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. This research provides novel findings of a possible relation between DevSecOps practices and IT service management controls as well as on "why" and "how" can these practices help ITSM. The novelty of the findings brings advantages for academics, and due to the exploratory nature of this research, it extends the body of knowledge. It also provides contributions for practitioners, by showing how these practices can be applied and the result of the implementation of these practices.

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).

To remain competitive, organizations must respond to the dynamic changes that markets require, to provide better customer experience and to innovate with new services and products (Tiwana & Konsynski, 2010). Part of these dynamic changes is based on technological advances. 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,

Citation Information: Zaydi, M., & Nassereddine, B. (2019). DevSecOps practices for an agile and secure it service management. *Journal of Management Information and Decision Sciences, 22*(4), 527-540.

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., 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 to 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 & 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 What are the benefits of using DevSecOps practices in IT Service Management?

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 and DevSecOps activities those 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 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;
- DevSecOps practices benefits for ITSM;

Citation Information: Zaydi, M., & Nassereddine, B. (2019). DevSecOps practices for an agile and secure it service management. *Journal of Management Information and Decision Sciences, 22*(4), 527-540.

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

This research aims to study the application of DevSecOps in the ITSM process. It is mandatory to search literature where it is possible to analyze the outcomes from DevSecOps applications and findings where DevOps was applied to the ITSM process. However, since DevSecOps is a new culture (Ebert et al., 2016), we decided to study existing studies linking these two domains through an in-depth literature review analysis.

To perform the literature review, we have searched and consulted the following digital libraries such as IEEE Explore, ACM, Research Gate and the search engine Google Scholar. Since this research focusses on IT service operation management, we have also searched for interesting studies amongst the top journals regarding service management, ITSM and operation management domains. These journals were found by searching in Scimago, a scientific journal-ranking website.

Moreover, this research took place between January 2019 and June 2019, but we have maintained currency to date. The keywords used to perform this research were as follows: DevSecOps case studies; IT security management; DevSecOps benefits; DevSecOps practices; DevOps; SecOps; ITSM; ITSM frameworks. To select the articles for this research, we tried to keep to relevant parameters, like the application domain, benefits, practical cases or researches and definitions.

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 (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.

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 the 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.

Citation Information: Zaydi, M., & Nassereddine, B. (2019). DevSecOps practices for an agile and secure it service management. *Journal of Management Information and Decision Sciences, 22*(4), 527-540.

TABLE 1
DEVSECOPS PRACTICES

Practice name	Description
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).
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).
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).
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).
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).
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).
Continuous Vulnerability Assessment and Remediation	It allows organizations to manage which environments need to be provisioned and configured to enable continuous delivery (Koopman, 2019).
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).
Stakeholder Participation	The participation of stakeholders will provide more feedback to the SecOps teams (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).
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).

RESEARCH METHODOLOGY

In the early stages, as stated in the previous section, the nature of this research is exploratory. It is meant to start a study on a determined phenomenon observed, where there are no prior (or few) works (Gagnon, 2010). Zainal, (2007) argues that "a case study (CS) enables the researcher to examine the data within a specific context". Moreover, a CS is built around a question (Thomas, 2015) which in this case is, "How do SecOps affect Continuous Security Improvement in IT Service Management"?. Thomas (2015) argues that this question is the subject of the CS, but the CS also should be defined on its purpose, approach and process. Moreover, the subject may lead to three different types of CSs: special or outlier (when the researcher tries to study a phenomenon that occurs frequently), a key case (when the researcher is studying a

Citation Information: Zaydi, M., & Nassereddine, B. (2019). DevSecOps practices for an agile and secure it service management. *Journal of Management Information and Decision Sciences, 22*(4), 527-540.

