computers

MDPI

Review

Cloud-Based Business Process Security Risk Management: A Systematic Review, Taxonomy, and Future Directions

Temitope Elizabeth Abioye [1], Oluwasefunmi Tale Arogundade [1,*], Sanjay Misra [2], Kayode Adesemowo [3] and Robertas Damaševičius [4,*]

[1] Department of Computer Science, Federal University of Agriculture, Abeokuta 2240, Nigeria; elizatope_2005@yahoo.com
[2] Department of Computer Science and Communication, Ostfold University College, 1783 Halden, Norway; ssopam@gmail.com
[3] School of ICT, Nelson Mandela University, Port Elizabeth 6031, South Africa; kayode@mandela.ac.za
[4] Department of Software Engineering, Kaunas University of Technology, 51368 Kaunas, Lithuania
* Correspondence: arogundadeot@funaab.edu.ng (O.T.A.); robertas.damasevicius@ktu.lt (R.D.)

Abstract: Despite the attractive benefits of cloud-based business processes, security issues, cloud attacks, and privacy are some of the challenges that prevent many organizations from using this technology. This review seeks to know the level of integration of security risk management process at each phase of the Business Process Life Cycle (BPLC) for securing cloud-based business processes; usage of an existing risk analysis technique as the basis of risk assessment model, usage of security risk standard, and the classification of cloud security risks in a cloud-based business process. In light of these objectives, this study presented an exhaustive review of the current state-of-the-art methodology for managing cloud-based business process security risk. Eleven electronic databases (ACM, IEEE, Science Direct, Google Scholar, Springer, Wiley, Taylor and Francis, IEEE cloud computing Conference, ICSE conference, COMPSAC conference, ICCSA conference, Computer Standards and Interfaces Journal) were used for the selected publications. A total of 1243 articles were found. After using the selection criteria, 93 articles were selected, while 17 articles were found eligible for in-depth evaluation. For the results of the business process lifecycle evaluation, 17% of the approaches integrated security risk management into one of the phases of the business process, while others did not. For the influence of the results of the domain assessment of risk management, three key indicators (domain applicability, use of existing risk management techniques, and integration of risk standards) were used to substantiate our findings. The evaluation result of domain applicability showed that 53% of the approaches had been testing run in real-time, thereby making these works reusable. The result of the usage of existing risk analysis showed that 52.9% of the authors implemented their work using existing risk analysis techniques while 29.4% of the authors partially integrated security risk standards into their work. Based on these findings and results, security risk management, the usage of existing security risk management techniques, and security risk standards should be integrated with business process phases to protect against security issues in cloud services.

Keywords: business process; cloud computing; security risk management; business process lifecycle; security standards

Citation: Abioye, T.E.; Arogundade, O.T.; Misra, S.; Adesemowo, K.; Damaševičius, R. Cloud-Based Business Process Security Risk Management: A Systematic Review, Taxonomy, and Future Directions. *Computers* **2021**, *10*, 160. https://doi.org/10.3390/computers10120160

Academic Editor: George Angelos Papadopoulos

Received: 19 October 2021
Accepted: 23 November 2021
Published: 26 November 2021

1. Introduction

Business Process Management (BPM) is a described as a field that merges knowledge from information technology and management sciences to the usefulness of business processes [1]. It is used in the formal presentation of business processes (BPs) for analysis and advancement purposes [2,3]. A business process (BP) is defined as a procedure carried out in a business establishment to obtain good results [4]. The specific purpose of BPM is to adjust business establishment processes to the purpose, objectives of the organization, and objectives that improve effectiveness and bring about competitive benefit [3,5]. The

most effective means of achieving BPM's purpose is to use cloud computing (CC) facilities for business processes. This is because of the resource-based availability of the cloud computing. Cloud computing provides a good and easy environment for all stakeholders in business to meet, rub minds, and invariably, transact business efficiently and in a fast manner [6].

Therefore, cloud computing, according to the National Institute of Standards and Technology (NIST), is a model that allows easy and readily available entry when required; a collection of configurable computing materials (e.g., networks, servers, storage, applications, and services) that are quickly obtained and utilized with little or no assistance from the service provider [7]. Cloud computing is an improved technology with many benefits that makes it vital for running a business. It represents a perfect technological device that can help organizations stay competitive and may be an innovative means of boosting business values. It allows cloud consumers to merge numerous different services, leading to high creativity and productivity. Cloud computing prevents facility costs and helps organizations focus on the main business processes rather than the system infrastructure [8].

As this technology is gaining more ground, cloud computing comes with its shortcomings: security issues, cloud attacks, and privacy. Business organizations should have adequate security on cloud services to protect their data from attackers. Therefore, it is paramount for cloud providers and cloud users to proactively combat these issues and recover from various malicious cloud attacks when such threats succeed (resilience). One of the best approaches to securing cloud-based business processes is the integration of security risk management into the business process life cycle, the usage of existing risk assessment methodologies as the basis of risk analysis for risk prioritization, and the integration of security risk standards. Lack of trust in a cloud services concerning the uncertainties related to its quality level can prevent consumers from adopting cloud technologies [9,10]. Although zero-level risk provision is impossible, an effective and efficient risk management mechanism can provide technological insurance that can pave the way to trust on the cloud consumer's side as well as an economical and secure productiveness of cloud providers' resources on the other side.

The basic concepts and the relationship between business process, cloud computing, and security risk management have been introduced; these three domains were merged to have more productive business process output. These systematic literature review objectives were based on four points: to know (i) the level of integration of security risk management process at each phase of the BPLC for securing cloud-based business processes, (ii) the use of an existing risk analysis technique as the basis of risk assessment model, (iii) the use of security risk standards as a guide in securing cloud-based security risk in business processes, and (iv) the classification of cloud security risks in cloud-based business processes. The motivation for this survey hinged on the fact that cloud computing is seen as the next evolution that will positively influence organization businesses and the management of IT infrastructures. There are numerous benefits of cloud computing, as mentioned, despite its many challenges. Having carried out a survey on these challenges, data security is the most invasive in cloud computing [11–13]. Furthermore, the outcome of a detailed industry-based review [14] revealed that 74% of IT chiefs said that the issue of security is the main cause of the low adoption of cloud computing services' low adoption by many organizations [15].

The survey also revealed that many business enterprises are yet to adopt cloud computing due to security and privacy issues; they are busy studying the pros and cons of these cloud paradigms from afar. Therefore, the need arises to carry out a review on cloud-based business processes that use security risk management processes as a form of security measure for data protection to identify research gaps. This is important due to the presence of security issues that affect business and organizational goals [16]. Here, a systematic review of current literature related to cloud-based business process security risk management is carried out, not only in accordance with the summarization of the

current points regarding this issue, but also to propose a background that can properly serve as an eye-opener to new research work. This systematic review synthesizes current studies in an unbiased way [17–19]. In contrast to the normal way of conducting a literature review, which is not systematically [20], this survey followed a precise and stated series of steps in a manner consistent with a theoretical procedure. This survey was conducted and aimed at a central issue, which represents the main investigation, and was indicated using definite, established, specified, and formal questions. The procedures, the advance plan to obtain the facts, and the concentration of the questions are well detailed to allow other researchers to follow the same practice and arbitrate the suitability of the principle selected for the specific problem [20]. This survey was carried out using the principles of systematic reviews suggested by [17–19]. We also used a template for the review protocol created by [20] that promotes the planning and implementation of the methodical survey in software engineering.

Based on the findings of our literature, there is no review of cloud-based business process security risk management. Most of the surveys focus on incorporating risk management into the business process in the traditional environment. Examples include Jakoubi [21], who presented a study on nine scientific approaches in which they aim to in-corporate risk and/or security areas in business process management. Richardson [22] carried out a survey in which there was a formal meeting with experienced risk managers to find research gaps in the domains of risk management, compliance, and internal control. Suriadi [23] conducted a survey on an existing study in a review, comparison, and gap analysis of risk-aware business process management. The main focus was to establish research gaps in the domain of risk-aware business process management and to propose a research agenda. Meanwhile, Sara and Aguilar-Saven [24] conducted a review of the literature on business process modeling: review and framework. Their survey was centered on business process modeling and the description of major modeling techniques. In addition, a framework for grouping business process modeling methods according to their use was suggested and deliberated on. Thabet [25] proposed an approach to the risk-aware BPM framework using the business process-risk management-integrated method (BPRIM) procedure following the engineering life cycle of the agile modeling method. Lamine [26] suggested an approach to bridge the gap that existed in the use of risk-aware business process management due to its lack of solid scientific foundations and conscientious tooling. Based on their findings, the BPRIM framework was established and a conscientious tool called ADOBPRIM was implemented.

Although the studies mentioned were similar to ours, the scope differs. Jakoubi [21] reviewed research papers dealing with the problem related to "security in business process management (BPM)" and the problem related to "risk in BPM". Furthermore, the scope of Richardson's [22] literature review involved studies on compliance and internal control and risk management. Therefore, this literature survey focused on integrating security risk management into cloud-based business processes, using existing risk assessment techniques and security risk standards to solve security and privacy issues in the cloud.

This study is structured in the following order: the background and related work is presented in Section 2. Section 3 discusses the scope of the systematic review. In Section 4, a literature search procedure is presented. Section 5 explains the research methodology. Section 6 discusses trends and the critical analysis. Finally, the summary and conclusion are set out in Section 7.

2. Background and Related Work

Business process management has generally been used in most organizations recently [27–30]. Business process management helps businesses by providing devices, processes, and techniques to establish and create business processes, analyze these procedures to create opportunities for advancement, implement the enhanced procedures, and monitor and control their implementation [31]. Normally, the business process consists of various organizational features; this includes human resources, business documents, and

technology. A process means how work is performed [3], while work is the physical or mental effort applied to get something done [5]. A process normally has some input that will produce an output; for example, a production line transforms unprocessed materials (taken as input) through its sequential steps into a processed material called a product. According to Mahal's [2] definition, a process is activated by an action regulated by a set of policies based on the right information and implemented using skilled personnel equipped with advanced tools and sustaining infrastructure. Processes are better explained using the amount of money, duration, and product/service features generated from the method, service quality or output of the service produced, and the risks associated with the process. Suppose that the company is not itself an information service provider for outside consumers, the services are provided to meet their needs; therefore, the quality triangle is presented in terms of effectiveness, service price, and the risks involved in the process of sourcing information for services.

Business process management can also be referred to as the traditional business process lifecycle and is similar to the popular Plan-Do-Check-Act approach, as depicted in Figure 1.

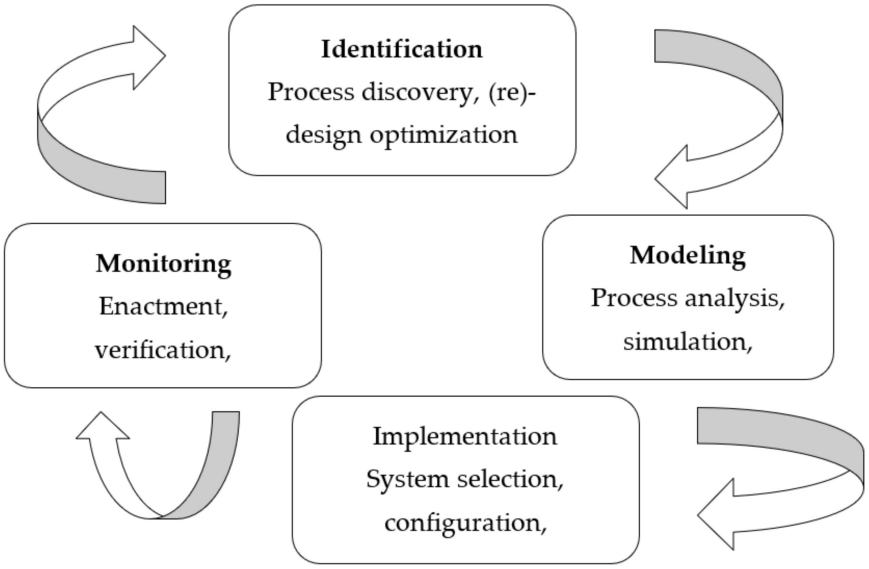

Figure 1. Business Process Management (BPM) life cycle.

