# Adapting to Change: Software Project Management in the Era of Security in Cloud Computing

Giusy Annunziata
gannunziata@unisa.it
University of Salerno
Salerno, Italy

## ABSTRACT

Cloud systems are becoming increasingly important nowadays, and at the same time, there is a need to ensure the security of those systems that pose specific problems. There is the lack of adequate skills and knowledge to deal with the complexity and challenges determined by security in cloud systems, particularly skills related to project management. This research aims to investigate the software project management issues and challenges in the design, development, maintenance, and operation of cloud systems while ensuring adequate security and understand best practices to address them. The ultimate goal of the research is to create a framework that will offer practical recommendations to enhance overall project understanding and support project managers in managing projects and programs related to security of cloud systems.

## CCS CONCEPTS

• **Software and its engineering** → Software creation and management; • **Security and privacy** → Systems security.

## KEYWORDS

Software Project Management, Security, Cloud Computing

**ACM Reference Format:**
Giusy Annunziata. 2024. Adapting to Change: Software Project Management in the Era of Security in Cloud Computing. In *28th International Conference on Evaluation and Assessment in Software Engineering (EASE 2024), June 18–21, 2024, Salerno, Italy.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3661167.3661208

## 1 ACADEMIC ADVISOR

*Advisor.* Filomena Ferrucci, University of Salerno, email: fferrucci@unisa.it

*Co-Advisor.* Gemma Catolino, University of Salerno, email: gcatolino@unisa.it

## 2 CONTEXT AND MOTIVATION

Software increasingly plays a central role in our society: it supports business and government initiatives, enables worldwide communications, and drives innovation. At the same time as the growing use of software, there is an increase in cyber attacks targeting businesses, governments, and individuals, becoming a substantial global risk, as highlighted by the World Economic Forum [9]. The latest ENISA[1] (European Union Agency for Cybersecurity) reports highlighting the threat complexity, suggesting that these attacks are increasingly sophisticated, targeted, and widespread [2].

In light of the substantial increase in cyber threats, the field of Cybersecurity has undergone significant growth and evolution over the past decade [10]. Rajapakse et al. [14] have investigated the main challenges related to the application of security approaches; among them, one of the most outstanding is its adaptation of security in cloud environments.

A *Cloud environment* is a virtualized infrastructure that allows users to access and manage computing resources, such as servers and storage, offering flexibility, scalability and on-demand availability [13]. Adoption and migrating to a cloud environment offers different benefits, including increased agility, improved collaboration, reduced infrastructure costs, and the ability to leverage advanced technologies.

Just as the cloud offers numerous benefits, it also presents potential vulnerabilities that can lead to disasters in the event of attacks or threats to its infrastructure. Ensuring security in cloud systems has become increasingly essential to avoid damages such as data loss, compliance with privacy regulations, and adequate resilience to cyber attacks and incidents in this transformation process [1].

Increasing demand for cloud systems drives the need to increase their security, satisfying cybersecurity standards at every stage of the system, i.e., designing, implementing, maintaining, and migrating.[2] Figures such as project managers require robust knowledge and strategies for managing secure cloud systems to ensure their implementation aligns with security standards and effectively prevents and mitigates vulnerabilities and cyber attacks.[3]

It is necessary to comprehend the principal software project management approaches employed within secure cloud systems and the associated issues and challenges these projects entail. A project manager of secure cloud systems must also consider stakeholder and human resource management and the issues they introduce into the project. In their comprehensive study, Larios-Vargas et al. [8] analyzes the relationships among the various stakeholders involved in cloud system projects. They study the stakeholder motivations, expectations, and attitudes toward the security approaches to be employed. The result of their research is a framework that informs and guides stakeholders on how to adopt security practices, ensuring that the resulting software meets and exceeds the organization's stringent security and quality requirements. However, these guides

*EASE 2024, June 18–21, 2024, Salerno, Italy*
© 2024 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-1701-7/24/06
https://doi.org/10.1145/3661167.3661208

[1] ENISA-European Union Agency for Cybersecurity https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends

[2] Fortinet, 2022 Cybersecurity Skills Gap (2022)

[3] ISACA - Implementing a Cybersecurity Culture

and recommendations are not addressed from a management perspective.

Another critical aspect that project managers must pay attention to when managing secure cloud systems is effectively managing vulnerabilities and threats. Robust *Risk Management* is a strategy applied to prevent system failures and mitigate potentially catastrophic risks that could disrupt not only the development but also the operation and maintenance of cloud systems. In their work, Faizi et al. [4] investigate the diverse applications organizations utilize for conducting Information Security Risk Assessment (ISRA). A key revelation from their investigation was the absence of a singular standard for adopting such risk assessment practices. Moreover, they underscored the critical need for these procedures to be simplified and accessible, emphasizing simplicity as an important factor.