phenomenon that happens a lot), and a local knowledge case (where the researcher is investigating something familiar to him) (Thomas, 2015). This CS is classified as a local knowledge case since the researchers of this study work on a team that applies SecOps practices and use ITSM practices. More information regarding this team can be found in (Yin, 2009), which argues that questions like "what" is exploratory since the purpose is to develop propositions for further inquiry, which fits the questions that were previously stated. A CS also has "how" and "why" questions, where the researcher does not have control over the variables, which suits this research (Perry et al., 2004). We decided to formulate two research questions that this research intends to answer. A research question (RQ) concentrates on the uncertainty that the researcher wants to investigate and solve (Thabane et al., 2009). 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 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 (2015) also suggests the following methodology for qualitative research studies: action research, comparative research, evaluation, experiments, and case studies. As previously stated, no literature was found investigating the relationship between SecOps and ITSM with regard to the security part.

Data Collection Methods

It is very crucial to determine the necessary skills to conduct the CS and develop a protocol where an extensive reading about the topic should be done, to create some draft questions. Tellis (1997) uses Yin (2009) as an example arguing that researchers should be good listeners and have the right interpretation of the responses.

In this research, the most required skill is to have a good knowledge of the ITSM process and security practices; thus, we can interpret the results and know what to ask the target audience. For the CS protocol, we performed an extensive literature review about the ITSM process and SecOps and security practices to reach a deep understanding of these domains and how they have been applied so far. To support the interviews, a question 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 5 MENA organizations that are adopting DevSecOps in their ITSM daily activities. This choice of this region concerns the accessibility of information and respondents. This study will provide an accurate snapshot of the state of adoption of the DevSecOps culture applied to ITSM in the MENA region. In the future, we plan to extend this study to an international scale.

Citation Information: Zaydi, M., & Nassereddine, B. (2019). DevSecOps practices for an agile and secure it service management. *Journal of Management Information and Decision Sciences, 22*(4), 527-540.

We noted that the majority of respondents expressed the potential of common DevSecOps such as automated monitoring to improve ITSM. This research provides novel findings of a possible relation between DevSecOps practices and IT service management controls as well as on "why" and "how" can these practices help ITSM. The novelty of the findings brings advantages for academics, and due to the exploratory nature of this research, it extends the body of knowledge. It also provides contributions for practitioners, by showing how these practices can be applied and the result of the implementation of these practices. To support the interviews, a questionnaire was built.

Data Analysis

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.

The interviews had been performed with members and ex-members of an ITSM team for anonym corporation (for reasons of confidentiality, we were unable to disclose the company's identity). All the team members work for the same corporation, and they work on the same project as consultants. This team uses several software in their daily tasks: LANDESK Service Desk to manage incidents, problems, requests and changes; LANDESK Management Suite as a code repository and to perform configuration items (CI), for building changes and packages of the code checked and to perform the installation of packages.

Observation can be seen as structured or unstructured (Thomas, 2015). Structured observation occurs when the researcher systematically looks for particular kinds of behaviors, while unstructured observation happens when the researcher informally observes important details of what is happening (Thomas, 2015). Unstructured observation may also be called participant observation, where the researcher is also a participant. The kind of observation that should be used in this research is unstructured observation since the observation will only be used to validate some of the results of the interviews, such as taking notes. We also analyzed some performance reports on team performance discrepancies that this team produced weekly to present to business users.

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.

At the end of the CS, we have interviewed a sample of 12 (We have chosen the maximum number of profiles that are involved in the ITSM.). Members from the team we worked with. The details about each interviewee are listed 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.

Citation Information: Zaydi, M., & Nassereddine, B. (2019). DevSecOps practices for an agile and secure it service management. *Journal of Management Information and Decision Sciences, 22*(4), 527-540.