An organization using the BPM style usually undergoes a series of stages called the BPM life cycle. Different models of BPM life cycles are available, as discussed by these authors [31,32]. The BPM lifecycle adopted by [33] shall be used in this study. It consists of four stages and they are identification, modeling, implementation, and monitoring. The identification phase has to do with analyzing the organizational and technical environment to uncover individual organizational business processes. It is used in checking and re-molding old procedures to make them more efficient. This is the initial phase of the cycle. The modeling phase is concerned with the graphical representation of the processes to state the informal description explained in the initial phase. Some standard languages permit simulation of the model to uncover a few unwanted execution sequences. Normally, the modeling phase helps to verify the process theoretically. Implementation is the phase where the transformation of the compilation process into a serviceable executable process takes place. It deals with changes in the organization for procedures that have to do with human activities. Concerning IT-dependent processes, it involves the implementation and configuration of software parts. The monitoring phase is a concern with the execution of processes. Monitoring of executed processes is essential for two main purposes. The first is to inspect the compliance of the execution with the initially stated procedures and

the second is to collect data and facts that are needed to begin a new cycle to improve the processes.

Unfortunately, the mode of operation of BPM systems is different from that available in the risk management area [16], resulting in the appearance of security issues that can affect business and organizational goals. One of the good practices in business processes is awareness of security risks, and more so, utilizing proactive risk management against the reactive method of risk treatment is more important. Business process management that incorporates risk management should establish and assess process-related risks specifically during the identification phase and, in addition to aiding in adopting risk aversion methods. In the modeling phase, the emergence of new risks should be constantly monitored. Once a risk event occurs, the right mitigation strategy should be applied to avert the risk. The log output from the implementation of business processes needs to be assessed to establish the event of risks in the executed procedures and understand why the risks occur. However, the ability just explained is under development in the research community and more work is required.

Cloud computing, on the other hand, offers great benefits that satisfy the need for business competitiveness and the realization of business objectives [34]. Cearley [35] defined cloud computing as a model in which modern scientific abilities are resizable, flexible, and offered to final consumers over the Internet. Armbrust [36] defined cloud computing as a collection of interconnected operative services that provide resizable and efficient services and an affordable computing facility that is easily accessible.

Many organizations are planning to deploy their business process to the cloud, whereas some have started enjoying the benefit of cloud-based services. Meanwhile, it is becoming increasingly difficult for organizations to survive in a traditional environment due to limitations in market access time and the rapid response to business demands from clients [34]. In addition, the processing time and cost for high-computing jobs are very high compared to cloud computing that has a reduced processing time and cost due to its architectural design [37]. In lieu of these limitations, it is essential for organizations to showcase their business ideas beyond the traditional environment to achieve competitive benefits. It allows quick modification to resource response to unforeseen requests and changes capital costs in operating payment using the prepaid method. Cloud computing has huge advantages, most importantly in a situation where cost reduction is needed.

Furthermore, the notion of a cloud security risk management procedure is an endless cycle of tasks, collection, collation, analysis, dissemination, and feedback that is similar to the theory of intelligence analysis [8]. A cloud security risk management process should be an active record that stakeholders frequently review, rather than a static record kept on the shelf. The significance of risk management in cloud computing is the need to help stakeholders make informed decisions related to legal agreements.

This survey examined existing research that worked in this domain and established research gaps.

3. Scope of the Systematic Review

To have a manageable scope for the literature survey, some criteria were formulated as a standard for selecting articles to be reviewed. Based on this, several similar works have been excluded while some were extracted. The exclusion and inclusion criteria for this work were listed as follows.

3.1. Inclusion Criteria

- Research publications that dealt with cloud-based security risk management for business process were extracted.
- Research publications with the content of CC security risk challenges/threats were extracted.
- Research publications written only in English language were considered.
- Research publications written and published within the last eleven years were considered.

- Research publications with similar title to our area of review were extracted.
- Research publications that possess common keywords to our specified search strings/words were considered.

3.2. Exclusion Criteria

- Research publications centered on cloud-based SRM were excluded.
- Research publications on security risk-aware business process were not considered.
- Research publications on business intelligence in CC were excluded.
- Research publications on cloud-based SRM "Something-as-a-Service" were excluded.
- Non-English language documented papers were excluded.
- Duplicated publications were excluded.
- Research publications on cloud security and not cloud security risks were excluded.
- Management process-based papers were not considered.
- Research works with the year of publication from 2009 and earlier were not considered.

A short but detailed selection requirement and the resulting list of research works excluded from our survey are explained in the remainder of this section. Table 1 shows the summary of the excluded papers.

Table 1. Summary of excluded papers.

S/N	Exclusion Criteria	Work Excluded
1	Cloud-based SRM centered work	36, 37, 38, 39, 40, 41, 42,43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57
2	Business intelligence in cloud computing	58, 59, 60
3	Cloud-based SRM "Something-as-a-Service"	61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72
4	Non-English language documented papers	73
5	Year of publication	74, 75, 76, 77
6	Cloud security papers	80, 81, 82, 83, 84, 85, 86
7	Management process-based papers	87

We considered papers that incorporate security risk management into the business process in the cloud environment. Therefore, articles that concentrate only on cloud-based security risk management aspects but do not link them with the business process were excluded. Examples of cloud-based security risk-management-centered work, which were excluded from these studies include: "Toward cloud computing SLA risk management: issues and challenges" by Morin et al. [38], @Research on risk evaluation of information security based on cloud computing" by Jiang [39], "A cloud security risk management strategy" by Choo [40], "Modeling risk management in cloud adoption" by Gupta and Saini [41], "Enhanced risk minimization framework for a cloud computing environment" by Razaque et al. [42]. Other works in this category include: Islam et al. [43], Gupta et al. [44], Basu et al. [45], Al-Anzi et al. [46], Aruna et al. [47], Aswin and Kavitha [48], Chang and Ramachandran [49], Dahbur et al. [50], Damenu and Balakrishna [51], Djemame et al. [52], El Kefel and Mohamed [53], Khan et al. [54], Marbukh [55], Albakri et al. [56], Drissi et al. [57], Wu et al. [58], and Xie et al. [59].

Similarly, papers that have to do with business intelligence in cloud computing without the business process activities were excluded. Papers in this category include: "Combining business intelligence with cloud computing to deliver agility in the actual economy" by Mircea et al. [60], "A decision framework model for migration into the cloud: Business, application, security, and privacy perspective" by Islam et al. [61]; "Agile business growth and cyber risk: how do we secure the Internet of Things (IoT) environment" by Griffy-Brown et al. [62].

We also excluded papers whose major contributions were centered on security risk management in the cloud, namely, "Something-as-a-Service". Examples include the following works: "A security as a service solution for the application in the cloud computing environment," by Chen et al. [63], "Security in the cloud: understanding the risks of cloud

as a service," by Peake [64], "On cloud security attacks: a taxonomy and intrusion detection and prevention as a service" by Iqbal et al. [65], "Security risk quantification mechanism for infrastructure as a service in cloud computing platforms," by Fall et al. [66]. Others include: Tang and Liu [9], Hussain and Abdul Salam [67], Senk [68], Al-Qurishi [69], Duan [70], Karadsheh [71], Elsayed and Zulkernine [72], and Benlian and Hess [73]. Although these papers may be somehow related, they were more concerned with the issue of "as-a-service" for security risks in the cloud environment. In brief, these papers have different objectives compared to our literature survey goals.

Papers that were related but were documented in the non-English language were excluded in this survey because they might not be understandable to almost all the scientific world due to language barriers. This includes: "R-BPM: Uma metodologia para gerenciamento de processos de negocios consciente dosriscos", by Ferreira et al. [74].

In addition, some papers were excluded from this literature review based on the year of publication. We were concerned with papers published between the years 2010 and the year 2020 so as to be informed about the current trend in cloud-based business process security risk management. Examples of papers exempted from this survey include: "Security analysis of electronic business process", by Röhrig and Knorr, [75]; "IT security risk analysis based on business process models enhanced with security requirements", by Taubenberger and Jurjens [76]; "The IS risk analysis based on a business model", by Suh and Han [77]; "Integration of risk identification with business process models," by Lambert et al. [78].

In the cloud computing domain, many works have been carried out, especially on the security aspect of the cloud. Our literature survey focus is on secured business processes [79,80] rather than cloud security. Based on this fact, many papers on cloud security have been excluded from this survey. Examples of such papers include Gonzalez [81], Bouayad [82], Almorsy [83], Ogîgău-Neamțiu [84], Saeed [85], Birje [86], and Sumter [87].

Finally, management process-based papers were not considered in this survey as there is no correlation with our review. An example of such work is Gao [88]. Repeated papers downloaded were only considered once.

4. Literature Search Procedure

4.1. Focus

The focus was to:

- Establish research approach and detailed study which consider security risk management in the business process as a means of security measure for cloud-based business process.
- Discover an approach incorporating security risk management in any of the business process management phases deployed to the cloud.
- Establish the incorporation of existing security risk assessment techniques as the basis of their analysis.
- Know whether the security risk standard is integrated in building a secure cloud-based business process.

4.2. Search Quality and Amplitude

Today, some enterprises are trying to adopt cloud services to expand their local facilities and compete in the market to achieve their business objectives. At the same time, a larger number of organizations are afraid to subscribe to cloud services due to security and privacy issues. These challenges are worsened due to the high rate of moving business processes to the cloud, which has to do with a high rate of on-demand application, platform, and infrastructure usage. This movement has contributed to the rise in cyber-attacks that result in security breaches in cloud-based business processes. To avoid these security breaches, the security risk management process presents a better view in this regard. To date, the potential of security risk management to address security challenges in cloud

services has not been fully maximized in business process management. Therefore, our research questions addressed the approaches that have been carried out to secure business processes in the cloud by integrating security risk management.

The keywords and search strings that were used in the composition of these questions and that were useful in this research include:

a. Cloud security.
b. Cloud-based business process security risk management,
c. Business process risk management in the cloud environment.
d. Business process risk-aware systems
e. Business process security risk management
f. Security risk as a service

In this review, the integration of security risk management in the business process to solve cloud-based security challenges was carefully studied. Therefore, the research works that were referenced include those publications that incorporate security risk management into the business process in the cloud. The expected result of this systematic survey is the identification of initiatives that use security risk management in business processes to combat security challenges, and the result shall be the number of identified approaches and research gaps in this area. The major application domains that will benefit from this review include and are not limited to cloud computing, business process management, and information system risk management, as well as security experts, cloud providers, and software experts. A conceptual structure is presented to expose new research areas in security risk management for a cloud-based business process to achieve our goal.

5. Research Methodology

In this section, the search techniques, the sources, the selection of the execution of the studies used, and the selection execution are well explained. More importantly, the review methodology is based on a standard research protocol.

5.1. Selection of Sources Used

The relevant literature was collected in two phases, first in January 2020 and second in October 2020. The first phase involved two literature selection processes that were used to choose strongly related papers. This was done by searching for relevant papers on academic forums and using three renowned learned article web browsers, such as Google Scholar, Scopus, and Web of Science. For the scope optimization of this study, journals that were applicable to the management of some extent of security risk management for cloud-based business processes were selected. In stage two of selection, selected journals were screened by removing articles that were not within the scope of this survey. In the second phase of our selection process, we widened our search by undertaking a process called "backward reference" search. In particular, any applicable journal cited by the articles under review was included in the collection of articles that were evaluated. For literature selection for taxonomy of cloud-based business process security risks, collection was done once and it was carried out during the second phase in October 2020. The same method of searching in academic forums as mentioned earlier was also used. Research publications on cloud-based security risks, cloud security threats, and its challenges were selected. Our literature collection methodology is explained below.

