A Study on Organizational IT Security in Mobile Software Ecosystems Literature

Caio Steglich, Azriel Majdenbaum, Sabrina Marczak
PPGCC - School of Technology - PUCRS
Porto Alegre, RS, Brazil
caio.borges@acad.pucrs.br
azriel.majdenbaum@pucrs.br
sabrina.marczak@pucrs.br

Rodrigo Santos
PPGI - UNIRIO
Rio de Janeiro, RJ, Brazil
rps@uniriotec.br

***Abstract*—Information security is a key topic for most organizations. With the digital revolution, smartphones have become popular not only for personal use but also within organizations where many employees use them for business purposes. As smartphones are increasingly present in organizations, it is necessary to understand what recommendations the literature provides for the safe use of such devices, helping organizations to protect themselves from threats. ISO 27000 is a well-known standard for information security in a business context. It provides a set of controls that must be observed to ensure more secure organizational information. Therefore, the goal of this study is to identify which controls presented in ISO 27000, more specifically ISO 27001, are present in the Mobile Software Ecosystem (MSECO) literature. To do so, we conducted a systematic mapping review supplemented by a snowballing process to identify studies in the field of MSECO that have addressed any subject that is present in ISO 27001. We found that 34 out of the 114 ISO 27001 controls are covered by the MSECO literature. Also, some of the ISO sections (e.g., Asset Management) have not yet been explored in the MSECO literature. Our results can inspire future and further studies on the topic of MSECO information security.**

***Index Terms*—Mobile Software Ecosystem, Organizational Information Security, ISO 27000, Security controls, Literature Review**

I. Introduction

In the digital age, many large organizations have suffered from breaches of information security, including companies such as Yahoo, Microsoft, Intel, despite their concerns about their data security [1]. Such breaches can occur for several reasons. Werlinger et al. [2] present three main groups of factors for information security, namely: i) Human-based factors, ii) Organizational factors, and iii) Technological factors. On the other hand, we have the context of Mobile Software Ecosystems (MSECO), where applications are produced for use on users' or company-owned devices. These software ecosystems mostly comprise elements that relate to mobile technology platforms, organized into three main dimensions: technical, business and social [3]–[5].

In this context, ISO 27000 is a standard family for information security to organizations. ISO 27000 is composed by the following standards:

- ISO 27001 presents the principles and vocabulary that define the nomenclature used in the ISO 27000 family standards. ISO 27001 also have an appendix composed of 14 sections divided into 114 objective controls [6].
- ISO 27002 presents the requirements for meeting the controls set forth in ISO 27001.
- ISO 27003 provides a good practice guide for meeting the controls set forth in ISO 27001.
- ISO 27004 provides ways to monitor, measure, analyze, and evaluate the application of ISO 27001 controls in an enterprise.
- ISO 27005 explains how to perform risk management when any of the controls in ISO 27001 are not met.

This standard has been used in many companies around the world [6], such as Google and Yahoo. Because it is a widely used standard in the business context, there is a need to investigate how the recommendations in ISO 27000 can help companies whose employees use mobile devices for their duties within the company, thus protecting them from security breaches. More specifically, in this study we aim to identify which ISO 27001 controls are present in the MSECO literature seeking to identify evidences about how they are used and what the literature brings about these controls, as well as possibilities for future contributions in the field. As key contributions, we found the following:

- Only 34 of 114 controls of ISO 27001 were identified in the MSECO literature;
- Only 2 out of the 14 sections had all of their respective controls reported in the MSECO literature. These sections are i) Information security policies and ii) Cryptography;
- The Asset management section is the only out of the 14 ISO 27001 sections that has no evidence of use or citation in MSECO studies.

The remainder of this paper is structured as follows. Section II presents the main concepts of information security and MSECO. Section III presents the research method adopted in this study. Section IV summarizes the results of our study. Section V brings the discussion over our results. Section VI presents the limitations of the research method. Section VII concludes our study and points out future work.

978-1-7281-4659-1/20/$31.00 ©2020 IEEE
DOI 10.1109/ICSA-C50368.2020.00047

II. Background

We introduce here concepts about organizational information security (Section II-A) and MSECO (Section II-B).

A. Information Security in Organizations

Organizations' information security has become a critical element in preventing damage from threats such as intrusions or unintentional data leaks. There are several challenges to organizations to keep information safe. Werlinger et al. [2] present three dimensions that influence information security–human-based factors, organizational factors or technological factors. Examples of human-based factors that become challenges for organizations are lack of training or experience, or communication security issues. Those challenges related to organizational factors are, for instance, incorrect risk estimation, lack of budget, wrong distribution of IT responsibilities, or weak access control to sensitive data. Yet, examples of technological challenges are the systems' complexity, the systems or applications' vulnerabilities, mobility and distributed access, or lack of effective security tools [2].

