DevSecOps PRACTICES FOR AN AGILE AND SECURE IT SERVICE MANAGEMENT

Mounia Zaydi, Hassan 1st University
Bouchaib Nassereddine, Hassan 1st University

ABSTRACT

Without appropriate consideration of security best practices, the continuous delivery of IT services facilitated by DevOps is risky. On the other hand, SecOps offers the possibility to reduce security risks if security is integrated into the continuous delivery pipeline according to best practices. The purpose of this paper is to investigate how DevSecOps culture can be applied in IT service management. We interviewed representatives of five Middle East and North Africa MENA organizations that are adopting SecOps in their ITSM daily activities. We note that the majority of respondents expressed the potential of common DevSecOps such as automated monitoring to improve ITSM. The findings of this study implies that organizations need a framework for understanding the DevSecops culture before they can adopt these practices in their ITSM. Likewise, this study explores the main DevSecOps practices relevant to efficient ITSM.

Keywords: IT Service Management, DevOps, SecOps, DevSecOps, ITSM practices.

INTRODUCTION

Organizations use information technology (IT) for different objectives. The achievement of most business goals of an organization relies primarily on the competence of IT support. IT service management (ITSM) is the branch of science that is concerned about the implementation and management of quality IT services that meet the needs of the business. IT service professionals achieve IT service management through an appropriate mix of people, processes and IT.

Currently, with improved ITSM processes and the adoption of best practice guides and benchmarks such as ITIL, ISO 20000. Compliance appears to be a need rather than a strategic choice to improve rapidly and easily decisions about IT and business processes. Be more agile allows the business to benefit from a higher growth of Return on Investment ROI and a constant competitive advantage (Nazımoğlu & Özsen, 2010).

Diversification of competition, increased innovation and changing customer needs are driving today's large companies to undertake a digital transformation to remain competitive. In this context, there is no longer any question of being subjected to the "tunnel effect" generated by traditional project management, which, according to the Standish Group, produces applications in which 64% of the functionalities are not or rarely used. These companies need to review their organization to become "agile", i.e. "customer-centric". To do so, they must offer only products that provide added value to their customers and reduce the "time to market" to make these products quickly usable.

As a result, organizations have realized that IT is fundamental to their success (Abdelkebir et al., 2017). Information technology is changing the way organizations operate, business processes, internal and external communication and, most importantly, the way organizations provide services to their customers (Mohamed & Singh, 2012).

Since organizations have started to see the importance of IT, they have begun to implement complex and dynamic IT systems to support their business processes (Bi et al.,

Citation Information: Zaydi, M., & Nassereddine, B. (2020). DevSecOps practices for an agile and secure it service management. Journal of Management Information and Decision Sciences, 23(2), 1-16.

2013). Given the increasing dependence on IT and to support these business processes, organizations began using the term service (Maleh et al., 2019).

The most recognized approach to IT service management has been significantly updated in the first quarter of 2019. A new version ITIL 4, which is firmly modern and in line with the expectations of its community. The new ITIL will focus on the DevOps, Agile and Lean movements to better reflect current digital uses.

DevOps is a culture that tries to eliminate the lack of collaboration between development and operations teams (Ebert et al., 2016) by teaming them up to promote cooperation, collaboration and communication (Read et al., 2016).

SecOps is the security-oriented variant of DevOps, allowing transparent collaboration between IT security and IT operations to effectively reduce risks (Sahid et al., 2018). The SecOps culture allows teams to prioritize and correct critical vulnerabilities, and systematically address compliance violations through an integrated and automated approach in current information systems.

Goals and Objectives of the Research Study

This paper aims to help organizations integrate security and DevOps into IT service management by summarizing experiences in the following areas of using ITSM practices.

According to Moore (Moore & Benbasat, 1991), organizations often prefer to learn from the experience of other organizations that are part of the team in the same industry. Thus, organizations considering adopting DevOps can also benefit from a study that identifies the names of organizations that have adopted DevOps and that use software to integrate security.

We set out the following research questions:

RQ1 What DevSecOps practices can be used in IT Service Management?

RQ2 How to integrate DevSecOps for an efficient ITSM?

We answer these research questions by first selecting and reviewing the literature on the use of DevSecOps best practices. We then identified DevSecOps perceptions of the system environment. DevSecOps activities that contribute to these perceptions. We have also identified a set of ITSM practices used to integrate security and development into DevSecOps. Based on the results of the study of our study on the analysis of best practices, we created a survey to analyze best practices further. Study DevSecOps' perceptions of ITSM service management and the activities that contribute to these perceptions. The survey was conducted among representatives of 5 organizations that have adopted DevSecOps practices.

We summarize the contributions of this paper as follows:

- A list of SecOps practices that appear to have an impact on ITSM practices;
- A conceptual model for an efficient ITSM based on DevSecOps practices;

The paper proceeds as follows. The first section is the introduction. The following section looks at the literature on factors influencing DevSecOps adoption challenges to construct a theoretical model for ITSM adoption. The third section describes the research methods. The fourth section describes the research results and discussion. The last section presents the conclusion and future works.

LITERATURE REVIEW

Citation Information: Zaydi, M., & Nassereddine, B. (2020). DevSecOps practices for an agile and secure it service management. Journal of Management Information and Decision Sciences, 23(2), 1-16.

The DevOps model is not just for development and operations teams. As an organization that wants to take full advantage of the agility and responsiveness of a DevOps approach, you also need to integrate IT security into the full lifecycle of your applications.

In the past, security-related processes were isolated and entrusted to a specific team at the final stage of development. This was not a problem at a time when development cycles lasted months or even years. But those days are over. While an effective DevOps approach ensures fast and frequent development cycles (sometimes a few weeks or days), outdated security practices can negate the benefits of the most effective DevOps projects.

Now, within the collaborative framework of the DevOps model, security is a shared responsibility, integrated from start to finish. This concept is so important that it has given rise to the term "DevSecOps" to emphasize the need to integrate security into DevOps.