Collections of renowned conferences and journals were carefully searched to choose studies relevant to cloud-based business process security risk management from 2010 to October 2020. Due to the participation of different domains in this study, research papers were collected from many disciplines: business process management, risk management, information security, and cloud computing.

From the individual established groups, the applicable journals were selected by examining their titles to ensure their relevance to the topic under study. For every work that appeared to be relevant, the abstract and the body of the paper were quickly scanned to ascertain the paper's relevance. Articles that passed these checks were included in the

literature list. At the same time, papers whose titles were clearly beyond our research scope were removed from the literature list. This method allowed us to select 93 related journals from more than 1243 journals for cloud-based business process security risk management while 12 papers were selected out of the pool of 36 journals for cloud security risk classification.

After the rigorous evaluation procedure, 47 out of those 93 articles discussed cloud security using the information security risk management procedure having nothing to do with business process management and were considered borderline articles that were not part of the scope of this review as discussed in Section 4; therefore, these papers were excluded. More so, three out of these 93 papers were PhD theses on closely related work, three papers were on "Business Intelligence with cloud computing", and 14 papers discussed cloud computing on "Something-as-a-Service". All these were equally excluded due to exclusion criteria. Nine articles were excluded based on the year of study and the use of non-English language. Table 2 depicts the breakdown of the selected literatures for review.

Table 2. Breakdown of the initial selected papers.

Category of Papers	Number of Papers
Cloud Security based on Information Security Risk Management	47
PhD thesis	3
Business Intelligence with Cloud Computing	3
Excluded Papers based on year of study and other languages except English	9
Cloud Computing "Something-as-a-Service" paradigm	14
Selected Papers due for evaluation	17
Total	93

The forum-based article collection method was complemented with a keyword-based search using web browsers, electronic databases, and manual searches, such as in a particular journal/conference/magazine/book or in research journals given by professionals in the area. Ultimately, the main sources of the initial literature list in which the literature survey execution was run were presented. These include ACM Digital Library, IEEE Digital Library, Science Direct, Google Scholar, Springer, Wiley, IEEE Cloud Computing Conference, ICSE conference, COMPSAC conference, ICCSA conference, Computer Standards and Interfaces Journal, and Taylor and Francis.

5.2. Studies Selection Procedure

The process, criteria, and evaluation method for selecting studies are discussed in this section. This is important to minimize the likelihood of bias; moreover, the selection conditions should be established at the stage of protocol definition. It has been stated that research works should showcase new approaches (11 years backward maximally) and should consider different kinds of security risk requirements in the business process in the cloud environment. Various processes, methods, steps, or descriptions needed as a guide to implement security risk management were stated in the selected studies. Studies that did not focus on security risk management in cloud-based business processes were not considered.

To obtain eligible articles for evaluation, a scrupulous search was carried out in eleven electronic databases with an outcome of 1243 journals. The summary of the distribution is given in Table 3. From the pool of 1243 articles obtained from the indexed databases, 461 articles were found duplicated among the 11 electronic search forums used after the preliminary screening exercise was conducted. Furthermore, 679 articles were equally screened based on the irrelevance of the journal title. Ninety-three articles were found eligible for evaluation after full text-based selection criteria were performed. To round it all up, 10 articles were eliminated due to an undefined methodology.

Table 3. Summary of downloaded publications from electronic databases.

Database	Number of Articles
ACM Digital Library	185
IEEE Xplore	112
Science@Direct	108
Google Scholar	289
Springer	211
Wiley	62
IEEE Cloud Computing conference	80
ICSE conference	47
COMPSAC conference	69
Computer Standards and Interfaces journal	32
Taylor and Francis	48

For cloud security risk taxonomy, research papers on cloud security were not considered. Twelve papers actually treated cloud security risk/threat while the remainder were on cloud security. The classification was done based on the existing procedure found in the literature. Cloud security risk classification is presented in Section 5.5.

5.3. How the Information Was Extracted

The search was conducted to get the first list of studies that were needed for further evaluation. The process of studies selections was used on all other works selected to confirm if the studies obeyed the inclusion and exclusion standards. The information extracted from the selected studies consisted of the following: techniques, methods, processes, steps, strategies, or any other approach to enact security risks management in cloud-based business process management. The information style used for this systematic survey contains identification, methodology, results, issues, general views, and study deductions. Regarding the study methodology, the way security risk management was used to combat security issues in business processes deployed to the cloud was examined in these selected studies. The next subsection summarizes the individual studies, which was based on the information extracted from the information forms.

5.4. Analysis of the Extracted Studies

Goettelman et al., 2014, "Integrating security risk management into business process management for the cloud".

The authors presented work on incorporating risk management with business process management in the cloud. Their main focus was on the integration of risk assessment, which is a procedure supported by business process management. As one of the actors in the cloud, Cloud broker was centered on in the risk assessment to furnish them with the right processes and tools that helped them perform their duties better.

Vijayakumar and Arun, 2017, "Analysis and selection of risk assessment frameworks for cloud-based enterprise applications".

The authors proposed an appropriate risk assessment method for cloud-based enterprises (finance, medical, business). Two main risk assessment frameworks, Common Weakness Risk Analysis Framework (CWRAF) and Common Weakness Scoring System (CWSS), were analyzed against three business domains. They discovered that CWRAF and CVSS were not detailed enough to handle the integrated software development life cycle. This study helped them obtain the right approach and framework that is best for risk assessment in these domains.

Goettelman et al., 2013, "A general approach for a trusted deployment of a business process in clouds".

The authors presented an approach that used modeling methods and cloud selection for secure deployment of a risk-aware business process in a security-prone cloud. They emphasized three main steps for cloud deployment. These steps included the definition of the requirements, the remodeling of the business process, and the selection of cloud. The

research focus was on the categorization of good procedures, which was later used in the implementation of the business process.

Kateeb and Almadallah, 2014, "Risk management framework in cloud computing security in business and organization".

The authors presented a study on security risks and issues related to the usage of cloud computing in businesses and organizations. A risk management framework was implemented using the NIST recommended format for security risks from the provider's side. The aim of this framework was to boost trust between cloud users and cloud providers and generally increase the usage of cloud computing.

Ali et al., 2017 "Cloud-based business services innovation: a risk management model".

The authors carried out a literature review on cloud-based business innovation, which was used to discover the major risks challenging the delivery of Software-as-a-Service (SaaS) to the user and to use innovation in implementing and achieving a notion to solve a particular problem and achieve a result for the organization and the customers. Emphasis was placed on the risks of services, technology, and processes. This category of risks was conceptualized in four areas: stakeholder commitment, technology growth, innovation planning, and innovation control. Finally, this review and the risk strategy model gave insight and tools for risk management in this area.

Vasiljeva et al., 2017, "Cloud computing: business perspectives, benefits and challenges (case of Latvia)".

The authors presented a study to determine the use of cloud computing adoption in boosting the business performance of Latvian small and medium enterprises in different industries. Their main focus was centered on the key elements that encouraged and supported the adoption of cloud computing services in Latvian small and medium enterprises (SMEs) and the future effect of this technology. In this study, the following questions were answered: to what extent are cloud computing services known to Latvian SMEs and how do they use cloud computing services? What is the effect of the usage of cloud computing on business performance? What is the ability and future perception of cloud computing services in Latvian SMEs in a different establishment? Responses to these questions were provided through a detailed theoretical and descriptive mixed-method literature survey. The outcome of this work provided insight and recommendations for SMEs, ICT merchants, service providers, students, and researchers.

Damasceno et al., 2011, "Modeling and executing business processes with annotated security requirements in the cloud".

The authors gave an insightful study on the development of cloud-based model-driven development and implementation area known as the SSC4 cloud, which allows many stakeholders to combine efforts to model business processes with the high-level specification of security requirements about the business process execution environment. This combined effort allowed different industries to reveal and share their business and security skills, which performed the same business tasks inside and outside the company.

Goettelman et al., 2014, "A security risk assessment model for business process deployment in the cloud".

The authors suggested a method for assessing the security risks of the business process prior to its multi-cloud deployment. This method was built on two major aspects: business process security needs and cloud provider's guideline compliance. The existing risk assessment procedure was used in their approach, which automatically produced safe and economic applications over many clouds.

Kozlov and Noga, 2018, "Risk management for information security of corporate information systems using cloud technology".

The author presented the risk management method using fuzzy logic and the fuzzy set technique. Their main focus was on the proposition to tackle the difficulty of threats with the attack tree technique. The concept of using fuzzy logic and fuzzy set theory permits the incorporation of the uncertainties present in the information system. They

concluded that this proposal could be used by distributed small and medium enterprises with a distributed branch network.

Goettelman et al., 2015, "Paving the way towards semi-automatic design-time business process model obfuscation".

The authors proposed a semiautomatic method of hiding a business process through a business process logic analysis that efficiently breaks this process into multiple fractions. These fractions were deployed to the different clouds to conceal important information regarding business technicality. An algorithm was formulated to support automation of the change in the business process model.

Hutchings et al., 2013, "Cloud computing for small business: criminal and security threats and prevention measures".

The authors present the characteristic of cloud computing threats for small businesses, its identification was reexamined, and the preventive and mitigation methods for the small business user were implemented. Moreover, ways to reduce or nullify the identified risks were provided for small business users and cloud service providers.

Jakoubi et al., 2010, "Risk-aware business process management: establishing the link between business and security".

The authors suggested a reference model that provided the incorporation of risks in business process simulation with graphical illustrations. The specific objective of this study was to incorporate the modeled business process with risks, including its detection, mitigation process, and recovery method of information to positively impact the business process. In addition, they stressed the importance of evaluating business process security using simulation and modeling.

Belov et al., 2018, "On the issue of information security risks assessment of business processes".

The authors implemented an approach for evaluating information security risks in business process notation and analysis. They presented a new risk evaluation method that dealt with the importance of the business process, the diverse importance of assets in the business process, and the effect of threats in a particular period with respect to the business process. More importantly, a software application was implemented to calculate the parameters represented by standard notation based on business process modeling.

Civica et al., 2014, "Cloud-based business process orchestration".

They designed and implemented a model that orchestrates the infrastructure that increases capacity by adding or subtracting nodes founded on business cycles, periodic, or sessional requests at a reduced price. This model explored the merits of the cloud monitoring technique to make it more effective. They developed a software device that gathers monitoring data on the type of device used and the specific location where the request was made. The device connected to other systems is equally responsible for collecting information about various sales, demands, and conversion rates. Having implemented this tool, business process orchestration was used for resource utilization through nodes addition and removal as the need arise. They concluded that the implemented model led to a cost reduction for enterprise IT resource control.

Youssef, 2019, "A framework for cloud security risk management based on business objectives of organizations".

The author proposed a new framework for cloud security risk management for organizations and cloud service providers (CSP). The author used the Delphi process to merge low-level management decisions with high-level business goals. This framework assisted both cloud consumers and cloud providers in identifying, evaluating, and militating against security risks in cloud computing platforms. A quantitative risk assessment methodology was made available to the consumer side to assess cloud security prior to the adoption of cloud services, while cloud service providers were able to provide an effective service to consumers. The resultant effect on the CSP side led to high profitability through proper cloud risks management.

Rupra and Omano, 2020, "A cloud computing security assessment framework for small and medium enterprise".

The authors presented an assessment framework for the enhancement of security for cloud-based SMEs. The objective of their research was to promote a unified language that compares the development of a SME's system risks. The framework was based on the objective question measurement method. The output of the framework was a security index with detailed security level achievement. This served as the first line of defense against cloud security risks for SMEs.

Ali et al., 2020, "Assessing information security risk in the cloud: a case study of Australian local government authorities".