These challenges can be controlled when the right decisions are made, which can eliminate them or mitigate the effects of these threats. The information security literature has a set of studies on how to protect organizational information, such as Hunker and Probst [7], who identify several approaches to counter internal threats within the organization, analyzing the technical, socio-technical, sociological and psychological factors. Hunker and Probst [7] also discuss several challenge such as access controls, company security policies, and motivation of the internal actors within organization.

Therefore, it is relevant to understand how these standards are applied to the mobile context since the ISO 27000 family, and mainly ISO 27001, has increasingly been considered an international standard for dealing with information security in organizations [6].

As previously mentioned, ISO 27001 specifies the requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System (ISMS) within the context of an organization. ISMS seeks to preserve the confidentiality, integrity, and availability of information by applying a risk management process that provides stakeholders with confidence in which risks are properly managed. An organization's ISMS specification and implementation is influenced by its needs and objectives, security requirements, organizational processes, employees, and size and structure of the organization.

In its appendix, ISO 27001 presents 14 sections organized into 114 controls. These sections refer to a set of generic information security objectives, compiled from risks commonly present in organizations. Each objective unfolds into several controls that must be implemented to achieve the proposed objectives. Requirements to implement such controls are discussed in ISO 27002, good practices to meet them compose ISO 27003, and so on.

ISO 27001 sections are as follows. Their respective controls are 1) Information security policies, 2) Organization of information security, 3) Human resource security, 4) Asset management, 5) Access control, 6) Cryptography, 7) Physical and environmental security, 8) Operations security, 9) Communications security, 10) System acquisition, development, and maintenance, 11) Supplier relationships, 12) Information security incident management, 13) Information security aspects of business continuity management, 14) Compliance.

B. Mobile Software Ecosystems

A Software Ecosystem is a set of elements around a common technological platform working together as an ecosystem [3] [4]. A Mobile Software Ecosystem (MSECO), on the other hand, is a Software Ecosystem focused in the mobile context [4] [8], i.e., the ecosystem around a mobile technological platform. MSECO are composed by 7 elements [4], namely: the technological platform, the internal or external developers, the ecosystem community, the applications, the application users, the application business market, and the evangelists, those representing the owner of the ecosystem when in contact with users and developers.

The MSECO literature [9] has some studies regarding security, generally applied to applications, but very few discuss information security at the organizational level. For instance, Reinfelder et al. [10] discussed the differences between Android and iPhone users in their aware with rules/policies security. The authors found that Android users check more security factors than iPhone users, considering their official store policies for applications. Finally, Watanabe et al. [11] explored the difference between paid and free applications regarding security and found that 50% of threats in paid applications and 70% in free applications come from libraries that developers choose.

We aim to identify papers that report on organizational information security in light of the ISO 27000 in MSECO.

III. Research Method

In order to identify which ISO 27001 controls are present in the MSECO literature we conducted a systematic mapping review [12] supplemented by a snowballing procedure [13]. We used our previous systematic mapping [9] on MSECO as a starting point. That previous review revealed 63 studies on the topic up to December, 2017. We replicated it using the exact same digital databases (ACM, IEEE, Science Direct, Scopus, Wiley Interscience, and Springer), and paper search and selection process (see [9] for details). We identified 31 papers published between Jan, 2018 and Dec, 2019.

To conduct the snowballing procedure, we once again followed the steps conducted in a preliminary study of ours on MSECO [8], attending the forward and backward snowballing guidelines by Wohlin [13]. The forward snowballing sought for papers that had cited one of the accepted papers in our literature. This search was conducted in Google Scholar with an end date of Dec 17, 2019 and revealed 49 new studies. The backward snowballing procedure investigated the references of each of the accepted papers in the systematic mapping, looking for new papers. This added 50 new papers to our list.

Table I
SECTION I - INFORMATION SECURITY POLICIES

Control	Citation
1) Policies for information security	Castle et al. [14]
2) Review of the policies for information security	Castle et al. [14]

The update on the systematic mapping (31 papers) followed by the forward (49) and the backward (50) snowballing procedures identified 130 additional papers, totaling a pull of 193 candidate papers for inspection. We read the title and abstract of each candidate paper aiming to identify whether it discussed any content related to any of the 114 ISO 27001 controls. When it was not clear, we set the paper apart for full reading. Upon an extensive reading process reviewed by a senior researcher with over 20 years of experience in software engineering, we selected 32 papers that discuss information security at the organizational level in the MSECO literature.