TABLE 2
INTERVIEWEE LIST

Interviewee	Position	Experience (years)	Experience in IT (years)	Experience in ITSM (years)	Projects in ITSM
A	Developer	4	4	3	2
B	Developer	4	4	3	2
C	Developer	3	3	2.5	2
D	Support Analyst	5	5	4	3
E	Support Analyst	5	5	3.5	3
F	IT Service Manager	4	4	4	3
G	Security Analyst	4	4	3.5	3
H	Security Analyst	3	3	3	2
I	Team Leader	7	6	5	5
J	IT Security Manager	12	10	10	5
K	IT Delivery Manager	10	10	8	8
L	Asset Manager	6	5	4.5	4.5

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 phases. The above approach enabled us to enquire and ask questions to capture the contributor's rich knowledge, experience and views.

TABLE 3
CASE STUDIES USED IN THIS RESEARCH

Organizations	Org_001	Org_002	Org_003	Org_004	Org_005
No of employees	700	860	2500	3400	5000
No of IT employees	28	43	95	120	280
Government (Gov.)/Semi-government (Semi)/Private (Priv.)	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

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 Org_001-Org_005. Table 3 presents each organization in terms of nature, size, ITIL implementation version, knowledge and experience of ITIL within the staff, 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

Citation Information: Zaydi, M., & Nassereddine, B. (2019). DevSecOps practices for an agile and secure it service management. *Journal of Management Information and Decision Sciences, 22*(4), 527-540.

of ITIL service through SecOps practices. Although questions of part 2 are used as a guide throughout the interviews we did not totally depend on these questions, other developed inquiries and thoughts during the interviews were also discussed.

RESULTS AND DISCUSSION

On the questionnaire, we asked some basic questions about DevSecOps, like what practices the interviewee knows about and what they apply or had applied on previous/current projects. When inquiring about the practices already applied, we made a scale from 0 to 2, where 0 meant didn't apply, 1 meant partially applied and 2 meant fully applied. One should assume partial implementation as a practice that is incomplete or could not be implemented in the entire context it was expected to work. For example, for deployment automation, a developer cannot use the deployment automation tool for production deployments while a team leader has permission to do it.

Table 4 shows the results of these two questions. From this table, we can see that the interviewees have considerable knowledge about the existence of SecOps practices. From Table 4 continuous vulnerability assessment, remediation, and threat intelligence were the only practices that the interviewees had no prior knowledge. Furthermore, from Table 4, we can conclude that the most known practices are being fully or partially applied. We also noted that there appears to exist a relation between the experiences of the interviewee and the practices implemented. For example, the deployment automation practice is fully applied by interviewees A, B, E, F, G, H, I, J, K and L, while the others only applied it partially. Test automation is being fully applied 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.

IT Service Management Process *vs* SecOps Practices

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 where each DevSecOps practice can be applied to each phase of the ITSM process.

The analyses 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.

The analyses also present 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,

Citation Information: Zaydi, M., & Nassereddine, B. (2019). DevSecOps practices for an agile and secure it service management. *Journal of Management Information and Decision Sciences, 22*(4), 527-540.

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.

TABLE 4
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	Total	Percentage
Practices Known												
A				●	●	●					*3/10*	*30%*
B		●	●		●	●			●		*5/10*	*50%*
C			●		●	●					*3/10*	*30%*
D	●			●	●				●	●	*5/10*	*50%*
E	●		●						●		*3/10*	*30%*
F	●	●	●		●		●	●	●	●	*8/10*	*80%*
G	●	●	●	●		●	●	●			*7/10*	*70%*
H	●		●	●	●	●	●		●		*7/10*	*70%*
I	●	●	●	●	●	●			●	●	*8/10*	80%
J	●	●	●	●			●	●	●	●	*8/10*	80%
K	●	●	●	●	●	●			●	●	*8/10*	80%
L	●		●	●	●	●			●	●	*7/10*	70%
Total	**9**	**6**	**10**	**8**	**9**	**8**	**4**	**3**	**9**	**6**		
Practices Fully vs Partially Applied												
A			●	◖	◖	●			◖		*2.5/10*	*25%*
B			◖	●	◖	●			◖	●	*4.5/10*	*45%*
C	◖		●	◖	◖	◖			●	◖	*4.5/10*	*45%*
D	●		●	◖		◖			●		*4/10*	*40%*
E	●		●	●	◖	●			●		*5.5/10*	*55%*
F	◖	◖	●	●	◖	●	◖		◖	◖	*6/10*	*60%*
G	◖		◖		◖		●	●			*3.5/10*	*35%*
H	●	◖	◖	◖		●	●	●	◖	●	*7/10*	*70%*
I	●	◖	●	◖	◖	●			◖	●	*6/10*	*60%*
J	●	◖		●		●	●	●	◖	◖	*6.5/10*	*65%*
K	◖	◖	◖	◖	◖	●	◖		●	◖	*5.5/10*	*55%*
L			◖	●	●	●			◖	◖	*4.5/10*	*45%*
Total	**7**	**2.5**	**8.5**	**8**	**4**	**10**	**4**	**3**	**7.5**	**5.5**		