The authors used a case study approach to investigate requirements related to the cloud-based model within local government settings. Here, a mixed sequential research methodology was used. The authors reviewed the ISO 27002 standard and discovered three security risk factors that represented greater challenges for government operations in the cloud. These include operational security, individual awareness, and compliance issues. After a series of interviews with domain experts and personnel from governmental organizations, they presented a cloud computing security requirement assessment model, which comprises four parts: data security, risk assessment, legal and compliance requirements, and business and technical requirements. This model served as a standard for government organizations to demand cloud security requirements before deploying their processes to the cloud.

5.5. Taxonomy of Cloud Security Risks That May Affect Cloud-Based Business Processes

Security risk is one of the main causes of technical risk recognized by consumers. This type of risk affects the security requirements of users during or after accessing cloud services [89]. Therefore, the main challenge of cloud service adoption is security. To this end, there is a need to categorize cloud computing security risks that could hinder the effectiveness of the business process deployed in the cloud. This categorization is what is referred to as the taxonomy of cloud security risks. The taxonomy of cloud security risks is discussed under six categories. These are data security, logical access, network security, physical security, compliance, and virtualization, as shown in Figure 2 [90].

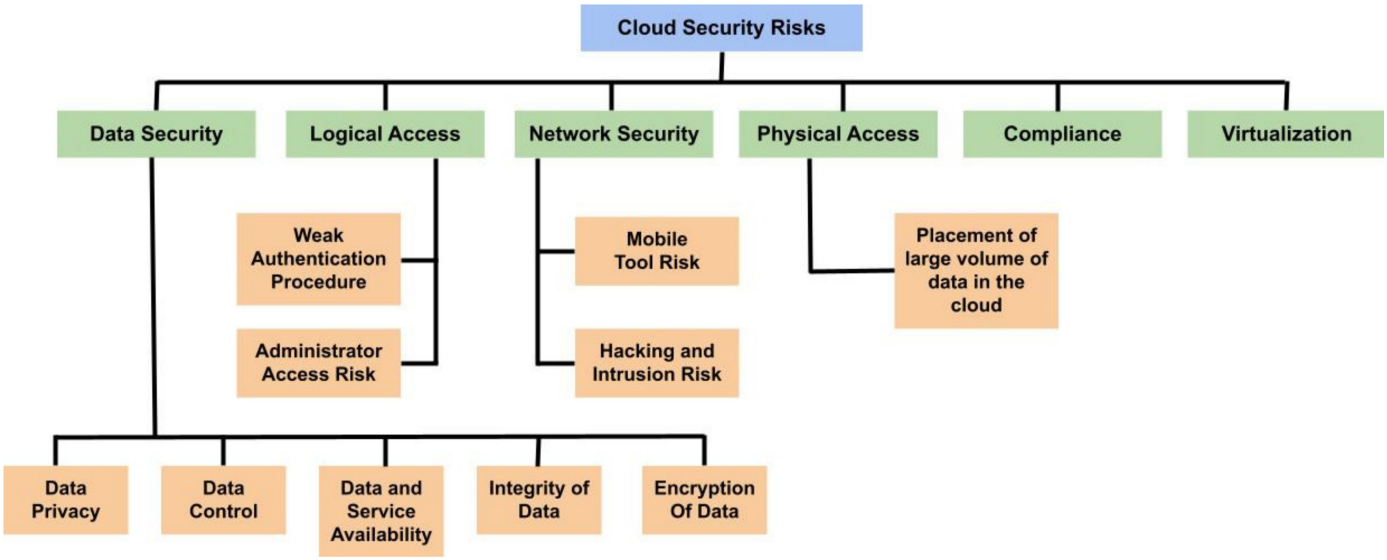

Figure 2. Taxonomy of cloud security risks that may affect cloud-based business processes.

5.5.1. Data Security

Data security risks are the main obstacle to cloud computing. Many businesses are yet to deploy their critical data and applications to the cloud due to data leakage which may result in confidential and privacy risks, uncontrolled access over hosted data and applications, cloud services and data availability concerns, data integrity impairment risk, and lack of effective protection of data in transit.

Data privacy—infrastructures are shared among many consumers, the location of data is not disclosed to consumers as data can be stored at multiple locations in the cloud. In addition, data are located externally from consumers' confined environment, resulting in data leakage, which gives rise to privacy risks due to unauthorized access.

Data control—the cloud provider manages the data deployed in the cloud and is therefore outside the control of the organization [91–94]. Since cloud facilities are shared among multiple consumers, a violation of the law by an organization could result in the seizure of all data managed by cloud providers [95].

Data and services availability—related to data recovery during a disaster to ensure smooth transmission of cloud-based services. Once the confidentiality of the data is altered, the backup and restore process might seem difficult. In addition, dependence on the Internet as a means of data transfer might present a risk of availability due to the reduction of the speed of the connectivity bandwidth [96,97].

Data integrity—Accessing data by multiple consumers and modifying data by cloud providers from remote locations may threaten data integrity [95,96,98,99].

Encryption of data—Lack of proper encryption and data key management could result in a serious risk, as the cloud environment is shared among many consumers and cloud providers that can easily access data via the public network.

5.5.2. Logical Access/Secrecy Issues

The logical or secrecy issue has to do with the risks associated with unauthorized access, such as accessing vital business data. This type of risk tends to multiply as data are accessed from an external server. Moreover, data access through the Internet leads to more exposure which invariably resulted in higher risks. These types of access are further discussed as follows:

Administrator access risk—Due to the management interface (on-demand self-service) required by cloud computing for its services, cloud administrators can easily access and modify the data via the Internet.

Weak authentication procedure—Lack of a robust authentication procedure can lead to unauthorized access to sensitive data and applications that many consumers can access at any location due to multiple tenancies of cloud environment [93,100].

5.5.3. Network Security

This has to do with malicious consumers gaining access to sensitive data through the remote system and web tools. Infected applications can be launched, which can negatively affect cloud consumers and cloud computing services. These security risks include the following.

Hacking and intrusion risk—Hackers gaining access to data and applications through the remote system and web application by launching infected applications, which will affect cloud consumers and their services.

Risk of mobile tools—The privilege of allowing cloud consumers to access data through their mobile device is a new trending risk in the cloud environment that results in security threats in this domain.

5.5.4. Physical Access

The emergence of cloud computing with its significant benefits has made many organizations deploy all their sensitive data to the cloud without considering its consequences. The placement of a large volume of data in the cloud exposes such organizations to great

risk from the malicious consumer, because hackers can access business data in any virtual location compared to the secure physical location [92,95].

5.5.5. Compliance

The usage of cloud services has to do with the remote external location of business data and applications that are not covered by policies and regulatory bodies that monitor data stored in the physical environment. Attackers can use this medium to gain unlawful access to business data leading to security risks.

5.5.6. Virtualization

Virtual resources cannot be separated from cloud computing because this is the framework on which the operation is based. Since virtual resources are conjoined with cloud facilities, intrusion risks become paramount as one of the significant security risks in the cloud environment.

5.6. Mapping of Cloud-Based Security Risk Taxonomy

Cloud security risks have been discussed, and from the discussions, there is a mapping or relationship between the threats leading to these risks, as depicted in Table 4. Looking at cloud security risks, there is a common threat to all the categories discussed: data leakage. In data security, sharing of cloud facilities allows business data to be stored in multiple clouds without the customer's knowledge. This act permits any user to access any data, leading to data leakage, causing privacy and confidentiality risk. Furthermore, unauthorized access to sensitive data via the Internet due to the on-demand self-service interface and the weak authentication procedure in the cloud environment may contribute to the threat of data leakage under the category of logical access security risk. Hackers can gain unlawful access to business data through malware [101], botnet attacks [102], and through intrusion into public networks [103] or by phishing [104], resulting in data leakage. Additionally, authorized cloud users can access data and cloud services through their mobile tool without passing through their organization network. Bypassing the organization's network may result in data leakage from malicious insiders. In brief, cloud security relies on data protection from cloud malicious consumers or users to guide against privacy and confidential risks that might come up due to data leakages.

Table 4. Mapping of cloud security risk.

Cloud Security Risk	Threat
Data security Data privacy Data control Data and services availability Integrity of data Encryption of data	Sharing of cloud facilities, unknown data location, no direct control by cloud consumers, internet-dependent for data transfer, network integrity, unauthorized access
Logical access/secrecy issue Administrator access risk Weak authentication procedure	Unauthorized access, cloud management interface issue, multi-factor authentication issue, weak passwords
Network security Hacking and intrusion risk Mobile tool risk	Unauthorized access via the remote system, injection of malicious applications, mobile device threat
Physical access Placement of large volume of data in the cloud environment	Deployment of vital business data on the cloud, unauthorized access via the remote system, data modification by cloud administrator
Compliance	Incompliance with standard regulatory bodies and policies given attackers avenues for unauthorized access
Virtualization	Mapping of physical resources to virtual resources

5.7. Literature Evaluation Framework

In this survey, the framework evaluation model is greatly influenced by the design science research paradigm [105]. The reason has to do with the kind of research carried out in the risk management domain, business process, and cloud computing that was seen as

a form of design science research. Design science simply means creating and evaluating IT artifacts to solve some specified organizational problems [105]. Here, we look at how security issues in business processes deployed to the cloud can be solved by incorporating security risk management with the business process. The scientific world is taking care of this problem by presenting different IT artifacts, such as constructs, models, methods, and instantiations [106]. This literature evaluation was carried out using two criteria: the BPM lifecycle and the extent to which the risk management field informs cloud-based business process security approaches. It should be noted that the evaluation of the selected articles was carried out using the stated evaluation framework criteria.

5.7.1. Business Process Lifecycle Evaluation

The main goal of this survey is to secure cloud-based business processes through risk management. The focus is on the assessment of the phases of the BPM life cycle to which a specific research artifact is applied. At this junction, the four phases of the BPM lifecycle explained in Section 2 were considered in the assessment framework. The four phases include the identification phase, the modeling phase, the implementation phase, and the monitoring phase. These phases were described by Goettelman [107]. The following "grades" were assigned to each criterion in the evaluation framework: maximum support (A), partial support (B), or no support (F).

For complete support criterion (A), this means that the security risk management process is used at each phase of the BPM to proactively treat security issues that may arise in any of the four phases of the business process deployed to the cloud.

For the partial support criterion (B), it shows that risk management is applied in one or two of the BPM phases to proactively treat security issues that may arise in any of the four phases of the business process deployed to the cloud.

For no support criterion (F), this means that the security risk management process is not applied in any of the BPM phases to proactively treat security issues in the business process deployed to the cloud.

For clarification purposes, the following questions serve as a guide in extracting information about the usage of SRM in each of the four phases of BPLC.

- Identification phase: Does the approach propose any means of risk identification in business process models and principles/guidelines that can reduce business process security risks?
- Modeling phase: Does the approach give risk assessment technique(s) to assess business process security risks during the modeling phase?
- Implementation phase: Is there any suggestion by the approach regarding technique(s) to assess business process security risks at the implementation phase?
- Monitoring phase: Is there any suggestion by the approach regarding techniques to assess security risks in the business process (during the monitoring phase) on the logs documentation from implementing the process?

5.7.2. Influence of Risk Management Domain on Cloud-Based Business Process Security

The second assessment criteria considered in this survey is the influence of risk management domain on cloud-based BP security, and this expressed how much the risk analysis techniques and security risk standards in the risk management field affect the approach of the business process under evaluation. Here, three evaluation indicators were considered: (i) risk analysis technique, (ii) security risk standard, and (iii) domain applicability.

Security Risk Analysis Technique

These evaluation criteria try to proffer an answer to whether or not any of the security risk analysis models such as NIST guideline, Octave, tool of The European Union Agency for Cybersecurity (ENISA), CVSS, risk watch for quantitative terms, etc. is applied in the implementation process of cloud-based business process. Three "grades" have been

assigned in the usage of security risk standard evaluation. The grades are maximum support (A), partial support (B), or no support (F).