The DevSecOps approach involves thinking about the security of the application and infrastructure from the start. It is also advisable to automate some security gateways in order to avoid slowing down DevOps workflows. To achieve these objectives, it is necessary to start by selecting the tools capable of ensuring the continuous integration of security, for example with a common integrated development environment that offers security functions. However, effective DevOps security requires more than just new tools. It is necessary to implement the cultural changes of DevOps within the security teams as soon as possible.

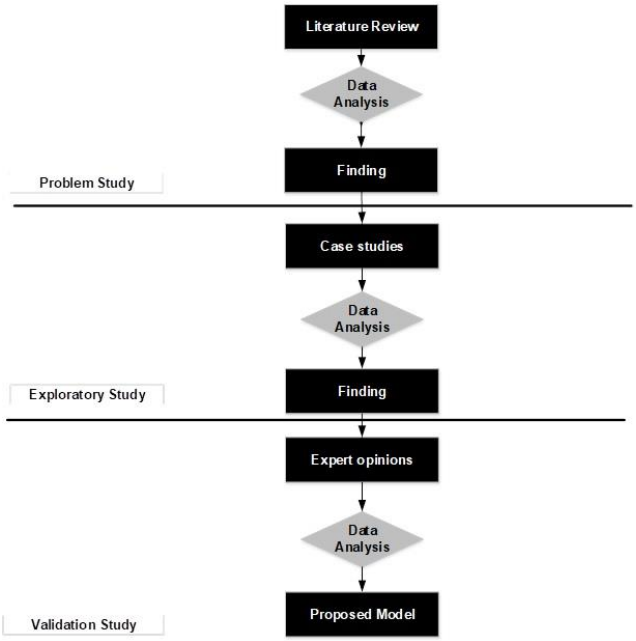

FIGURE 1

RESEARCH METHODOLOGY

This research consists of a descriptive part carried out in the form of literature reviews and a design research part. We use the research method described by (Wieringa, 2014). Their study explores the usability and usefulness of language through projects conducted by one of the authors, in the form of action research within two organizations. The study concludes that the concept of the goal is perceived as useful to ensure traceability between business objectives and IS architecture. Nevertheless, it appears that some sophisticated concepts of requirements engineering are not usable in companies because they are difficult to understand. The second study seeks to confirm this result and to evaluate the comprehensibility of these concepts. The

Citation Information: Zaydi, M., & Nassereddine, B. (2020). DevSecOps practices for an agile and secure it service management. Journal of Management Information and Decision Sciences, 23(2), 1-16.

results show empirically that, despite the asserted expertise of the participants, several concepts are indeed used incorrectly because they are misunderstood. The method used in this paper is described in Figure 1.

A literature review is a selection of documentation regarding a certain topic that contains information, data, ideas, and evidence to fulfil certain aims or express particular views about the topic. For easier understanding of the peers, as well as to add more scientific rigor to our research, we decided to follow the concept centric approach proposed by Webster and Watson (Webster & Watson, 2002).

To obtain an overview of all relevant literature concerning SecDevOps practices, a structured literature review based on the method suggested by Kitchenham et al. (2007) was conducted. This method provides details on search terms and inclusion and exclusion criteria to ensure a consistent and unbiased selection of relevant literature.

According to Kitchenham et al. (2007), the quality of a study refers to the fact that that it minimizes bias and maximizes validity and generalizability. Quality assessment can be used to complete the selection phase by excluding studies that do not meet a certain quality threshold. The quality assessment can also be used to measure and account for the importance of studies.

When analyzing the results. In this case, it is used to complete data extraction. Studies with a low score will not be excluded but will be evaluated with regard to their quality score. The quality assessment is done with the help of a checklist. This is in the form of a questionnaire consisting of questions to assess the quality of each primary study according to selected factors. The answers to these questions each have a value that will measure the quality of each study. In the protocol, it is necessary to define the questions and answers constituting the checklist, as well as the choice of an evaluation strategy. This strategy indicates the number of participants in the process, the validation of results, and the resolution of evaluation conflicts, in the case of several evaluators per study. It is also necessary to define, if applied, a minimum score threshold and the fate of primary studies that have not reached it.

In this section, we list the primary practices and benefits of DevOps/SecOps found in the literature. A recent study was published (Bou Ghantous & Gill, 2017; Senapathi et al., 2018), where we synthesized the practices that DevOps practitioners have applied to date. For SecOps practices, there are only a few articles published in the literature. We have used (Hsu, 2018; Koopman, 2019; Mansfield-Devine, 2018; Mohan et al., 2018). Other studies of DevOps/SecOps practices can be found in the literature (Jabbari et al., 2018; Lwakatare et al., 2019; Prates et al., 2019) but not as comprehensive as that presented in Table 1 which includes the most relevant DevOps/SecOps practices.

TABLE 1
DEVSECOPS PRACTICES

Practice	Description	Reference
Continuous Planning	Business owners will see the growth of the application, so they can give feedback on whether the application is corresponding to their needs.	Jabbari et al., 2018; Hsu, 2018
Security Continuous Integration (SCI)	The developers will check in their code on the source control repository and integrate it with the code from other teams, allowing CI.	Williams, 2018; Shajadi, 2019
Feedback Loops between Dev, Sec and Ops	The goal of this practice is to get as much feedback as possible to perform the necessary corrections.	Nguyen & Dupuis, 2019, Pendyala, 2020
Automated Monitoring	It allows a better perception of the health of the system. This will allow continuous monitoring of the application.	Senapathi et al., 2018; Hsu, 2018
Deployment Automation	These tools facilitate by managing the software components that need to be deployed and what middleware components and	Senapathi et al., 2018; Tomas et al.,

Citation Information: Zaydi, M., & Nassereddine, B. (2020). DevSecOps practices for an agile and secure it service management. Journal of Management Information and Decision Sciences, 23(2), 1-16.

