcing access control requirements in business processes. in Proceedings of the 17th ACM symposium on Access Control Models and Technologies. 2012. ACM.

[11] Meijer, A., Understanding modern transparency. International Review of Administrative Sciences, 2009. 75(2): p. 255-269.

[12] Schnackenberg, A.K. and E.C. Tomlinson, Organizational transparency: A new perspective on managing trust in organization-stakeholder relationships. Journal of Management, 2016. 42(7): p. 1784-1810.

[13] Bannister, F. and R. Connolly, The trouble with transparency: a critical review of openness in e-government. Policy & Internet, 2011. 3(1): p. 1-30.

[14] Wehmeier, S. and O. Raaz, Transparency matters: The concept of organizational transparency in the academic discourse. Public Relations Inquiry, 2012. 1(3): p. 337-366.

[15] Menéndez-Viso, A., Black and white transparency: Contradictions of a moral metaphor. Ethics and information technology, 2009. 11(2): p. 155-162.

[16] Ibini, E. and T. Izims, Effect of Organizational Transparency on Organizational Performance: A Survey of Insurance Companies in Lagos State Nigeria. Journal of Economics, Management and Trade, 2020: p. 52-62.

[17] Meijer, A., Understanding the complex dynamics of transparency. Public Administration Review, 2013. 73(3): p. 429-439.

[18] Heald, D., Why is transparency about public expenditure so elusive? International Review of Administrative Sciences, 2012. 78(1): p. 30-49.

[19] Milani, F., et al., Criteria and heuristics for business process model decomposition. Business & Information Systems Engineering, 2016. 58(1): p. 7-17.

[20] Polyvyanyy, A., S. Smirnov, and M. Weske, Business process model abstraction, in Handbook on Business Process Management 1. 2015, Springer. p. 147-165.

[21] Vaisu, L., M. Warren, and D. Mackay, Defining fraud: issues for organizations from an information systems perspective. PACIS 2003 Proceedings, 2003: p. 66.

[22] Shao, S., What are Some Best Practices for Internal Controls to Prevent Occupational Fraud in Small Businesses? 2016.

[23] Golden, T.W., et al., A guide to forensic accounting investigation. 2011: John Wiley & Sons.

[24] Jans, M., et al., A business process mining application for internal transaction fraud mitigation. Expert Systems with Applications, 2011. 38(10): p. 13351-13359.

[25] Trout, J., Fraudsters, Churches, Economy, and the Expectations Gap: Applying Trends of Occupational Fraud to an Assurance Engagement Team Plan and Fraud-Prevention Client Proposal. 2014, University of Mississippi.

[26] Peiris, M. and U. Rathnasiri, Detection of Occupational Fraud on Leasing Companies. 2016.

[27] Sreejesh, S., S. Mohapatra, and M. Anusree, Business research methods: An applied orientation. 2014: Springer.

[28] Vaccaro, A. and P. Madsen, Firm information transparency: Ethical questions in the information age. Social informatics: An information society for all? In remembrance of Rob Kling, 2006: p. 145-156.

[29] Kohlbacher, M. and S. Gruenwald, Process ownership, process performance measurement and firm performance. International Journal of Productivity and Performance Management, 2011. 60(7): p. 709-720.

[30] Malinova, M. and J. Mendling. A qualitative research perspective on BPM adoption and the pitfalls of business process modeling. in International Conference on Business Process Management. 2012. Springer.

[31] Wells, J.T., Protect small business. Journal of Accountancy, 2003. 195(3): p. 26.

[32] Cowan, C., Software security for open-source systems. IEEE Security & Privacy, 2003. 99(1): p. 38-45.

[33] Rawlins, B.R., Measuring the relationship between organizational transparency and employee trust. 2008.

[34] Vössing, M., et al., Designing useful transparency to improve process performance—evidence from an automated production line. 2019.

[35] Hultman, J. and B. Axelsson, Towards a typology of transparency for marketing management research. Industrial marketing management, 2007. 36(5): p. 627-635.

[36] De Fine Licht, J., Do we really want to know? The potentially negative effect of transparency in decision making on perceived legitimacy. Scandinavian Political Studies, 2011. 34(3): p. 183-201.

[37] Huda, S., R. Sarno, and T. Ahmad, Increasing Accuracy of Process-based Fraud Detection Using a Behavior Model. International Journal of Software Engineering and Its Applications, 2016. 10(5): p. 175-188.

[38] Reijers, H. and J. Mendling. Modularity in process models: Review and effects. in International Conference on Business Process Management. 2008. Springer.

[39] Laue, R. and A. Gadatsch. Measuring the understandability of business process models-Are we asking the right questions? in International Conference on Business Process Management. 2010. Springer.

[40] Recker, J. and A. Dreiling, Does it matter which process modelling language we teach or use? An experimental study on understanding process modelling languages without formal education. ACIS 2007 Proceedings, 2007: p. 45.

[41] Melcher, J., et al. On measuring the understandability of process models. in International Conference on Business Process Management. 2009. Springer.

[42] Saunders, M.N. and P. Lewis, Doing research in business & management: An essential guide to planning your project. 2012: Pearson.

[43] Design, Q., How to Plan, Structure and Write Survey Material for Effective Market Research (Market Research in Practice Series)(Paperback) by Ian Brace; 289 pages. Kogan Page.

[44] Zugal, S., et al. Assessing the impact of hierarchy on model understandability–a cognitive perspective. in International conference on model driven engineering languages and systems. 2011. Springer.

[45] Dikici, A., O. Turetken, and O. Demirors, Factors influencing the understandability of process models: A systematic literature review. Information and Software Technology, 2018. 93: p. 112-129.

[46] Hair, J.F., et al., Multivariate data analysis (Vol. 6). 2006, Upper Saddle River, NJ: Pearson Prentice Hall.

[47] Van Der Aalst, W., et al. Process mining manifesto. in International Conference on Business Process Management. 2011. Springer.