***My Proposal***. In response to the gaps and limitations identified in current management approaches, this proposal aims to create a comprehensive framework designed specifically for software project managers working on managing secure cloud systems. The proposed framework aims not only to simplify the management of secure cloud systems but also to offer solid guidance for dealing with the many challenges encountered at various stages, such as maintenance and migration.

One of the key aspects of the framework will be the approach to secure risk management, which will support the manager in identifying, preventing, and mitigating vulnerability and threats.

In addition, the proposed framework will focus on stakeholder and human resource management in secure cloud systems. Effective stakeholder management is essential to the success of any project; the framework will incorporate guidelines and strategies designed to provide strategies for managing these resources while avoiding the introduction of challenges and issues.

By comprehensively addressing these challenges and issues related to the management of secure cloud systems, the proposed framework seeks to equip project managers with the strategies and approaches needed to manage a secure cloud project adequately.

## 3 RESEARCH PLAN

I defined a research goal, which will be achieved through different research objectives.

🔍 ***Research Goal***. *Build a framework that aims to expand current knowledge related to the knowledge areas of Software Project Management by considering secure cloud systems.*

The proposed framework seeks to advance knowledge areas of software project management by integrating the aspects of secure cloud systems. This framework aims to address the evolving challenges and complexities inherent in managing secure cloud systems. To achieve this goal, I plan to satisfy three research objectives:

### 3.1 $RO_1$ - Investigate Approaches, Challenges and Issues of Software Project Management for Secure Cloud Systems.

The goal of this research objective is to extract key approaches, challenges and issues from the literature and related recommendations. To address the first research objective, I will conduct a *Multivocal Literature Review* (MLR) [5] to explore current application of software project management for secure cloud systems. A MLR was chosen because of the expansive nature of security cloud systems. This context includes the industrial and scientific sectors as well as the public and administrative sectors. In order to comprehend entirely the approaches, issues and challenges associated with tha management of the secure cloud systems, it is imperative to delve into its various applications. Therefore, it is necessary to analyzing both established sources, commonly referred to as white literature (i.e., books, papers, etc.), and less conventional sources, known as gray literature (i.e., pre-prints, blogs, etc.).

The survey will build on established project management theories and methodologies, providing insights into the practical application of manage of secure cloud systems development. This approach aims to understand the complexities of managing secure cloud projects and suggest, to the project managers, the best practices to manage them, considering the different application contexts, i.e., industrial, administrative, etc. [6].

The result of this research objective will be a catalogue of approaches, challenges and issues related to the secure cloud systems and related recommendations and insights to advance knowledge in managing them. In addition, these investigations will spend particular attention to two areas: the investigation of risk management and the investigation of stakeholder and human resources management.

*3.1.1* ***$RO_{1.1}$ - Investigate Approaches, Challenges and Issues of Risk Management for Secure Cloud Systems***. One of the most complex practices related to project management is risk management. This practice is most delicate when interfacing with the complexity nature of secure cloud systems, which are undermined by threats and vulnerabilities. This research objective aims to investigate risk management in secure cloud systems.

A literature survey will be conducted through a *Systematic Mapping Study* [11, 12]. The survey will gather existing knowledge on approaches, challenges and issues on risk management for secure cloud systems. In particular, the focus will be identifying widely recognized risks, prevailing threats and vulnerabilities which are causes of those risks, main context application of risk management, and approaches applied in various industries.

The results will be a comprehensive mapping of the literature on the recognized risks in secure cloud systems. It will not only identify the primary threats and vulnerabilities responsible for these risks but also highlight risk management strategies employed in different industries. This mapping will be a starting point for further research work, offering insights into vulnerability identification, risk prevention and mitigation.

*3.1.2* ***$RO_{1.2}$ - Investigate Approaches, Challenges and Issues of Stakeholder and Human Resources Management for Secure Cloud Systems***. This research objective aims understanding the approaches, challenges and issues related to stakeholders and human resources management in secure cloud systems. Larios-Vargas et al. [8] in their work have investigated the behaviors of stakeholders that lead to the adoption of security practices. Starting from them, I want to investigate on the main challenges and issues introduced by stakeholders and human resources, in the secure cloud systems. Attached to those issues and challenges, I aim to analyze the managements approaches that project managers can adopt with stakeholders and human resources.

To archive this goal, I will conduct a *Systematic Mapping Study* [11, 12] on Socio-Technical aspects in secure cloud systems.

The results will be a mapping of issues, challenges and management approaches on stakeholder and human resource management in the context of secure cloud systems.

### 3.2 *RO$_2$* - Validate and Expand the Catalogue of Approaches, Challenges and Issues of Project Management for Security Cloud Systems.