For maximum support criteria (A), this question serves as guide in getting the information on the usage of existing security risk analysis method.

- Is there anywhere any of the existing risk analysis techniques are applied in the approach?

For partial support criteria (B), this question also serves as a guide:

- Is there any way any of the existing security risk analysis techniques are adapted for use?

For no support criteria (F), this question also serves as a guide:

- Does the proposed approach use any existing security risk analysis method or not?

Usage of Security Risk Standard

One of the key facts about research in the security risk management domain is the need to obey different risk-related regulations/standards. These evaluation criteria find out whether or not any of the security risk standards such as ISO 31000, ISO 27005, generic security risk standard, etc. is applied in the implementation process of cloud-based business process. Three "grades" have been assigned in the usage of security risk standard evaluation. The grades are maximum support (A), partial support (B), or no support (F).

For maximum support criteria (A), the idea is to know whether there is usage of any security risk standard(s).

For partial support criteria (B), this indicator seeks to discover if the approach is partially used or whether the standard is adapted in cloud-based business process.

For no support criteria (F), the notion is to discover if there is no fact supporting the usage of security risk standards in the research work involving cloud-based BPs or the approach uses one or more standards without full explanation on its integration.

Domain Applicability

This evaluation criteria try to find out which field(s) has the implemented approach applied. Examples of applicable fields include finance, procurement or shipping, industry, government agencies, banks, school, military, etc. Here, there are no evaluation criteria assigned, the applicable is stated for clarification.

6. Trends and Critical Analysis

Many new techniques, processes, and methodologies try to facilitate cloud security by integrating security risk management to have a better-secured cloud. However, only a few studies incorporated security risk management into one of the phases of the business process that is deployed to the cloud. Table 5 summarizes the number of studies per approach used. Table 6 shows the main contributions of each selected approach to security risk management in the deployment of business processes to the cloud.

Table 5. Summary of the quantity of studies per approach used.

Approach Type	Number of Studies
Framework	6
Technique (Model)	6
Methodology	4
Process	1

Table 6. Evaluation—integrating security risk in the BP life cycle phase.

Authors	Identification	Modeling	Implementation	Monitoring
Goettelman et al., 2014 [107]	F	F	A	F
Vijayakumar and Arun, 2017 [108]	F	F	F	F
Goettelman et al., 2013 [10]	F	F	F	F
Kateeb and Almadallah, 2014 [109]	F	F	F	F
Ali et al., 2017 [110]	F	F	F	F
Vasiljeva et al., 2017 [108]	F	F	F	F
Damasceno et al., 2011 [111]	F	F	F	F
Goettelman et al., 2014 [112]	F	F	A	F
Kozlov and Noga, 2018 [113]	F	F	F	F
Goettelman et al., 2015 [114]	F	F	F	F
Hutchings et al., 2013 [115]	F	F	F	F
Jakoubi et al., 2010 [116]	F	F	A	A
Belov et al., 2018 [117]	F	F	F	F
Ciovica et al., 2014 [118]	F	F	F	F
Youssef, 2019 [119]	F	F	F	F
Rupra and Omamo, 2020 [120]	F	F	F	F
Ali et al., 2020 [121]	F	F	F	F

However, at the end of the evaluation process, the conclusion is that each of the selected approaches exposes more vital areas to manage security issues in the cloud-based business process. These characteristics served as the basis for new methodologies/processes/frameworks/techniques or extensions to existing ones.

6.1. Business Process Life Cycle Evaluation Result

The business project life cycle model adopted for this study comprises four phases and these includes the identification phase, modeling phase, implementation phase, and monitoring phase. As seen in Table 6, each selected paper was compared with each phase of the business process to know whether the work incorporates security risk management in any of the BP life cycle phases. The grading was done according to the description in Section 5.7.1 of this study.

The evaluation result shown in Table 6 is explained as follows. The work carried out by Goettelman [107,112] incorporated security risk management in the implementation phase of the business process life cycle. A detailed SRM processes (risk identification, assessment, monitoring, and communication) were effected at the implementation phase of the BPLC. Meanwhile, SRM processes were not considered at the other three phases of the BPLC. Similarly, the work done by Jakoubi [116] integrates security risk management at both the implementation phase and monitoring phase of the BPLC. The SRM processes were fully considered only; the running time analysis of BP security risk management was not implemented.

For the work carried out by Vijayakumar and Arun [114], there were no findings where the authors implemented SRM processes in any of the four phases of the BPLC. Their work focused on the analyses of two security risk assessment frameworks for cloud-based enterprise in order to know the preferred model. Furthermore, the work carried out by Goettelman [10] did not incorporate SRM into any of the four phases of the BP. Their work emphasized cloud selection for a secure deployment of cloud-based risk-aware BPs. In addition, Kateeb and Almadallah's [109] work was a theoretical risk management framework that uses NIST standard which catered for security risks on the provider's side and therefore, SRM processes were not supported at any of the four phases of BPLC.

Ali's [110] work had no support for SRM processes in the four phases of BPLC, rather they focused on the conceptualization of risk category for solving problems for individual cloud users and cooperate organization. In addition, Vasiljeva [108] did not support SRM processes at any of the phases of BPLC. The aim of their study was the determination of the usage of cloud computing adoption in boosting business performance of Latvian small

and medium enterprises. The research approach was empirical and did not involve the implementation SRM processes.

In the work done by Damasceno [111], the integration of SRM processes into the BPLC was not supported because the research work was basically on annotated security requirement for cloud business processes. Kozlov and Noga's [113] work has no support for the integration of SRM for BPLC mainly because the study focused on the usage of fuzzy logic and the fuzzy set technique for SMEs using cloud technology. Goettelman's [114] work was centered on the design-time business process model obfuscation. Therefore, the integration of SRM into the business process life cycle was not supported at any of the four phases.

Hutchings' [115] work has no support for the integration of cloud-based SRM in the business process life cycle. This study provided a theoretical identification and mitigation processes for cloud based SRM threats that have nothing to do with the BPLC. The approach presented by Belov [117] was on the evaluation of cloud-based security risks in business process notation and analysis and has no support for the incorporation of SRM with BPLC. Therefore, each phase of BPLC was graded "F".

Ciovica [118] worked on cloud-based business process infrastructure orchestration and has nothing in common with the integration of SRM with BPLC. Based on this sub-mission, this work has no support for the identification phase, modeling phase, implementation phase, and the monitoring phase of BPLC.

The works carried out by Youssef [119] and Rupra and Omamo [120] proposed cloud-based security assessment frameworks; the authors used Delphi quantitative assessment model and the objective question measurement method respectively. Their work did not follow BPLC and therefore, it has no support for the integration of SRM with BPLC. The four phases of the BPLC were graded "F". Lastly, Ali [121] did not support cloud-based SRM with BPLC because the author dealt with the investigation of the mode of assessing cloud-based security risks in the governmental processes.

In summary, most of the evaluated works that deal with risk assessment do not incorporate it into the business process; only 17% did. Being a new area to explore, there is a research gap in modeling security risk management into two or more phases of the business process life cycle to properly secure the important data of the business process.

6.2. Influence of Risk Management Domain Evaluation Result

According to the evaluation criteria, three key indicators were established to support our findings. They are domain applicability, usage of existing risk management techniques, and integration of risk standards. The details of these criteria were provided in Section 5.7.2.

6.2.1. Domain Applicability Evaluation Result

The domain application of these works shows that the approaches were test-run in real time, thereby making the work reusable; otherwise, there is a need to subject such approaches to further analysis. The evaluation result of the domain applicability is presented in Table 7.

It can be seen from Table 6 that the works done by Goettelman [10,107,112,114] were applied in the production industry, shipping, insurance company, and the finance and banking sector, respectively. The implication of the domain application of these works is an affirmation that it can be reused.

Vijajakumar and Arun [108] had its domain applicability in three different fields, namely, medical, finance, and accounting. Furthermore, authors recommended that the proposed system can be applied in any field with a little enhancement.

Table 7. Domain applicability evaluation results.

Author	Domain Applicable
Goettelman et al., 2014 [107]	Production company
Vijayakumar and Arun, 2017 [108]	Medical, Finance, Accounting
Goettelman et al., 2013 [10]	Shipping
Kateeb and Almadallah, 2014	SME
Ali et al., 2017 [110]	-
Vasiljeva et al., 2017 [108]	SME
Damasceno et al., 2011 [111]	-
Goettelman et al., 2014 [112]	-
Kozlov and Noga, 2018 [113]	-
Goettelman et al., 2015 [114]	Finance/Banking
Hutchings et al., 2013 [115]	-
Jakoubi et al., 2010 [116]	-
Belov et al., 2018 [117]	-
Ciovica et al., 2014 [118]	-
Youssef, 2019 [119]	-
Rupra and Omamo, 2020 [120]	SME
Ali et al., 2020 [121]	Local government

The works by authors Kateeb and Almadallah [109], Vasiljeva [108], and Rupra and Omamo [120] also find their application in the small and medium enterprises (SMEs).

The works by Ali [110], Damasceno [111], Kozlov and Noga [113], Hutchings [115], Jakoubi [116], Belov [117], Ciovica [118], and Youssef [119] were not tested real-time. Therefore, these works need subjection to further analysis; they were not applied to any domain. By calculation, 53% of the evaluated works were tested in real time and therefore, the works were validated. It is necessary to ensure business compliance [122] that the system developed is tested in real time for validation purposes.

6.2.2. Evaluation Result for Usage of Existing Risk Management Techniques

The evaluation result for the usage of existing security risk analysis techniques is shown in Table 8.

Table 8. Existing risk analysis evaluation result.

Author	Maximum Support (A)	Partial Support (B)	No Support (F)
Goettelman et al., 2014 [107]	A	-	-
Vijayakumar and Arun, 2017 [108]	-	B	-
Goettelman et al., 2013 [10]	A	-	-
Kateeb and Almadallah, 2014 [109]	A	-	-
Ali et al., 2017 [110]	-	-	F
Vasiljeva et al., 2017 [108]	-	-	F
Damasceno et al., 2011 [111]	-	-	F
Goettelman et al., 2014 [112]	A	-	-
Kozlov and Noga, 2018 [113]	A	-	-
Goettelman et al., 2015 [114]	-	-	F
Hutchings et al., 2013 [115]	-	-	F
Jakoubi et al., 2010 [116]	-	-	F
Belov et al., 2018 [117]	-	B	-
Ciovica et al., 2014 [118]	-	-	F
Youssef, 2019 [119]	A	-	-
Rupra and Omamo, 2020 [120]	-	B	-
Ali et al., 2020 [121]	-	-	-

Goettelman [107] used Cloud Security Alliance (CSA) control framework as the basis of their risk assessment work. Therefore, the approach proposed by this author was in full support of the evaluation criteria and it was graded "A". Vijayakumar and Arun's [108]

work was based on the comparison between the Common Vulnerability Scoring System (CVSS) and the Common Weakness Risk Assessment Framework (CWRAF) for risk analysis. This work is in partial support of the usage of existing risk analysis criteria. The works carried out by Goettelman [10,107,112,114] used the European Network of Information Security Agencies (ENISA) framework as the basis of their risk assessment model and therefore, the usage of existing risk analysis criteria was fully supported.

Kateeb and Almadallah [109] used the generic risk assessment framework as the model the risk analysis in their proposed study. The work fully supported the usage of existing risk analysis criteria. In the study presented by Koslov and Noga [113], the generic information security risk assessment model based on fuzzy principle was used as the main risk assessment method for their work. The work was in support of the evaluation criteria. Belov [117] used critical factor of the success (SCF) in getting the valuable assets for risk analysis and therefore, their work is in partial support of the evaluation criteria.