	configurations need to be updated. This will allow for continuous deployment.	2019
Test Automation	Test automation will save some time by performing regression tests to be sure that older functionalities will not be impacted by new developments. This will also allow a continuous testing approach.	Senapathi et al., 2018; Tomas et al., 2019
Continuous Vulnerability Assessment and Remediation	It allows organizations to manage which environments need to be provisioned and configured to enable continuous delivery.	Koopman, 2019; Hsu, 2018
Threat intelligence	The study of adversary operations to devise detective and responsive actions for the organization. Because the organization has limited resources to deploy defense, understanding the techniques that adversaries use allows for effective defenses to be deployed to detect, disrupt, and deceive the attacker.	Mansfield-Devine, 2018; Koskinen, 2019
Stakeholder Participation	The participation of stakeholders will provide more feedback to the SecOps.	Jabbari et al., 2018
Self-assessment	The ongoing assessment of the state of systems and people within the organization. This includes change management and detection; configuration management, vulnerability assessments, penetration testing; and setting up a "red team" to promote effectiveness. These are frequently considered security tasks. But incorporating these tasks into SecOps becomes an effective way to facilitate detection and advise the operational capabilities on the status of the environment. For example, if the vulnerability scan team works with threat intelligence, rapid detection via network security monitoring can be accomplished when new threats or vulnerabilities are discovered. Coordination among these groups in mature SecOps often leads to the discovery of previously unknown threats and vulnerabilities.	Hsu, 2018; Cruzes et al., 2018
Deployment Automation	These tools facilitate by managing the software components that need to be deployed and what middleware components and configurations need to be updated. This will allow for continuous deployment.	Senapathi et al., 2018; Tomas et al., 2019

We also tried to understand the real benefits and challenges of SecOps adoption by organizations. To do this, we analyzed the articles we found in our literature review. The results regarding he benefits and challenges of SecOps are summarized in Table 1.

We have focused on practices that are repeated in the selected papers. We have decided to use this list, assuming that it is the most comprehensive collection of SecOps practices in the literature.

We also tried to understand the benefits of the adoption of DevOps/SecOps by organizations. To do this, we analyzed the articles we found in our literature review. The results of the most adopted DevOps/SecOps practices are summarized in Table 1.

RESEARCH METHODS

The literature review showed that there is a lack of empirical research on the merging of Devops and Secops practices in IT service management. Although most articles did not perform in-depth analyses of security practices for DevOps, the literature has provided a substantial amount of automated controls and agile development that can be used by organizations to control their IT processes. However, no strategy has been developed to address operations security and integrate it effectively into the day-to-day operations of the IT department. The literature review therefore contributed primarily to assess the current state of research in this area. The empirical component of this research should give a more detailed impression of development practices and integrate security measures into operational processes, and above all give a first insight into DevSecops practices that can be used by companies.

Citation Information: Zaydi, M., & Nassereddine, B. (2020). DevSecOps practices for an agile and secure it service management. Journal of Management Information and Decision Sciences, 23(2), 1-16.

Semi-structured Interviews

The case studies were conducted in the form of interviews with the agencies' DevSecops teams. In each case study, at least one interview was conducted. This represented 12 interviews. Interviewees were selected based on their experience with DevSecOps processes in their company and function. The interviews were conducted collectively and individually. The interviews were directional, the interview guide is very detailed (themes, sub-themes...) and before finishing the interview it is necessary to check that each theme has been addressed. The results of these interviews were presented and discussed with the different interviewees in order to validate them. As advised by (Tashakkori & Creswell, 2007), we also used RQs as a way to shape the design of our investigation.

Exploratory research often builds on secondary research, such as reviewing available literature and/or data, or qualitative approaches, such as informal discussions with consumers, employees, management or competitors, and more formal approaches through in-depth interviews, focus groups, projective methods, case studies or pilot studies (Kuruzovich et al., 2012). (Perry et al., 2004) also argues that case studies are a powerful method for exploratory researches because they try to understand and explain the phenomenon or construct theory. (Thomas, 2015) asserts that the researchers should explain or explore a phenomenon, which leads to the following purposes: intrinsic, instrumental, evaluative, explanatory and exploratory. Since the objective of this research is to understand the impacts of a phenomenon, one can conclude that the purpose of this research is exploratory. For this approach, Thomas also suggests the following: testing a theory, building a theory, drawing a picture, descriptive, interpretative, and experimental (Thomas, 2015). As previously stated, no literature was found investigating the relationship between SecOps and Incident Management; therefore, the purpose of this research is to build theory. Some author provides insights about the structure of a CS (Tellis, 1997). Table 1 presents the approach suggested by (Yin, 2009), which will be followed in this research.

Interviews Validation

In order to be able to validate the results of the literature and the various case studies, we conducted a DevSeops practice validation study with international experts in the field of development and security (Whiting, 2008). The experts were selected on the basis of their expertise on the subject of IT Security and/or DevOps. None of the experts was involved in the research as a matter of priority in order to be able to give an unbiased opinion on the results. Telephone and email interviews were conducted to validate the results of the first semi-structured interviews. After each interview, a short report was written summarizing the various comments from the interviews.

Case Study Results

At this stage, we performed interviews to collect practitioners' opinions and experience about the implementation of DevSecOps practices for continual security improvement in ITSM.

Since our RQs aim to explore what or how DevSecOps practices influence the work of professionals in the ITSM process, we used semi-structured interviews. This type of interview is used when one needs to gather more detailed information by giving the interviewees the liberty to express their opinions (Whiting, 2008). To accomplish the triangulation goal, other techniques for data collection were also used, such as data extraction from performance reports and direct observation.

Citation Information: Zaydi, M., & Nassereddine, B. (2020). DevSecOps practices for an agile and secure it service management. Journal of Management Information and Decision Sciences, 23(2), 1-16.

Since our RQs aim to explore what or how DevSecOps practices improve security in the ITSM process, we used semi-structured interviews. This type of interview is used when one needs to gather more detailed information by giving the interviewees the liberty to express their opinions (Whiting, 2008). To accomplish the triangulation goal, other techniques for data collection were also used, such as data extraction from IT Dashboards and direct observation.