"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.

Citation Information: Zaydi, M., & Nassereddine, B. (2019). DevSecOps practices for an agile and secure it service management. *Journal of Management Information and Decision Sciences, 22*(4), 527-540.

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

SecOps Benefits (RQ2)

To find the benefits that the SecOps practices brought to this team, we have asked the interviewees, "Why have you started to apply this practice?" to determine its benefits as viewed by the participants. The answers are provided in Table 5 and serve as the answer to RQ2. In this table, we show the number of matches and some quotes from the interviewees citing their justifications.

Analyzing this table, we tried to identify keywords that could translate into generic benefits of each practice. The keywords identified were the following: feedback, mitigate, impact, alignment, and quality. By looking at Table 4, these words are used mainly by the interviewees in several practices. For better understanding, we highlighted these keywords on the quote's column of Table 5.

In analyzing the table provided in Table 5 it is possible to find that there is a relationship between these keywords and the practices, which enabled us to investigate the benefit behind that practice.

Based on the same table, we were able to elicit and synthesize the benefits described by the interviewees for each practice, as shown in the Table 5.

After analyzing Table 4, we summed up the benefits of SecOps adoption in the ITSM process, raising 5 major concepts, ie feedback, impact, alignment, quality and mitigate which were possible to map with the benefits identified in the literature review. This can be seen in Table 5.

Participants identified the quality of service delivery (software, hardware...) in several areas. The quality of service delivery is essential for each development team. The quality of service delivery should not be measured at the time of product delivery, but during all stages up to delivery: requirements collection, design, construction, testing. If quality is improved in all phases, the quality of software delivery will be higher.

The commitment of all stakeholders to the application is a crucial success factor for the application. Everyone, including business users, developers, IT security teams, operators, managers, etc., have to be aligned; otherwise, the success of the application will not be maximized.

The objective of each project is to bring value to the company. Based on the quotes from interviewees, they strive to obtain feedback from the company and provide feedback to companies to improve them. They know that the company depends on applications and since they are responsible for maintaining these applications, they try not only to repair them but also to improve

Citation Information: Zaydi, M., & Nassereddine, B. (2019). DevSecOps practices for an agile and secure it service management. *Journal of Management Information and Decision Sciences, 22*(4), 527-540.

them and avoid potential problems. They implement practices that help them quickly find problems to minimize impacts and even find them before they occur.