This research objective aims to validate the approaches, challenges, and issues in secure cloud systems identified in the first research objective, creating a validated classification. Moreover, I want to expand it with the insights provided by experts, such as determining management approaches, extracting existing solutions, and grasping the nuances of current practices and their limitations.

To achieve this research objective, will be conducted an empirical survey on how managers manage secure cloud systems. This will involve qualitative methods such as *interviews* and *survey* with industry experts and manager, specialized knowledge in secure cloud management, to obtain a comprehensive view of managerial approaches, challenges, and strategies employed [3, 7].

In addition, will be sought collaboration with reputable entities such as the Project Management Institute (PMI)[4] to enrich the research process. Using the experience and resources offered by PMI, the research findings can be further validated.

The results obtained in this research objective will be a validated catalogue of the current approaches, challenges and issues of software project management for secure cloud systems. This will help highlight limitations and related management strategies and be the starting point for developing innovative solutions and frameworks to address them.

### 3.3 *RO$_3$* - Create a Framework that Software Project Managers can Adopt to Manage Secure Cloud Systems.

This research question aims to construct a robust framework tailored for software project managers, equipping them with comprehensive guidelines for ensuring the management of secure cloud systems. It will particularly focus on managing risk, stakeholders, and human resources. The framework aims to synthesize findings from previous research questions, consolidating insights from diverse perspectives to offer a detailed roadmap.

The validation process for this framework will incorporating both qualitative and quantitative methods to ensure its applicability. Qualitative surveys and interviews will be conducted in collaboration with the PMI, engaging industry experts to provide insights and real-world experiences [3, 7]. These qualitative assessments will evaluate the relevance, practicality and feasibility of the framework, ensuring its applicability to the needs and challenges faced by project managers in the secure cloud systems context.

Complementing the qualitative validation, quantitative methods will be employed to assess the framework's efficacy through real-world case studies. These case studies will examine the practical application of management approaches, evaluating their impact on project timelines, effectiveness in mitigating security risks, and adherence to industry standards and compliance requirements. The quantitative validation will provide empirical evidence of the framework's effectiveness in real-world scenarios.

The results will be a framework validated through a rigorous validation process to ensure its robustness and relevance in addressing the challenges of secure cloud systems. By integrating insights from both qualitative and quantitative assessments, the framework will offer guidance for software project managers, supporting them in managing secure cloud systems.

### 3.4 Schedule

The three identified research objectives should be completed following the schedule proposed in Figure 1, throughout the three-year of the Ph.D. program. In addition, the the writing of the Ph.D. thesis is scheduled to begin toward the conclusion of the second year.

During my first year and part of the second year, I will focus on the first research objective, and relative sub-objectives, investigating the approaches, challenges and issues in the context of secure cloud systems and identifying possible recommendations and strategies.

The remainder of the second year will aim to realize the second research objective by validating the lists of approaches, challenges and issues obtained from the first research objective through interviews and surveys with practitioners and experts.

Finally, the third year will focus on the creation and validation of the framework.

## 4 EXPECTED IMPACT OF THE RESEARCH

This research aims to make a substantive contribution to the field of software project management, expanding the knowledge also in the secure cloud systems field, by creating a framework that can enhance the effectiveness of software project management with a particular focus on secure cloud systems. The research aims not only to expand the theoretical understanding but also to offer tangible strategies and approaches that can be directly applied in real-world scenarios. In conclusion, the framework will be designed to support project managers in:

- *Apply tailored strategies*: The proposed framework will be created based on data extracted from a Multivocal Literature Review on approaches, challenges and issues in secure cloud systems management, considering the different applications that systems may have, i.e., administrative, public, industrial, etc. According to a specific application contexts, managers can adopt strategies targeted to the context of the system they are managing.
- *Enhancing security risk management for secure cloud systems*: The framework will improve security management in secure cloud systems by providing strategies for robust management and prevention against attacks, threats, and vulnerabilities. Project managers, through the mitigation strategies proposed by the framework, will be able to implement measures that strengthen