In this section, we will briefly describe each organization studied. Most of the respondents mentioned that the DevSecOps teams in their companies had different levels of maturity. A summary of all the companies and interviewees described in the following is given in table 2.

The average experience of the team is about 5 years. Moreover, most of the interviewees have been involved in more than one ITSM project, allowing us to retrieve a range of ideas on best practices.

To validate our interview, we conducted a qualitative study. We have carefully identified five organizations in the MENA region that are either fully or partially implemented DevSecOps practices. Since this research is exploratory we have used a qualitative research method using the five organizations as case studies to identify the best practices for implementing ITIL service transition phase. The above approach enabled us to enquire and ask questions to capture the contributor's rich knowledge, experience and views.

TABLE 2
CASE STUDIES USED IN THIS RESEARCH

Organizations	Org A	Org B	Org C	Org D	Org E
No of employees	700	860	2500	3400	5000
No of IT employees	28	43	95	120	280
Government (Gov.) / Semi-government (Semi)/Private	Semi	Priv.	Priv.	Gov.	Gov.
ITIL Version	V3	V3	V3	V3	V3
Knowledge of ITIL with IT staff / Familiarity	50%	50%	40%	25%	> 30%
Certified ITIL staff	40%	55%	35%	40%	50%
Stage of ITIL Implementation (Fully (F), Largely (L), Partially (P))	P	L	F	F	F
Stage of DevOps/ SecOps Implementation (Fully (F), Largely (L), Partially (P))	P	L	F	F	F
Interviewees	- IT operation Manager - IT Security Manager	- IT Manager - Security Engineer	- IT Project Manager - DevOps Consultant - Security Engineer	- IT Project Manager - Scrum Master - Security Engineer	- IT Project Manager - DevOps Consultant

We have conducted case semi-structured interviews with the organization's IT service managers. Due to the business sensitivity of the information and comments, the real business names of the organizations can't be revealed. The five organizations are referred to throughout the research discussion as cases OrgA-OrgE. Table 2 presents each organization in terms of nature, size, ITIL implementation version, knowledge and experience of ITIL within the staff,

Citation Information: Zaydi, M., & Nassereddine, B. (2020). DevSecOps practices for an agile and secure it service management. Journal of Management Information and Decision Sciences, 23(2), 1-16.

phase of ITIL implementation and SecOps stages implementations. ITIL professionals in these organizations were interviewed and questioned. The interview questionnaire comprises two main parts: part 1 contains questions about the organization demographics (i.e. nature, size, number of IT employees, etc.). Part 2, covers questions about the best practice in implementing each process of ITIL service through DevSecOps practices. Although questions of part 2 are used as a guide throughout the interviews we did not depend on these questions, other developed inquiries and thoughts during the interviews were also discussed.

RESULTS AND DISCUSSION

IT Service Management Process vs SecOps Practices

In this section, interviewees were asked to describe their understanding of the DevSecOps culture and the extent to which they have adopted the different practices. This was done to understand the maturity of their DevSecOps processes and the experience the company had in applying each practice. Several companies indicated that they were still in the implementation phase and we're currently conducting pilot projects. When inquiring about the practices already applied, we made a scale from N/A to 5, where:

- N/A: If the organization is not involved,
- 1: If the action is not implemented or the topic is not addressed,
- 2: If the action is requested or the topic is under consideration;
- 3: If the action is partially implemented and the subject matter is partially addressed, estimated at less than 50%,
- 4: If the action is partially implemented, the subject matter is partially covered and the coverage is estimated to be more than 50%,
- 5: Whether the action is fully implemented or the subject matter is fully addressed.

Table 3 shows the results of these two questions. From Table 3, we can see that the interviewees have considerable knowledge about the existence of DevSecOps practices. From the 10 practices described in Table 1, continuous vulnerability assessment and remediation, and threat intelligence were the only practices that the interviewees had no prior knowledge. Security Continuous Integration (SCI) and Feedback Loops between Dev, Sec and Ops practices are partially implemented.

Furthermore, from Table 3, we can conclude that the most known practices are being implemented. We also noted that there appears to exist a relation between the experience of the interviewee and the practices implemented. For example, deployment automation and stakeholder participation practices are fully implemented by the interviewed organizations. Test automation is being implemented by most of the team, likely because it is an intuitive and easy practice to employ due to the existence of tools that allow this practice.

Given the practical experience and knowledge of the interviewees, we validated our questionnaire on 5 case studies of organizations from different sectors in the MENA region, which have adopted DevSecOps approaches in their IT service management. This gives a better understanding of where each DevSecOps practice can be applied to each phase of the ITSM process.

The analysis shows that the only practice for which respondents did not find a possible correlation was Continuous Vulnerability Assessment and Remediation and the threat intelligence. The respondents' lack of knowledge of the corresponding practice is one of the possible reasons for this finding. Concerning all other practices, interviewees engaged in one or more phases of ITSM service management.

Citation Information: Zaydi, M., & Nassereddine, B. (2020). DevSecOps practices for an agile and secure it service management. Journal of Management Information and Decision Sciences, 23(2), 1-16.