Youssef's [119] work was in full support of the usage of existing risk analysis method as the bases of its assessment. Delphi quantitative risk assessment procedure was implemented in this study. Rupra and Omamo [120] reviewed many existing risk assessment methods, such as CSF, ENISA, CVSS, etc., before their risk analysis model was proposed. This study is in partial support of the evaluation criteria.

Other works by Vasiljeva [108], Damasceno [111], Hutchings [115], Jakoubi [116], Ciovica [118], and Ali [121] have no support for the usage of existing risk assessment methods. Nine authors out of seventeen (52.9%) carried out their research work using the existing risk analysis technique. It is paramount to note that the use of existing risk management techniques paves the way for better results and new development. Therefore, there is a need to establish information system projects on existing technology to cover every necessary research aspect.

6.2.3. Evaluation Result for the Integration of Security Risk Standards

The third criterion in this aspect is the integration of security risk standards. In IS, it is difficult to obtain certification in security standards (for instance, IS built for the Defense Ministry or NATO). A suitable initiative is the one that perfectly fulfills the stated condition "risk standard integration" and equally looks at the required security risk standard. When considering the security risk in all phases of the business process, the most preferred suggestions would be those that meet the criterion. The analysis of this result is seen in Table 8 and the discussion is as follows.

Goettelman [107] used ISO/27017 security risk standard in their study. Therefore, the approach proposed by these authors is in full support of the evaluation criteria and it is graded "A".

Vijayakumar and Arun [108] briefly mentioned the use of security risk standard in their work. This work is in partial support of security standard usage. Kozlov and Noga's 2018 work has a grade of "B" because of the partial integration of ISO/IEC 27002 security risk standard.

Ali [121] equally used ISO 27002 security risk standard in their study. Here, this security risk standard was maximized and therefore, the proposed study is in full support of the usage of security standard.

The works of Goettelman [10], Kateeb and Almadallah [109], Ali [110], Vasiljeva [108], Damasceno [111], Goettelman [112], Goettelman [114], Hutchings [115], Jakoubi [116], Belov [117], Ciovica [118], and Youssef [119] did not use security risk standards. Therefore, approaches proposed by these authors are no support of the usage of security risk standard.

As Table 9 shows, the conclusion drawn at the end of the evaluation process indicated that though many security risk standards (examples include ISO/IEC 15408:2009, ISO/IEC 27001:2013, etc.) have been implemented and helped in the process of secured business process development, it was tedious to implement a methodology/process that incorporated all the stated conditions and the security restrictions. Consequently, many methodologies/processes do not integrate these standards in an easily understandable

and methodical way. Five authors constituted 29.4% integrated security risk standards in their work. This survey suggests that new initiatives should be implemented to integrate security risk standards into the business process life cycle, that is, new suggestions that will systematically uphold the fulfillment of risk standards and integrate new techniques during the business development process.

Table 9. Integration of security risk standard evaluation result.

Author	Maximum Support (A)	Partial Support (B)	No Support (F)
Goettelman et al., 2014 [107]	A	-	-
Vijayakumar and Arun, 2017 [108]	-	B	-
Goettelman et al., 2013 [10]	F	F	F
Kateeb and Almadallah, 2014 [109]	F	F	F
Ali et al., 2017 [110]	F	F	F
Vasiljeva et al., 2017 [108]	F	F	F
Damasceno et al., 2011 [111]	F	F	F
Goettelman et al., 2014 [112]	F	F	F
Kozlov and Noga, 2018 [113]	-	B	-
Goettelman et al., 2015 [114]	F	F	F
Hutchings et al., 2013 [115]	F	F	F
Jakoubi et al., 2010 [116]	F	F	F
Belov et al., 2018 [117]	F	F	F
Ciovica et al., 2014 [118]	F	F	F
Youssef, 2019 [119]	F	F	F
Rupra and Omamo, 2020 [120]	F	F	F
Ali et al., 2020 [121]	A	-	-

6.3. Future Directions

The business process is dealt with mostly from a technical angle during the implementation phase. Although it is an essential aspect, security issues should be mitigated in all phases of business process development because it is the basis for achieving a robust system. Although great work has been done by [49], many areas of cloud-based security management of business processes based on the cloud need to be improved. From the literature survey conducted, some of the areas that need improvement are listed. Security risk management must be properly integrated in each phase of business process management to provide a reliable and secure business process. The use of qualitative and quantitative risk assessment methodologies that offer a balance evaluation procedure will be needed to assess cloud offers for a secured business process. There is a need for a combination of three or more existing risk analysis techniques to produce stronger and more formidable secure systems. Although there is no perfect secure system, the need to integrate current security risk standards into business process management should be considered.

7. Summary and Conclusions

In this study, a comprehensive survey of cloud-based business process security risk management was conducted. The detailed process of the selected literature used was provided and the theoretical background in which this evaluation framework was developed is also given.

After a systematic evaluation of each initiative using the stated evaluation framework, the following conclusions were arrived at:

- For the business process lifecycle evaluation, the result shows that most of the evaluated works that dealt with risk assessment do not incorporate it into the business process lifecycle; only 17.6% did so, which constitutes 3 studies out of 17 evaluated works.
- For domain applicability evaluation result, 53% of the evaluated works were tested in real time and therefore the works were validated and reused.

- The evaluation result for the usage of existing security risk analysis techniques shows that 9 authors out of 17 (52.9%) carried out their research work using the existing risk analysis technique.
- The evaluation result for the integration of security risk standards indicates that it was tedious to implement a methodology/process that incorporated all the stated conditions and the security restrictions. Consequently, many methodologies/processes do not integrate these standards in an easily understandable and methodical way. Five authors constituted 29.4% integrated security risk standards in their work.

Based on the outcome of this literature review, lapses were established in this study area. In summary, the management of risks in business processes has been the main topic of discourse in the research community in recent years [26]; however, very little work has been done on cloud-based business process security risk management. Although this research area is still under exploration, there are challenges facing systems that need further investigation, including security risk management in the modeling and monitoring phases. Furthermore, the integration of existing security risk management techniques into this area of research, which is partially or in most cases not supported, should be appropriately investigated. The issue of not incorporating security risk standards in the few studies evaluated in this review deserves serious attention. Most of these approaches need to be validated in real-time to know their feasibility and effectiveness. Based on these findings and results, security risk management, the use of emerging security risk management techniques, and security risk standards should be integrated with the phases of the business process to mitigate against security issues.

Limitation of the Study

The fields of business process management, cloud computing, and security risk management have been interesting fields when studied individually. The reason is that a lot of research work has been carried out in these fields of study. Integrating these three domains as one is good for a new research proposal, but the challenge is that of getting research materials. Having searched through different academic forums using well-known learned article web browsers, such as Google Scholar, Scopus, and Web of Science, we discovered that limited journals are available for research purposes in this area.

Author Contributions: T.E.A., O.T.A., S.M., K.A. and R.D. contributed equally. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviation

BPM	Business Process Management
BP	Business Process
BPLC	Business Process Life Cycle
SRM	Security Risk Management
CC	Cloud Computing
ENISA	European Network of Information Security Agencies
CVSS	Common Vulnerability Scoring System
CWRAF	Common Weakness Risk Assessment Framework
CFS	Critical Factor of the Success

References

1. Van der Aalst, V.M. Business process management: A comprehensive survey. *ISRN Softw. Eng.* **2013**, *2013*, 507984. [CrossRef]
2. Mahal, A. *How Work Gets Done: Business Process Management, Basics and Beyond*; Technics Publications, LLC: Lavallette, NJ, USA, 2010.
3. Damelio, R. *The Basics of Process Mapping*; Taylor & Francis: Boca Raton, FL, USA, 2011.
4. Van Looy, A.; Shafagatova, A. Business process performance measurement: A structured literature review of indicators, measures and metrics. *SpringerPlus* **2016**, *5*, 1797. [CrossRef] [PubMed]
5. Harmon, P. *Business Process Change: A Guide for Business Managers and BPM and Six Sigma Professionals*, 2nd ed.; Morgan Kaufmann: Burlington, MA, USA, 2010.
6. Vaquero, L.; Rodero-Marino, L.; Caceres, J.; Lindner, M. A Break in the Clouds: Towards a Cloud Definition. *SIGCOMM Comput. Commun. Rev.* **2008**, *39*, 137–150. [CrossRef]
7. NIST. *The NIST Definition of Cloud Computing*; Gartner: Stamford, CT, USA, 2012.
8. Ratcliffe, J. Intelligence-Led Policing. *Trends Issues Crime Crim. Justice* **2003**, *248*, 1–6.
9. Tang, C.; Liu, J. Selecting a trusted cloud service provider for your SaaS program. *Comput. Secur.* **2015**, *50*, 60–73. [CrossRef]
10. Goettelmann, E.; Mayer, N.; Godart, C. A general approach for a trusted deployment of a business process in clouds. In Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction, Luxembourg, 28–31 October 2013; pp. 92–99. [CrossRef]
11. Chen, D.; Zhao, H. Data Security and Privacy Protection Issues in Cloud Computing. In Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 23–25 March 2012; pp. 647–651.
12. Jansen, W.A. Cloud Hooks: Security and Privacy Issues in Cloud Computing. In Proceedings of the 2011 44th Hawaii International Conference on System Sciences, Kauai, HI, USA, 4–7 January 2011; pp. 1–10.
13. Leuprecht, C.; Skillicorn, D.B.; Tait, V.E. Beyond the Castle Model of cyber-risk and cyber-security. *Gov. Inf. Q.* **2016**, *33*, 250–257. [CrossRef]
14. Kuo A., M. Opportunities and challenges of cloud computing to improve health care services. *J. Med. Internet Res.* **2011**, *13*, e67. [CrossRef]
15. Bhagawat, V.C.; Kumar, A.L.S. Survey on data security issues in cloud environment. *Int. J. Innov. Res. Adv. Eng.* **2015**, *2*, 31–35.
16. Conforti, R.; Fortino, G.; La Rosa, M.; ter Hofstede, A. History-aware Real-time Risk Detection in Business Processes. In *CoopIS, DOA-SVI, and ODBASE LNCS*; Meersman, R., Dillon, T., Herrero, P., Kumar, A., Reichert, M., Qing, L., Ooi, B., Damiani, E., Schmidt, D., White, J., et al., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; Volume 7044, p. 100.
17. Kitchenham, B. *Procedures for Perfoming Systematic Review*; Joint Technical Report; Software Engineering Group, Department of Computer Science, Keele University: Keele, UK; Empirical Software Engineering, National ICT Australia Ltd: Sydney, Australia, 2004.
18. Kitchenham, B. *Guideline for Performing Systematic Literature Reviews in Software Engineering*; Version 2.3; University of Keele and Durham: Keele, UK, 2007.
19. Brereton, P.; Kitchenham, B.; Budgen, D.; Turner, M.; Khalil, M. Lessons from applying the systematic literature review process within the software engineering domain. *J. Syst. Softw.* **2007**, *80*, 571–583. [CrossRef]
20. Biolchini, J.; Mian, P.G.; Natali, A.C.C.; Travassos, G.H. *Systematic Review in Software Engineering*; Systems Engineering and Computer Science Department COPPE/UFRJ: Rio de Janeiro, Brazil, 2005.
21. Jakoubi, S.; Tjoa, S.; Goluch, G.; Quirchmayr, G. A Survey of Scientific Approaches Considering the Integration of Security and Risk Aspects into Business Process Management. In Proceedings of the 2009 20th International Workshop on Database and Expert Systems Application, DEXA'09, Linz, Austria, 31 August–4 September 2009; pp. 127–132. [CrossRef]
22. Rikhardsson, P.; Best, P.; Green, P.; Rosemann, M. Business Process Risk Management and Internal Control: A Proposed Research Agenda in the Context of Compliance and ERP Systems. 2006. Available online: https://eprints.qut.edu.au/5192 (accessed on 3 September 2020).
23. Suriadi, S.; Weiß, B.; Winkelmann, A.; Arthur, H.M.; Hofstede, T.; Adams, M.; Conforti, R.; Fidge, C.; La Rosa, M.; Ouyang, C.; et al. Current Research in Risk-aware Business Process Management—Overview, Comparison, and Gap Analysis. *Commun. Assoc. Inf. Syst. (CAIS)* **2014**, *34*, 52. [CrossRef]
24. Aguilar-Saven, R.S. Business process modeling: Review and framework. *Int. J. Prod. Econ.* **2004**, *90*, 129–149. [CrossRef]
25. Thabet, R.; Bork, D.; Boufaied, A.; Lamine, E.; Korbaa, O.; Pingaud, H. Risk-aware business process management using multi-view modeling: Method and tool. *Requir. Eng.* **2021**, *26*, 371–397. [CrossRef]
26. Lamine, E.; Thabet, R.; Sienou, A.; Bork, D.; Fontanili, F.; Pingaud, H. BPRIM: An integrated framework for business process management and risk management. *Comput. Ind.* **2020**, *117*, 1–17. [CrossRef]
27. Dixon, J. *BPM Survey Insights: Maturity Advances as BPM Goes Mainstream*; Gartner: Stamford, CT, USA, 2011.
28. Dixon, J.; Jones, T. *Hype Cycle for Business Process Management*; Gartner: Stamford, CT, USA, 2011.
29. Vollmer, K.; Leganza, G.; Pilecki, M.; Smillie, K. *The EA View: BPM Has Become Mainstream*; Forrester: Cambridge, MA, USA, 2008.
30. Gengler, B. BPM to Buck Slowing Spend Trend. The Australian. 2008. Available online: http://www.theaustralian.com.au/news/ (accessed on 3 September 2020).
31. Dumas, M.; Van der Aalst, V.; ter Hofstede, V. *Process-Aware Information Systems: Bridging People and Software through Process Technology*; John Wiley & Sons: Hoboken, NJ, USA, 2005.