TABLE 5
PRACTICES, KEYWORDS, AND QUOTES

Practice	Keywords	Interviewee Alphabet code	# of Matches	Quotes
Continuous Planning	Feedback Impact	A, B, E, D, F, L	6	"Receive **feedback** from the customer as soon as possible to improve the management of the service center if necessary."
				"Show the progress of developments at the company to see if a new plan is needed."
				"Plan for the medium to long-term to ensure continuous delivery."
				"Meetings have been held to redefine priorities if necessary."
				"Due to changes in requirements due to developments."
				"Meetings are held to discuss the most critical incidents/problems and changes on the pipeline to be resolved."
Security Continuous Integration (SCI)		B, E, F, G	4	"Making security testing an integral part of continuous integration reinforces the security standards of your ITSM and identifies security as a key **quality** attribute of your project."
				"Making this decision at the beginning of a new project allows development and operations managers to make informed decisions on architecture, design, and implementation with full consideration of the necessary security requirements."
				"To keep the integrity to decrease the number of errors to ensure the **quality** of the software"
				"Due to the increase of deliveries by all the teams, it's needed to have all the code integrated to avoid that the code gets overwritten and guarantees the Security **alignment** between teams"
Feedback Loops between Dev, Sec and Ops	Feedback Impact Alignment	B, F, I, K	4	"To **mitigate** errors on deployment activities and enhance recovery activities"
				"To guarantee a better security **alignment** between teams."
				"Getting **feedback** from other teams."
				"There are knowledge transfer sessions between the Dev's, Sec's and the Ops where the dev's share their new developments; so, the Sec' test dev in terms of
				vulnerabilities and the ops could share their concerns on
Automated Monitoring	Impact Quality	A, G, H, J, L	5	"To monitor system health."
				"It verifies the system health before, during, and after the deployments"
				"Saves time and finds new issues."
				"Saves time and find issues introduced by new software deliveries or middleware issues, ensuring **quality**" "Finds issues in preliminary stages, causing less **impact** to businesses."
Deployment Automation	Mitigate Quality	A, B, D, E, I, L	6	"**Mitigates** human error, and the process becomes standard."
				"Saves time for the developers by deploying their changes to test environments"

Citation Information: Zaydi, M., & Nassereddine, B. (2019). DevSecOps practices for an agile and secure it service management. *Journal of Management Information and Decision Sciences, 22*(4), 527-540.

				"Saves time and makes a standard process that everyone will follow."
				"Helps in the deployment reducing human error" "**Mitigate**s the human error."
				"Saves time and **mitigates** human error."
Test Automation	Mitigate Impact Quality	A, B, E, J, K	5	"**Mitigates** the risk of breaking existing functionalities." "So, the regression tests can be done more severely." "More **quality** on testing."
				"Guarantees a rigid regression test plan was verifying that the new developments will not result in new errors on the software."
				"Regression tests are made to guarantee the **quality** of the solution."
Continuous vulnerability assessment and remediation		A, F, I	3	"Run automated vulnerability scanning tools against all systems on the network and applications frequently."
				"Ensure that all vulnerability scanning is performed in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested."
				"Deploy automated patch management tools and software update tools for the operating system and third-party software on all systems."
Threat intelligence	Mitigate Feedback	D, G	2	"Threat intelligence is the knowledge that allows you to prevent or **mitigate** cyber-attacks."
				"Threat intelligence can be used to inform decisions with a **feedback** regarding the subject's response to that menace or hazard."
Stakeholder Participation	Feedback Alignment	F, L	2	"Provides continuous feedback on the existing processes"
				"Helps in understanding the needs of the business."
Self-assessment	Mitigate Feedback	E, J	2	"Self-assessment involves typical tasks; however, incorporating these tasks in the SecOps organization **mitigates** risk by promoting threat detection and informing the operational team of the organization's security environment."
				"Receiving **feedback** from security teams"

The concept behind SecOps is to reach operators, developers, and security. By joining these three working groups, they will share their knowledge, which will create more competent professionals who are able to work for both working groups.

Based on the participants' comments, the SecOps canvas is not being adopted at this time. IT teams tend to confuse SecOps with DevOps. But they confirm the need for a security approach in software development and applications and IT service management in general.

CONCLUSION

The objective of this paper is to make contributions to the academic community by exploring an area that has not yet been explored, improving the body of knowledge and establishing new baselines for further research.