TABLE 3
PRACTICES KNOWN VS FULLY AND PARTIALLY APPLIED

	Continuous Planning	Security Continuous Integration (SCI)	Feedback Loops between Dev, Sec and Ops	Automated Monitoring	Deployment Automation	Test Automation	Continuous Vulnerability Assessment and Remediation	Threat intelligence	Stakeholder Participation	Self-assessment
Org A	4	3	2	3	3	3	1	N/A	4	3
Org B	3	2	2	3	3	4	1	N/A	5	4
Org C	4	3	1	3	4	4	N/A	1	5	4
Org D	5	3	2	3	4	4	1	N/A	4	3
Org E	4	3	2	2	3	3	N/A	1	4	3

The analysis also presents the state of organizations that would benefit from the application of the DevSecOps culture to the ITSM process and how to achieve these benefits. The information collected response to QR1 by describing in more detail the relationship between DevSecOps practices and the phases of the ITSM process, based on the experience of the IT team under study. Such a mapping is a step forward in this area. The resulting data provide us with interesting and new qualitative information to answer QR 1, which gives the respondents' arguments to justify why and how DevSecOps practices can be applied to each phase of the ITSM process. The practices with more correspondences in the different ITSM processes were "Deployment Automation" and "Test Automation," corresponding to 10 practices of ITSM, ie (Service Desk, incident, problem, change, release and deployment, service level, availability, capacity, configuration and security management) different phases of the ITSM. Since most of the processes of incident management, problem management, change management, release management, availability management and configuration management are software development processes, it makes sense for teams applying this process to try to establish a standard for each phase, so that it is easier for all team members to follow it. The test automation framework is used to ensure that tests of new features and incident/problem/change/configuration corrections have the desired quality and that everything is working correctly.

"Stakeholder Participation" is also a recognized practice and widely used by ITSM teams to better manage and deliver a quality end product that meets the expectations of end customers.

Practices that corresponded to fewer ITSM steps were: "Security Continuous Integration (SCI)," "Continuous Vulnerability Assessment and Remediation." These practices correspond to a phase that is "security management." These three practices are known more by security analysts than by developers and helpdesk analysts, despite the interest shown by participants in the need for Security Continuous Integration in service management.

For "Continues Planning," Feedback Loops between Dev, Sec and Ops" and "Self-assessment." The organizations have demonstrated the need to apply these practices to accelerate the delivery of services offered. Nevertheless, the problem lies in the internal culture of IT teams, which largely neglects these practices, which above all requires a high degree of

Citation Information: Zaydi, M., & Nassereddine, B. (2020). DevSecOps practices for an agile and secure it service management. Journal of Management Information and Decision Sciences, 23(2), 1-16.

collaboration between the development, security and operations teams during all stages of design and implementation of the service.

Best Practices Selection (RQ2)

The first research question-answer (RQ1) provided the most relevant DevSecOps practices daily used in the IT Service Management activities. Answering the second question requires a qualitative study that will provide the most relevant ITSM processes. To do so, we used the results obtained from a study that is being finalized for the design of a new information security governance framework, which is the Delphi method (Okoli & Pawlowski, 2004). In the following, the various stages are described, as well as the corresponding results and their evaluation. To achieve the desired result, Delphi covers 7 phases, we have compressed them into 5 as follows:

(I) **Establish experts' selection criteria:** The choice of experts is a crucial step that influences the quality of the results (Adler & Ziglio, 1996), (Bolger & Wright, 1994). As this is not a simple opinion survey, the validity of the results of the Delphi method does not depend on sampling but the knowledge, skills and, above all, the intentional cooperation of the experts consulted; therefore, the choice is based on the professional field of the expert, the duration of experience in IS security, IT management and IT governance, and the number of projects conducted in the said fields; the professional field can be broken down into different statuses, in particular: security managers, analysts, IT project managers with more than 10 years of experience in the implementation of security systems, IT service management and IT projects.

(II) **Prepare and reach out to potential experts:** We used LinkedIn to select the experts, in which the different profiles containing details of both academic and professional career paths, the various positions held with the corresponding durations, the list of IT projects conducted as well as the list of IT certifications, after browsing through LinkedIn more than 100 profiles that corresponded to the established criteria, a list of 76 experts was drawn up on a Word document containing the confidential number assigned to the expert to guarantee his anonymity, e-mail address, function, company name, telephone number and country of residence.

(III) **Invite experts to participate to the study:** in this step we reached the experts listed in step 2 by the LinkedIn online messenger when they express their collaboration and willingness to participate in our study, we move on to step IV.

(IV) **Manage and consolidate answers:** Of the 76 potential experts targeted, 18 of them, from 13 countries (England, Australia, Morocco, Canada, United States, Spain, Estonia, Finland, Hungary, India, Portugal, Switzerland, Thailand) accepted to participate in our Delphi survey, therefore the validation condition required by the Delphi method is met with this number of participants. At this stage, questions (175 questions covering aspects of all ITSM processes described in the ITIL repository) are sent to the experts, three rounds of the Delphi survey were necessary to reach a consensus on the questions. To assess the degree of consensus of participants, we adopted and adapted the Likert scale (Subedi, 2016), which includes 6 answers: Strongly agree (6), agree (5), somewhat agree (4), neutral (3), disagree (2) and strongly disagree (1); each expert had to provide one of these answers according to his or her experience.

(V) **Assess results:** To analyze the data for consensus and divergence, we opted for the following measures: For each expert, these numerical responses are entered into a spreadsheet that will calculate descriptive statistics:

Me: the median of each proposal;

Citation Information: Zaydi, M., & Nassereddine, B. (2020). DevSecOps practices for an agile and secure it service management. Journal of Management Information and Decision Sciences, 23(2), 1-16.

EAM: the absolute deviation from the median;

Using the following equation:

$$EAM = \frac{|\sum_i^n X_i - M|}{n}$$

Where,

Xi: the degree of the proposal appreciated by the expert i;

M: median of the proposal;

n: total number of experts.