32. Dumas, M.; La Rosa, M.; Mendling, J.; Reijers, H.A. *Fundamentals of Business Process Management*; Springer: Berlin/Heidelberg, Germany, 2013.
33. Bernardo, R.; Galina, S.V.R.; de Pádua, S.I.D. The BPM lifecycle: How to incorporate a view external to the organization through dynamic capability. *Bus. Process Manag. J.* **2017**, *23*, 155–175. [CrossRef]
34. Klems, M.; Nimis, J.; Tai, S. Do Clouds Compute? A Framework for Estimating the Value of Cloud Computing. *Lect. Notes Bus. Inf. Process.* **2009**, *22*, 110–123. [CrossRef]
35. Cearley, D. *Hype Cycle for Applications Development*; Gartner Group Reporter Number G00147982; Gartner: Stamford, CT, USA, 2009.
36. Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.D.; Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Stoica, I.; et al. A view of cloud computing. *Commun. ACM* **2010**, *53*, 50–58. [CrossRef]
37. Aljabre, A. Cloud Computing for Increased Business Value. *Int. J. Bus. Soc. Sci.* **2012**, *3*, 234–239.
38. Morin, J.-H.; Aubert, J.; Gateau, B. Towards Cloud Computing SLA Risk Management: Issues and Challenges. In Proceedings of the 2012 45th Hawaii International Conference on System Sciences, Maui, HI, USA, 4–7 January 2012; pp. 5509–5514.
39. Jiang, S. Research on Risk Evaluation of Information Security Based on Cloud Computer. In Proceedings of the 2018 International Conference on Internet and e-Business, Singapore, 25–27 April 2018. [CrossRef]
40. Choo, K.-K.R. A Cloud Security Risk-Management Strategy. *IEEE Cloud Comput.* **2014**, *1*, 52–56. [CrossRef]
41. Gupta, S.; Saini, A.K. Modeling Risk Management in Cloud Adoption. In Proceedings of the IEEE 5th International Conference on System Modeling & Advancement in Research Trends, Moradabad, India, 25–27 November 2016; pp. 238–241.
42. Razaque, A.; Li, Y.; Liu, Q.; Khan, M.J.; Doulat, A.; Almiani, M.; Alflahat, A. Enhanced Risk Minimization Framework for Cloud Computing Environment. In Proceedings of the 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), Aqaba, Jordan, 28 October–1 November 2018; pp. 1–7. [CrossRef]
43. Islam, S.; Fenz, S.; Weippl, E.; Mouratidis, H. A Risk Management Framework for Cloud Migration Decision Support. *J. Risk Financ. Manag.* **2017**, *10*, 10. [CrossRef]
44. Gupta, S.; Saxena, K.B.C.; Saini, A.K. Towards Risk Managed Cloud Adoption: A Conceptual Framework. In Proceedings of the 2016 International Conference on Industrial Engineering and Operations Management, Kuala Lumpur, Malaysia, 8–10 March 2016; pp. 1–7.
45. Basu, S.; Sengupta, A.; Mazumdar, C. A Quantitative Methodology for Cloud Security Risk Assessment. In Proceedings of the 7th International Conference Proceedings on Cloud Computing and Services Science (CLOSER 2017), Porto, Portugal, 24–26 April 2017; pp. 92–103.
46. Al-Anzi, F.S.; Yadav, S.K.; Soni, J. Cloud Computing: Security Model Comprising Governance, Risk Management and Compliance. In Proceedings of the 2014 International Conference on Data Mining and Intelligent Computing (ICDMIC), Delhi, India, 5–6 September 2014; pp. 1–6.
47. Aruna, E.; Shri, A.; Lakkshmanan, A. Security concerns and risk at different levels in Cloud Computing. In Proceedings of the 2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), Chennai, India, 12–14 December 2013; pp. 743–746.
48. Aswin, M.; Kavitha, M. Cloud intelligent track—Risk analysis and privacy data management in the cloud computing. In Proceedings of the 2012 International Conference on Recent Trends in Information Technology, Chennai, India, 19–21 April 2012; pp. 222–227.
49. Chang, V.; Ramachandran, M. Towards Achieving Data Security with the Cloud Computing Adoption Framework. *IEEE Trans. Serv. Comput.* **2016**, *9*, 138–151. [CrossRef]
50. Dahbur, K.; Mohammad, B.; Tarakji, A.B. A survey of risks, threats and vulnerabilities in cloud computing. In Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications, Amman, Jordan, 18–20 April 2011; p. 12.
51. Damenu, T.K.; Balakrishna, C. Cloud Security Risk Management: A Critical Review. In Proceedings of the 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, Cambridge, UK, 9–11 September 2015; pp. 370–375.
52. Djemame, K.; Armstrong, D.; Guitart, J.; Macias, M. A Risk Assessment Framework for Cloud Computing. *IEEE Trans. Cloud Comput.* **2014**, *4*, 265–278. [CrossRef]
53. El Kefel, M.D.; Mohamed, B. Risk Management in Cloud Computing. In Proceedings of the 2013 Third International Conference on Innovative Computing Technology (INTECH), London, UK, 29–31 August 2013; pp. 127–131.
54. Khan, A.U.; Oriol, M.; Kiran, M.; Jiang, M.; Djemame, K.; Khan, A.U. Security risks and their management in cloud computing. In Proceedings of the 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings, Taipei, Taiwan, 3–6 December 2012; pp. 121–128.
55. Marbukh, V. Systemic Risks in the Cloud Computing Model: Complex Systems Perspective. In Proceedings of the 2016 IEEE 9th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 27 June–2 July 2016; pp. 863–866.
56. Albakri, S.H.; Shanmugam, B.; Samy, G.N.; Idris, N.B.; Ahmed, A. Security risk assessment framework for cloud computing environments. *Secur. Commun. Netw.* **2014**, *7*, 2114–2124. [CrossRef]
57. Drissi, S.; Houmani, H.; Medromi, H. Survey: Risk Assessment for Cloud Computing. *Int. J. Adv. Comput. Sci. Appl.* **2013**, *4*, 143–148. [CrossRef]

58. Wu, J.; Wang, Z.; Gao, S. Assessing the cloud migration readiness: A fuzzy AHP approach based on BTR framework. In Proceedings of the 2014 11th International Conference on Service Systems and Service Management (ICSSSM), Beijing, China, 25–27 June 2014; pp. 1–6. [CrossRef]
59. Xie, F.; Peng, Y.; Zhao, W.; Chen, D.; Wang, X.; Huo, X. A risk management framework for cloud computing. In Proceedings of the 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems, Hangzhou, China, 30 October–1 November 2012; Volume 1, pp. 476–480.
60. Mircea, M.; Ghilic, B.; Stoica, M. Combining Business Intelligence with Cloud Computing to Delivery Agility in Actual Economy. *J. Econ. Comput. Econ. Cybern. Stud. Res.* **2012**, *45*, 39–54.
61. Islam, S.; Weippl, E.R.; Krombholz, K. A Decision Framework Model for Migration into Cloud: Business, Application, Security and Privacy Perspectives. In Proceedings of the 16th International Conference on Information Integration and Web-based Applications & Services, Hanoi, Vietnam, 4 December 2014; pp. 185–189.
62. Griffy-Brown, C.; Lazarikos, D.; Chun, M. Agile Business Growth and Cyber Risk. In Proceedings of the 2018 IEEE Technology and Engineering Management Conference (TEMSCON), Evanston, IL, USA, 28 June–1 July 2018; pp. 1–6.
63. Chen, W.; Sharieh, S.; Blainey, B. A Security-as-a-Service Solution for Applications in Cloud Computing Environment. In Proceedings of the Society for Modeling and Simulation (SCS) International, Baltimore, MD, USA, 15–18 April 2018. [CrossRef]
64. Peake, C. Security in the cloud: Understanding the risks of cloud-as-a-service. In Proceedings of the 2012 IEEE Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 13–15 November 2012; pp. 336–340.
65. Iqbal, S.; Kiah, M.L.M.; Dhaghighi, B.; Hussain, M.; Khan, S.; Khan, M.K.; Choo, K.-K.R. On cloud security attacks: A taxonomy and intrusion detection and prevention as a service. *J. Netw. Comput. Appl.* **2016**, *74*, 98–120. [CrossRef]
66. Fall, D.; Okuda, T.; Kadobayashi, Y.; Yamaguchi, S. Security Risk Quantification Mechanism for Infrastructure as a Service Cloud Computing Platforms. *J. Inf. Process.* **2015**, *23*, 465–475. [CrossRef]
67. Hussain, M.; Abdulsalam, H. SECaaS: Security as a Service for Cloud-based Applications. In Proceedings of the 2nd Kuwait Conference on E-Services and E-Systems, Kuwait City, Kuwait, 5–7 April 2011; pp. 1–4.
68. Senk, C. Adoption of security as a service. *J. Internet Serv. Appl.* **2013**, *4*, 11. [CrossRef]
69. Al-Qurishi, M.; Al-Rakhami, M.; AlRubaian, M.; Alamri, A. A Framework of Knowledge Management as a Service over Cloud Computing Platform. In Proceedings of the International Conference on Big Data and Internet of Thing, IPAC'15, Batna, Algeria, 23 November 2015; pp. 1–4. [CrossRef]
70. Duan, Y.; Fu, G.; Zhou, N.; Sun, X.; Narendra, N.C.; Hu, B. Everything as a Service (XaaS) on the Cloud: Origins, Current and Future Trends. In Proceedings of the 8th International Conference on Cloud Computing, New York, NY, USA, 27 June–2 July 2015; pp. 621–626.
71. Karadsheh, L. Applying security policies and service level agreement to IaaS service model to enhance security and transition. *Comput. Secur.* **2012**, *31*, 315–326. [CrossRef]
72. Elsayed, M.; Zulkernine, M. Offering security diagnosis as a service for cloud SaaS applications. *J. Inf. Secur. Appl.* **2018**, *44*, 32–48. [CrossRef]
73. Benlian, A.; Hess, T. Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. *Decis. Support Syst.* **2011**, *52*, 232–246. [CrossRef]
74. Ferreira, F.S.; Alves, C.F.; Cavalcanti, R.C. R-BPM: Uma Metodologia para Gerenciamento de Processos de Negócios Consciente dos Riscos. *Rev. Bras. Sist. Inf. Rio J.* **2016**, *9*, 15–37. [CrossRef]
75. Röhrig, S.; Knorr, K. Security analysis of electronic business process. *Electron. Commer. Res.* **2004**, *4*, 59–81. [CrossRef]
76. Taubenberger, S.; Jürjen, J. IT Security Risk Analysis Based on Business Process Models Enhanced with Security Re-quirements. In Proceedings of the Workshop on Modelling Security (MODSEC08) Held as Part of the 2008 International Conference on Model Driven Engineering Languages and Systems (MODELS), Toulouse, France, 28 September 2008.
77. Suh, B.; Han, I. The IS risk analysis based on a business model. *Inf. Manag.* **2003**, *41*, 149–158. [CrossRef]
78. Lambert, J.H.; Jennings, R.K.; Joshi, N.N. Integration of risk identification with business process models. *Syst. Eng.* **2006**, *9*, 187–198. [CrossRef]
79. Bhandari, R.; Suman, U. Secure integrated framework for business processes. In Proceedings of the International Conference on Computer Communication and Control (IC4), Indore, India, 10–12 September 2015; pp. 1–6. [CrossRef]
80. Yu, W.Y.; Yan, C.G.; Ding, Z.J.; Jiang, C.J.; Zhou, M.C. Modeling and verification of online shopping business processes by considering malicious behavior patterns. *IEEE Trans. Autom. Sci. Eng.* **2016**, *13*, 647–662. [CrossRef]
81. Gonzalez, N.; Miers, C.; Redıgolo, F.; Simplıcio, M.; Carvalho, T.; Naslund, M.; Pourzandi, M. A quantitative analysis of current security concerns and solutions for cloud computing. *J. Cloud Comput. Adv. Syst. Appl.* **2012**, *1*, 1–18. [CrossRef]
82. Bouayad, A.; Blilat, A.; Mejhed, N.E.H.; El Ghazi, M. Cloud computing: Security challenges. In Proceedings of the 2012 Colloquium in Information Science and Technology, Fez, Morocco, 22–24 October 2012; pp. 26–31. [CrossRef]
83. Almorsy, M.; Grundy, J.; Ibrahim, A.S. Collaboration-Based Cloud Computing Security Management Framework. In Proceedings of the 2011 IEEE 4th International Conference on Cloud Computing, Washington, DC, USA, 4–9 July 2011; pp. 364–371. [CrossRef]
84. Ogîgău-Neamțiu, F. Cryptographic Key Management in Cloud Computing. In Proceedings of the 10th International Scientific Conference "Defense Resources Management in the 21st Century", Braşov, Romania, 15 November 2015; pp. 1–6.
85. Saeed, M.Y.; Khan, M. Data Protection Techniques for Building Trust in Cloud Computing. *Int. J. Mod. Educ. Comput. Sci.* **2015**, *7*, 38–47. [CrossRef]