[4] PMI - Project Management Institute https://www.pmi.org

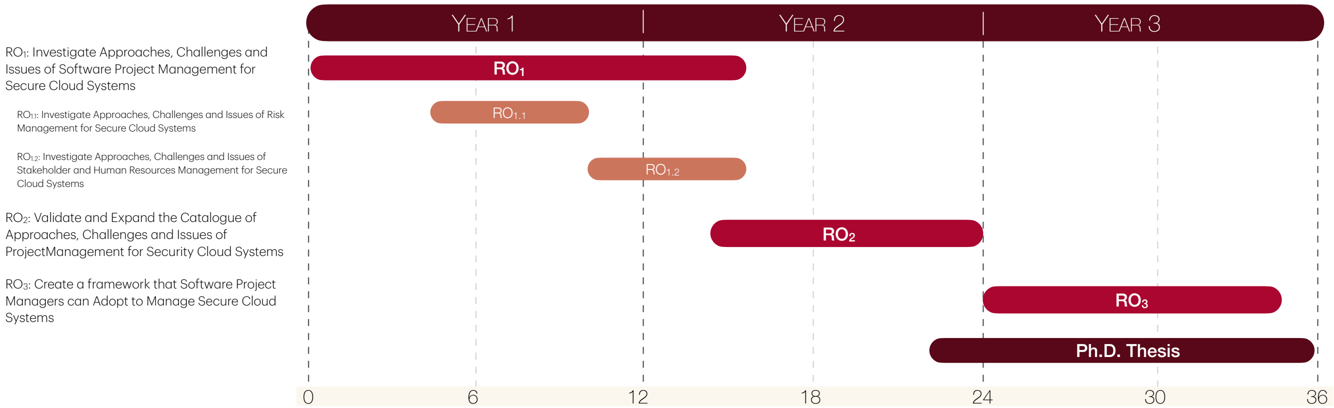

**Figure 1: Distribution of the research objectives for the three-year Ph.D. program**

the security of such systems, thus contributing to a more robust defense against evolving cyber threats.

- *Enhancing stakeholders and human resources management for secure cloud systems*: The framework will provide project managers with recommendations for managing the challenges and issues that stakeholders and human resources will introduce into secure cloud systems. The framework will enable managers to integrate strategies that take into account the organizational dynamics of human resources and stakeholders. This knowledge is essential for creating a comprehensive defense strategy during the management of secure cloud systems.

## REFERENCES

[1] Roaa Al Nafea and Mohammed Amin Almaiah. 2021. Cyber security threats in cloud: Literature review. In *2021 international conference on information technology (ICIT)*. IEEE, 779–786.

[2] Borka Jerman Blažič. 2021. The cybersecurity labour shortage in Europe: Moving to a new concept for education and training. *Technology in Society* 67 (2021), 101769. https://doi.org/10.1016/j.techsoc.2021.101769

[3] Peter M Chisnall. 1996. Qualitative Interviewing: The Art of Hearing Data. *Journal of the Market Research Society* 38, 4 (1996), 553–555.

[4] Ana Faizi, Ali Padyab, and Andreas Naess. 2022. From rationale to lessons learned in the cloud information security risk assessment: a study of organizations in Sweden. *Information & Computer Security* 30, 2 (2022), 190–205.

[5] Vahid Garousi, Michael Felderer, and Mika V Mäntylä. 2019. Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information and software technology* 106 (2019), 101–121.

[6] Helen Heath and Sarah Cowley. 2004. Developing a grounded theory approach: a comparison of Glaser and Strauss. *International journal of nursing studies* 41, 2 (2004), 141–150.

[7] Siw Elisabeth Hove and Bente Anda. 2005. Experiences from conducting semi-structured interviews in empirical software engineering research. In *11th IEEE International Software Metrics Symposium (METRICS'05)*. IEEE, 10–pp.

[8] Enrique Larios-Vargas, Omar Elazhary, Soroush Yousefi, Derek Lowlind, Michael L. W. Vliek, and Margaret-Anne Storey. 2023. DASP: A Framework for Driving the Adoption of Software Security Practices. *IEEE Trans. Softw. Eng.* 49, 4 (apr 2023), 2892–2919. https://doi.org/10.1109/TSE.2023.3235684

[9] Marsh McLennan. 2021. The Global Risks Report 2021 16th Edition. World Economic Forum Cologny, Switzerland.

[10] Håvard Myrbakken and Ricardo Colomo-Palacios. 2017. DevSecOps: a multivocal literature review. In *Software Process Improvement and Capability Determination: 17th International Conference, SPICE 2017, Palma de Mallorca, Spain, October 4–5, 2017, Proceedings*. Springer, 17–29.

[11] Kai Petersen, Robert Feldt, Shahid Mujtaba, and Michael Mattsson. 2008. Systematic mapping studies in software engineering. In *12th international conference on evaluation and assessment in software engineering (EASE)*. BCS Learning & Development.

[12] Kai Petersen, Sairam Vakkalanka, and Ludwik Kuzniarz. 2015. Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and software technology* 64 (2015), 1–18.

[13] Daryl C Plummer, Thomas J Bittman, Tom Austin, David W Cearley, and David Mitchell Smith. 2008. Cloud computing: Defining and describing an emerging phenomenon. *Gartner, June* 17 (2008), 1–9.

[14] Roshan N. Rajapakse, Mansooreh Zahedi, M. Ali Babar, and Haifeng Shen. 2022. Challenges and solutions when adopting DevSecOps: A systematic review. *Information and Software Technology* 141 (2022), 106700. https://doi.org/10.1016/j.infsof.2021.106700