To measure the degree of consensus or divergence for each process and control, it is possible to use a threshold EAM, an EAM less than or close to 1 synonymous with consensus [6, 7] and/or to analyze the dispersion of the responses:

%IIQ: the percentage of responses in the range [q1; q3];

Consensus: $4 < Me < 7$ $0,6 < EAM < 1$

Without consensus: $3 < Me < 5$ $1,1 < EAM < 1,8$

TABLE 4
CUSTOMIZED DELPHI METHOD

Q1	exp 1	exp 2	exp 3	exp 4	exp 5	exp 6	exp 7	exp 8	exp 9	exp 10	exp 11	exp 12	exp 13	exp 14	exp 15	exp 16	exp 17	exp 18	M	EAM	Error%
Tour1	4	5	4	3	5	3	5	3	3	3	5	5	6	3	5	4	5	5	4,222	1,003	23,761
Tour2	5	6	5	4	3	5	4	4	4	4	5	4	5	5	6	5	6	5	4,722	0,826	17,501
Tour3	5	6	6	6	6	6	5	4	5	5	5	5	6	5	6	5	6	6	5,444	0,616	11,309

Which leads to the following measurable consensus results (Table 5):

TABLE 5
CONSENSUS REACHED AROUND THE 3 ISS-GOV DISCIPLINES OF THE 3 ROUNDS

	Me	**EAM1**	**EAM2**	**EAM3**	**IM1%**
Q1	4.8	1	0.82	0.61	76%
Q50	3.3	1.79	1.55	1.31	46%

The statistical analysis revealed two main groups of processes: Q1 which has consensus (rather a strong median between 4 and 7, with small deviations from the median between 0.6 and 1) and Q50 (corresponds to the supplier management process of the ITIL Service Design Phase) has disagreement (weak medians between 3 and 5, with strong deviations from the median between 1.1 and 1.7). The Table 4 above gives the example of the figures for Q1 (with consensus) and Q50 (without consensus), corresponds to the process "supplier management". And we have proceeded in the same way for the other questions, we have had the following processes that reached a consensus; Service level management, Availability management, Capacity management, service continuity management, Change management, Release

Citation Information: Zaydi, M., & Nassereddine, B. (2020). DevSecOps practices for an agile and secure it service management. Journal of Management Information and Decision Sciences, 23(2), 1-16.

management, Configuration management, Incident management, Problem management, Service desk and access authorization.

MERGING RESULTS OF RQ1 AND RQ2

The desired results obtained from the first question identified the relevant practices used in IT service management daily tasks. While the results of the second research question provided us with the relevant ITSM practices judged appropriate and validated by experts in the field.

At this stage, we can design a secure and agile ITSM aligned with the needs and objectives of all organization stakeholders including the core business team, the development team, the operational team and the security team, so that they can start working together to co-create value, meet business needs and objectives in an agile and secure way while having a single integrated team.

Figure 2 shows the conceptual model of this new secure and agile ITSM concept composed of the most relevant DevSecOps practices and ITSM processes.

The final conceptual model is divided into four dimensions: the first one is about DevOps in its organizational and cyclical aspect, now ITSM will be both cyclic and continuous. The second dimension is about implementing and managing the relevant ITSM practices, the third dimension is about security which will become an integral part of IT service management and the last dimension is a managerial aspect that also will be part of the whole process from planning to value delivery. Now the Business, DevOps, Operations and Security can be aligned and at the same level, sharing the same philosophy, the same terminology, the same objectives and using the same tools, as shown in Figure 3:

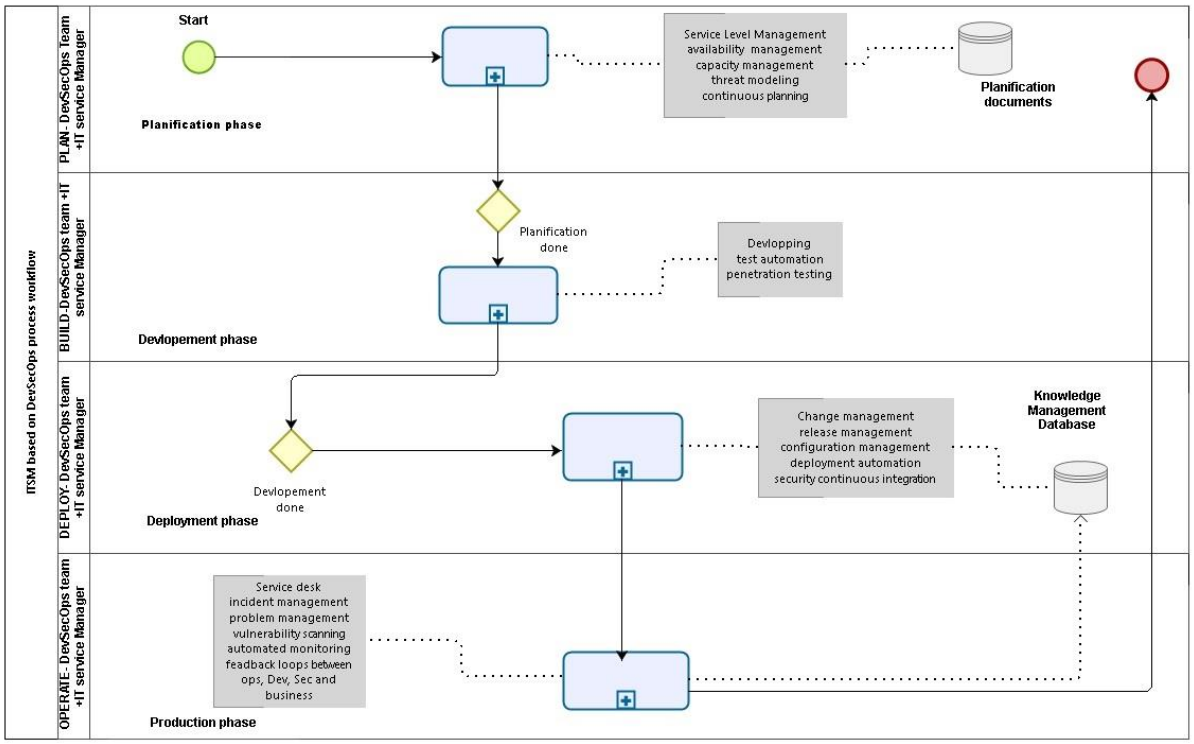

FIGURE 2

ITSECAG-SM, THE NEW COSTUMED ITSM AGILE AND SECURE

Citation Information: Zaydi, M., & Nassereddine, B. (2020). DevSecOps practices for an agile and secure it service management. Journal of Management Information and Decision Sciences, 23(2), 1-16.