86. Birje, M.N.; Challagidad, P.S.; Goudar, R.H.; Tapale, M.T. Cloud computing review: Concepts, technology, challenges and security. *Int. J. Cloud Comput.* **2017**, *6*, 32–57. [CrossRef]
87. Sumter, L.-Q. Cloud Computing: Security Risk. In Proceedings of the ACMSE'10, Oxford, MS, USA, 15 April 2010; pp. 1–4.
88. Gao, Z.; Tang, H.; Zhu, Z.; Li, Y. Management process based cloud service security model. In Proceedings of the International Conference on Cyberspace Technology (CCT 2013), Beijing, China, 23 November 2013; pp. 278–281.
89. Ratansingham, P.; Kumer, K. Trading partner trust in electronic commerce participation. In Proceedings of the 21st International Conference on Information Systems, Brisbane, Australia, 10–13 December 2000; pp. 544–552.
90. Caroll, M.C.; Merwe, A.V.D.; Kortze, P. Secure Cloud Computing: Benefits, Risks and Control. In Proceedings of the Information Security for South Africa, Johannesburg, South Africa, 15–17 August 2011; pp. 1–9.
91. Weitz, C.; Hindley, N.; Ilse, R. A Balancing Act: What Cloud Computing Means for Business, and How to Capitalize on It. 2010. Available online: www.deloitte.com (accessed on 3 September 2020).
92. Ponemon, L. Security of Cloud Computing Users: A Study of Practitioners in the US & Europe. 2010. Available online: http://www.ca.com/~/media/Files/IndustryResearch/security-cloud-computing-users_235659.pdf (accessed on 3 September 2020).
93. Raval, V. Risk Landscape of Cloud Computing. *ISACA J.* **2010**, *1*, 26.
94. Gregg, M. 10 Security Concerns for Cloud Computing. 2010. Available online: www.globalknowledge.com (accessed on 3 September 2020).
95. Rittinghouse, J.W.; Ransome, J.F. *Cloud Computing Implementation, Management, and Security*; CRC Press: Boca Raton, FL, USA, 2010.
96. Centre for the Protection of National Infrastructure (CPNI). Information Security Briefing 01/2010: Cloud Computing. Available online: http://www.cpni.gov.uk/Docs/cloud-computing-briefing.pdf (accessed on 3 September 2020).
97. Kelson, N. Cloud Computing Management Audit/Assurance Program. 2010. Available online: www.isaca.org (accessed on 3 September 2020).
98. Clavister: Security in the Cloud. 2010. Available online: www.clavister.com/resources/ (accessed on 3 September 2020).
99. Third Brigade. Cloud Computing Security: Making Virtual Machines Cloud-Ready [White Paper]. 2009. Available online: http://resources.thirdbrigade.com/ (accessed on 3 September 2020).
100. Open Cloud Manifesto. Open Cloud Manifesto: Dedicated to the Belief That the Cloud Should Be Open 2009. Available online: www.opencloudmanifesto.org/ (accessed on 3 September 2020).
101. Azeez, N.; Odufuwa, O.; Misra, S.; Oluranti, J.; Damaševičius, R. Windows PE Malware Detection Using Ensemble Learning. *Informatics* **2021**, *8*, 10. [CrossRef]
102. Alharbi, A.; Alosaimi, W.; Alyami, H.; Rauf, H.; Damaševičius, R. Botnet Attack Detection Using Local Global Best Bat Algorithm for Industrial Internet of Things. *Electronics* **2021**, *10*, 1341. [CrossRef]
103. Toldinas, J.; Venčkauskas, A.; Damaševičius, R.; Grigaliūnas, Š.; Morkevičius, N.; Baranauskas, E. A Novel Approach for Network Intrusion Detection Using Multistage Deep Learning Image Recognition. *Electronics* **2021**, *10*, 1854. [CrossRef]
104. Azeez, N.A.; Salaudeen, B.B.; Misra, S.; Damaševičius, R.; Maskeliunas, R. Identifying phishing attacks in communication networks using URL consistency features. *Int. J. Electron. Secur. Digit. Forensics* **2020**, *12*, 200. [CrossRef]
105. Hevner, A.R.; March, S.T.; Park, J.; Ram, S. Design Science in Information Systems Research. *MIS Q.* **2004**, *28*, 75. [CrossRef]
106. March, S.T.; Smith, G.F. Design and natural science research on information technology. *Decis. Support Syst.* **1995**, *15*, 251–266. [CrossRef]
107. Goettelmann, E.; Mayer, N.; Godart, C. Integrating Security Risk Management into Business Process Management for the Cloud. In Proceedings of the 2014 IEEE 16th Conference on Business Informatics, Geneva, Switzerland, 14–17 July 2014; Volume 1, pp. 86–93.
108. Vasiljeva, T.; Shaikhulina, S.; Kreslins, K. Cloud Computing: Business Perspectives, Benefits and Challenges for Small and Medium Enterprises (Case of Latvia). *Procedia Eng.* **2017**, *178*, 443–451. [CrossRef]
109. Kateeb, I.; Almadallah, M. Risk Management Framework in Cloud Computing Security in Business and Organizations. In Proceedings of the IAJC/ISAM Joint International Conference, Orlando, FL, USA, 25–27 September 2014.
110. Ali, A.; Warren, D.; Mathiassen, L. Cloud-based business services innovation: A risk management model. *Int. J. Inf. Manag.* **2017**, *37*, 639–649. [CrossRef]
111. Damasceno, J.; Lins, F.; Medeiros, R.; Silva, B.; Souza, A.; Aragaão, D.; Maciel, P.; Rosa, N.; Stephenson, B.; Li, J. Modeling and Executing Business Processes with Annotated Security Requirements in the Cloud. In Proceedings of the 2011 IEEE International Conference on Web Services, Washington, DC, USA, 4–9 July 2011; pp. 137–144. [CrossRef]
112. Goettelmann, E.; Dahman, K.; Gateau, B.; Dubois, E.; Godart, C. A Security Risk Assessment Model for Business Process De-ployment in the Cloud. In Proceedings of the IEEE International Conference on Services Computing, Anchorage, AK, USA, 27 June–2 July 2014; pp. 307–314.
113. Kozlov, A.D.; Noga, N.L. Risk Management for Information Security of Corporate Information Systems Using Cloud Technology. In Proceedings of the 2018 Eleventh International Conference "Management of Large-Scale System Development" (MLSD), Moscow, Russia, 1–3 October 2018; pp. 1–5.
114. Goettelman, E.; Amina, A.-N.; Youcef, S.; Godart, C. Paving the way towards semi-automatic design-time business process model obfuscation. In Proceedings of the IEEE International Conference on Web Services, New York, NY, USA, 27 June–2 July 2015.
115. Hutchings, A.; Smith, R.G.; James, L. Cloud Computing for Small Business: Criminal and Security Threats and Preventive Measures. *Trends Issues Crime Crim. Justice* **2013**, *456*, 1–8. [CrossRef]

116. Jakoubi, S.; Tjoa, S.; Goluch, S.; Kitzler, G. Risk-aware Business Process Management—Establishing the Link between Business and Security. In *Complex Intelligent Systems and Their Applications, Springer Optimization and Its Applications*; Xhafa, F., Barolli, L., Papajorgji, P., Eds.; Springer: New York, NY, USA, 2010; Volume 41, pp. 109–135.
117. Belov, V.M.; Pestunov, A.; Pestunova, T.M. On the Issue of Information Security Risks Assessment of Business Processes. In Proceedings of the 2018 XIV International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE), Novosibirsk, Russia, 2–6 October 2018; pp. 136–139.
118. Ciovică, L.; Cristescu, M.P.; Frăţilă, L.A. Cloud Based Business Processes Orchestration. *Procedia Econ. Financ.* **2014**, *16*, 592–596. [CrossRef]
119. Youssef, A. A Framework for Cloud Security Risk Management based on the Business Objectives of Organizations. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 186–194. [CrossRef]
120. Rupra, S.S.; Omamo, A. A Cloud Computing Security Assessment Framework for Small and Medium Enterprises. *J. Inf. Secur.* **2020**, *11*, 201–224. [CrossRef]
121. Ali, O.; Shrestha, A.; Chatfield, A.; Murray, P. Assessing information security risks in the cloud: A case study of Australian local government authorities. *Gov. Inf. Q.* **2020**, *37*, 101419. [CrossRef]
122. Mustapha, A.M.; Arogundade, O.; Misra, S.; Damasevicius, R.; Maskeliunas, R. A systematic literature review on compliance requirements management of business processes. *Int. J. Syst. Assur. Eng. Manag.* **2020**, *11*, 561–576. [CrossRef]