This research contains a set of data collected from interviews with IT professionals who applied DevOps practices while working with the ITSM process and resolving incidents and collected from the performance documentation provided by this team. From these interviews and

Citation Information: Zaydi, M., & Nassereddine, B. (2019). DevSecOps practices for an agile and secure it service management. *Journal of Management Information and Decision Sciences, 22*(4), 527-540.

documentation, it can be concluded that these practices can contribute to improving the performance of the ITSM team as well as engagement with professional users by involving them in the solutions provided by the ITSM team.

Due to automation practices such as testing and deployment, respondents also indicated that they could meet and fulfill the expectations of more emergency changes, thus contributing to the agility and security of the application and resolving more quickly incidents that cause more impact. They also shared that they would like to fully apply some practices such as Continuous Vulnerability Assessment and Remediation, the threat intelligence and self-assessment because they understand that by using this, they would have more benefits. Most of the practices have been implemented at the request of the ITSM team client, but some of them, such as feedback loops between development, security and operations, and process standardization, are practices that team management encourages to put into practice because of the improved performance that these practices can provide. Besides, due to feedback loops, the ITSM team could raise some concerns about new developments, which would contribute to the quality of new developments and avoid future security issues.

Future work could involve interviews with other professionals to refine the results of this research. Besides, other researchers can also study how DevSecOps practices can be applied in each ITIL process separately. This is an objective that we intend to pursue shortly, for example the incident, problem, and change management process. Besides, further research is proposed to explore other challenges in the implementation of SecOps, as more researchers are exploring its benefits.

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.

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.

Bou Ghantous, G., & Gill, A. (2017). DevOps: Concepts, Practices, Tools, Benefits and Challenges. *Proceedings of the Pacific Asia Conference on Information Systems (PACIS-2017)*, 1-12.

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

Gagnon, Y. C. (2010). *The case study as research method: A Practical Handbook*. PUQ.

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.

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

Kuruzovich, J., Bassellier, G., & Sambamurthy, V. (2012). IT Governance Processes and IT Alignment: Viewpoints from the Board of Directors. *Proceedings of the 45th Hawaii International Conference on System Sciences*, 5043-5052.

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

Maleh, Y., Sahid, A., & Belaissaoui, M. (2019). *Strategic IT Governance and Performance Frameworks in Large Organizations*. IGI Global, USA.

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

Mohamed, N., & Singh, J. K. a/p G. (2012). A conceptual framework for information technology governance effectiveness in private organizations. I*nformation Management & Computer Security, 20*(2), 88-106.

Citation Information: Zaydi, M., & Nassereddine, B. (2019). DevSecOps practices for an agile and secure it service management. *Journal of Management Information and Decision Sciences, 22*(4), 527-540.

Mohan, V., Othmane, L. ben, & Kres, A. (2018). BP: Security Concerns and Best Practices for Automation of Software Deployment Processes: An Industrial Case Study. *Proceedings of the 2018 IEEE Cybersecurity 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. *In Proceedings of the 20th Annual SIG Conference on Information Technology Education*, 93-98.

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

Prates, L., Faustino, J., Silva, M., & Pereira, R. (2019). DevSecOps Metrics. In S. Wrycza & J. Maślankowski (Eds.), Information *Systems: Research, Development, Applications, Education* (pp 77-90). Cham: Springer International Publishing.

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

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. *In Proceedings of the 22Nd International Conference on Evaluation and Assessment in Software Engineering 2018*, 57-67.

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.

Thabane, L., Thomas, T., Ye, C., & Paul, J. (2009). Posing the research question: not so simple. *Canadian Journal of Anesthesia, 56*(1), 71-79.

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

Tiwana, A., & Konsynski, B. (2010). Complementarities between organizational IT architecture and governance structure. *Information Systems Research, 21*(2), 288-304.

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.

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

Zainal, Z. (2007). Case study as a research method. *Jurnal Kemanusiaan, 5*(1), 1-6.

Citation Information: Zaydi, M., & Nassereddine, B. (2019). DevSecOps practices for an agile and secure it service management. *Journal of Management Information and Decision Sciences, 22*(4), 527-540.