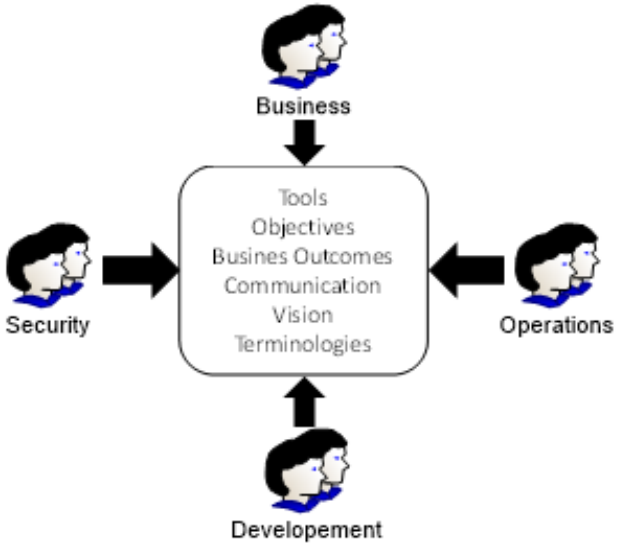

FIGURE 3

OBJECTIVES ALIGNMENT BETWEEN, BUSINESS, OPS, DEV. AND SECURITY

Now we can design a secure and agile custom ITSM, the new cycle of managing a service is about to go through 4 major cyclical phases of DevOps (the organizational aspect), a planification involving reaching consensus on the service level agreement with the customer, resource availability, capacity management for the new service, hence, a security practice is positioned in this stage, I called threat modeling, using abstractions to facilitate reflection on risks. A threat model identifies security threats affecting IT services and/or their components (software and hardware) and provides the capabilities to address or mitigate them in the context of a use case, and ideally during development, this phase is transversal, it can be re-planned at any time to adjust the desired service. A planning deliverable, when completed, is ready for the second phase, which is development itself, so during this phase, we have integrated some game-changing security practices, such as penetration testing, which simulates a cyber-attack with a well-defined scope, to check for exploitable vulnerabilities and determine their severity. Pentesting aims to find as many vulnerabilities and configuration issues as possible, within the time allowed, and then try to exploit them to determine the risk of the vulnerability. The automation of testing planned at this level, once the product is done, tested we proceed to its deployment. At this level, several practices come into play to successfully put the system into production, in particular change, release and configuration management, as well as a gradual automated deployment. Integration of security at this stage is therefore conceivable via the practice "security continuous integration", once deployed, the system can be used and operated daily in a production environment and here we distinguish several practices that coexist in terms of operation, service center and security, including incident and problem management, vulnerability scanning to provide results on new vulnerabilities affecting ITSM and provide solid data on their level of severity. This data must be fed into the vulnerability management system and prioritized based on common scoring mechanisms, followed by analysis and feedback between the teams involved in this new approach, namely the development, security, operations and IT service managers. The key to success depends on the co-operation and collaboration that had just been established between these teams with this new management vision.

Citation Information: Zaydi, M., & Nassereddine, B. (2020). DevSecOps practices for an agile and secure it service management. Journal of Management Information and Decision Sciences, 23(2), 1-16.

CONCLUSION AND FUTURE WORKS

This study aimed to explore the possibilities for companies to manage these IT operations, development and security and increase process control while using DevSecOps without sacrificing too much of the agility and benefits that DevOps offers. Second, it aimed to study how these companies can exploit DevSecOps practices in the management of their IT operations. Demonstrate their internal control to IT auditors.

We conducted two main research questions. The first What DevSecOps practices can be used in IT Service Management. And the second, how can these practices be integrated into effective IT Service Management?

To answer this question, we conducted a literature review to define the most common DevSecOps practices. An exploratory study was then carried out through 5 case studies. The results of this study were evaluated with 18 experts who responded to the case studies.

All respondents were generally positive about the use of DevSecOps, although opinions differed widely on what DevOps is and how it should be handled. It, therefore, seems impossible to develop a framework with which all those involved in DevOps would fully agree.

This study provided a comprehensive overview of practices that can be applied in DevSecOps for ITSM. These practices include both traditional practices that can be used in combination with DevOps, as well as security practices integrated into the application development process. The most complicated practices have been classified into several categories: Continuous Vulnerability Assessment and Remediation, the threat intelligence and Feedback Loops between Dev, Sec and Ops.

The validation results of this study with the Delphi method proved the most relevant DevSecOps practices for effective ITSM. The results of this study resulted in a conceptual model of IT Service Management based on DevSecOps practices.

For future work, we are currently working on the validation of this model through the projection of DevSecOps practices on ITSM practices, and more specifically the change management process in organizations.

REFERENCES

Abdelkebir, S., Maleh, Y., & Belaissaoui, M. (2017). An agile framework for its management in organizations: a case study based on DevOps. *Proceedings of the 2Nd International Conference on Computing and Wireless Communication Systems*, 67, 1-8.

Adler, M., & Ziglio, E. (1996). *Gazing into the oracle: The Delphi method and its application to social policy and public health*. Jessica Kingsley Publishers.

Bi, R., Davidson, R., Kam, B., & Smyrnios, K. (2013). Developing organizational agility through it and supply chain capability. *Journal of Global Information Management, 21*(4), 38–55.

Bolger, F., & Wright, G. (1994). Assessing the quality of expert judgment: Issues and analysis. *Decision support systems, 11*(1), 1-24.

Bou Ghantous, G., & Gill, A. (2017). DevOps: concepts, practices, tools, benefits and challenges. *Proceedings PACIS2017*, 96.

Cruzes, Daniela S., Jaatun, Martin G., ET Oyetoyan, Tosin DT. D (2018, April). Challenges and approaches of performing canonical action research in software security. *Proceedings of the 5th Annual Symposium and Bootcamp on Hot Topics in the Science of Security*, 1-11.

Ebert, C., Gallardo, G., Hernantes, J., & Serrano, N. (2016). DevOps. *IEEE Software, 33*(3), 94-100.

Hsu, T. H. C. (2018). *Hands-On Security in DevOps: Ensure continuous security, deployment, and delivery with DevSecOps*. Packt Publishing Ltd.

Jabbari, R., bin Ali, N., Petersen, K., & Tanveer, B. (2018). Towards a benefits dependency network for DevOps based on a systematic literature review. *Journal of Software: Evolution and Process, 30*(11), e1957.

Kitchenham, B. et Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering*. Rapport technique EBSE 2007-001, Keele University and Durham University Joint Report.

Koopman, M. (2019). *A framework for detecting and preventing security vulnerabilities in continuous integration/continuous delivery pipelines*. Master's Thesis, University of Twente.

Citation Information: Zaydi, M., & Nassereddine, B. (2020). DevSecOps practices for an agile and secure it service management. Journal of Management Information and Decision Sciences, 23(2), 1-16.

Kuruzovich, J., Bassellier, G., & Sambamurthy, V. (2012). IT governance processes and IT alignment: viewpoints from the board of directors. *In 2012 45th Hawaii International Conference on System Sciences*, 5043-5052.

Lwakatare, L. E., Kilamo, T., Karvonen, T., Sauvola, T., Heikkilä, V., Itkonen, J., Lassenius, C. (2019). DevOps in practice: A multiple case study of five companies. *Information and Software Technology, 114*, 217-230.

Koskinen, A. (2019). *DevSecOps: building security into the core of DevOps*. Masters Thesis, University of Jyväskylä.

Maleh, Y., Sahid, A., & Belaissaoui, M. (2019). *Strategic IT governance and performance frameworks in large organizations*. IGI Global.

Mansfield-Devine, S. (2018). DevOps: finding room for security. *Network Security, 2018*(7), 15–20.

Mohamed, N., & Kaur, J., & Singh, G. (2012). A conceptual framework for information technology governance effectiveness in private organizations. *Information Management & Computer Security, 20*(2), 88-106.

Mohan, V., Othmane, L. ben, & Kres, A. (2018). BP: security concerns and best practices for automation of software deployment processes: an industrial case study. *In 2018 IEEE Cyber security Development (SecDev),* 21-28.

Moore, G., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research, 2*(3), 192.

Nazımoğlu, Ö. & Özsen, Y. (2010). Analysis of risk dynamics in information technology service delivery. *Journal of Enterprise Information Management, 23*(3), 350-364.

Nguyen, J., & Dupuis, M. (2019). Closing the feedback loop between ux design, software development, security engineering, and operations. *Proceedings of the 20th Annual SIG Conference on Information Technology Education*, 93-98.

Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: an example, design considerations and applications. *Information & management, 42*(1), 15-29.

Pendyala, V. (2020). Evolution of integration, build, test, and release engineering into devops and to DevSecOps. In *Tools and Techniques for Software Development in Large Organizations: Emerging Research and Opportunities* (pp. 1-20). IGI Global.

Perry, D. E., Sim, S. E., & Easterbrook, S. M. (2004). Case studies for software engineers. *Proceedings. 26th International Conference on Software Engineering*, 736-738.

Prates, L., Faustino, J., Silva, M., & Pereira, R. (2019). DevSecOps metrics BT- information systems: research, development, applications, education. In S. Wrycza & J. Maślankowski (Eds.) (pp. 77–90). Cham: Springer International Publishing.

Read, W., Report, T., & Takeaways, K. (2016). *Agile and DevOps adoption drives digital business success*. Forrester Research.

R. J. Wieringa (2014), *Design science methodology for information systems and software engineering*. Springer-Verlag Berlin, Heidelberg.

Sahid, A., Maleh, Y., & Belaissaoui, M. (2018). A practical agile framework for IT service and asset management ITSM/ITAM through a Case Study. *Journal of Cases on Information Technology, 20*(4), 71-92.

Senapathi, M., Buchan, J., & Osman, H. (2018). DevOps capabilities, practices, and challenges: insights from a case study. *Proceedings of the 22Nd International Conference on Evaluation and Assessment in Software Engineering 2018*, 57-67.

Shajadi, A. (2019). *Automating security tests for web applications in continuous integration and deployment environment*. https://www.theseus.fi/handle/10024/166541

Subedi, B. P. (2016). Using Likert type data in social science research: Confusion, issues and challenges. *International journal of contemporary applied sciences, 3*(2), 36-49.

Tashakkori, A., & Creswell, J. W. (2007). Exploring the nature of research questions in mixed methods research. *Journal of Mixed Methods Research, 1*(3), 207-211.

Tellis, W. M. (1997). Application of a case study methodology. *The Qualitative Report, 3*(3), 1-19.

Thomas, G. (2015). *How to do your case study*. SAGE Publications.

TOMAS, Nora, LI, Jingyue, et HUANG, Huang (2019). An empirical study on culture, automation, measurement, and sharing of DevSecOps. *Proceedings 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). IEEE*, 1-8.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS quarterly, 26*(2), 13-23.

Whiting, L. S. (2008). Semi-structured interviews: guidance for novice researchers. *Nursing Standard, 22*(23), 35-41.

Williams, L. (2018). Continuously integrating security. *In Proceedings of the 1st International Workshop on Security Awareness from Design to Deployment*, 1-2.

Citation Information: Zaydi, M., & Nassereddine, B. (2020). DevSecOps practices for an agile and secure it service management. Journal of Management Information and Decision Sciences, 23(2), 1-16.

Yin, R. K. (2009). *Case study research: design and methods*. Applied Social Research Methods Series, 5. SAGE Publications.

Citation Information: Zaydi, M., & Nassereddine, B. (2020). DevSecOps practices for an agile and secure it service management. Journal of Management Information and Decision Sciences, 23(2), 1-16.