Extracted data was organized by ISO 27001 section and control in an spreadsheet for consolidation and reporting.

IV. RESULTS

In this section, we present the results of our literature review organized by ISO 27001 section. For each section, we show a table with their controls and the citations of authors who described this control.

The first section of ISO 27001 is "Information security policies", which has two controls as shown in Table I. Both controls were reported by Castle et al. [14]. The authors investigated in an interview-based study how these are implemented in organizations. Control 2 - Review of policies was mentioned by one out of the 7 interviewees only.

The second section of ISO 27001 is "Organization of information security", which is composed of 7 controls as presented in Table II. No papers reported on the controls 2, 4, 5, and 7. Control 1 is discussed by Krupskiy et al. [15] in which the authors categorize actors engaged in the business process of an application store and identified their responsibilities. It is also reported by Acar et al. [16], which reports on the importance of understanding the roles around an ecosystem to check the related challenges, including security ones. Control 3 is addressed by Gamba et al. [17]. The authors propose recommendations to detect deceptive behaviors, including attribution and accountability. For these, they recommend the use of certificates signed by global-trusted authorities. Control 6 is more largely discussed by literature. We found evidence of it in 8 papers ([15]–[22]). Examples are the study of Liu et al. [19], that discuss privacy of users focuses on the Android devices; Andriotis and Tryfonas [21] investigate the impact of user data privacy on mobile devices, focusing on Android ecosystem; and Barrera and Oorschot [22] discuss the difference of security frameworks in different ecosystems, such as iOS and Android.

The third section is entitled "Human resource security" and is comprised of 6 controls as presented in Table III. Controls 1, 5 and 6 were not cited by any of the selected papers. Control 2 is reported by Kareborn and Howcroft [23]. The authors explain the crowdsourcing format used by Apple ecosystem, but also point out the importance of clarifying the terms of use. Another study is by Reuver [24], which explains that organizations typically govern its internal activities through employment contracts and hierarchical control. Control 3 is seen in the study of Miclaus et al. [25], in which the authors explain that an application store needs to sign additional responsibilities to employers. Control 4 is discussed by Castle et al. [14], in which they explain that some possible causes of vulnerabilities are the lack or limited security education.

Table II
SECTION II - ORGANIZATION OF INFORMATION SECURITY

Control	Citation
1) Information security roles and responsibilities	Krupskiy et al. [15] Acar et al. [16]
2) Segregation of duties	-
3) Contact with authorities	Gamba et al. [17]
4) Contact with special interest groups	-
5) Information security in project management	-
6) Mobile device policy	Krupskiy et al. [15] Acar et al. [16] Gamba et al. [17] Lee et al. [18] Liu et al. [19] Xu et al. [20] Andriotis and Tryfonas [21] Barrera and Oorschot [22]
7) Teleworking	-

Table III
SECTION III - HUMAN RESOURCE SECURITY

Control	Citation
1) Screening	-
2) Terms and conditions of employment	Kareborn and Howcroft [23] Reuver [24]
3) Management responsibilities	Miclaus et al. [25]
4) Information security awareness, education and training	Castle et al. [14]
5) Disciplinary process	-
6) Termination or change of employment responsibilities	-

Table IV
SECTION IV - ASSET MANAGEMENT

Control	Citation
1) Inventory of assets	-
2) Ownership of assets	-
3) Acceptable use of assets	-
4) Return of assets	-
5) Classification of information	-
6) Labelling of information	-
7) Handling of assets	-
8) Management of removable media	-
9) Disposal of media	-
10) Physical media transfer	-

The fourth section, named "Asset management" and composed of 10 controls as presented in Table IV, was not discussed by any of the selected papers.

The fifth section of ISO 27001 "Access control" consists

Table V
SECTION V - ACCESS CONTROL

Control	Citation
1) Access control policy	-
2) Access to networks and network services	-
3) User registration and de-registration	Williams and Mahmoud [26]
4) User access provisioning	Jaramillo et al. [27]
5) Management of privileged access rights	Acar et al. [16]
6) Management of secret authentication information of users	Watanabe et al. [28]
7) Review of user access rights	-
8) Removal or adjustment of access rights	-
9) Use of secret authentication information	-
10) Information access restriction	-
11) Secure log-on procedures	-
12) Password management system	Campbell et al. [29] Samonte et al. [30]
13) Use of privileged utility programs	-
14) Access control to program source code	-

of the 14 controls listed in Table V. Nine of the 14 controls–1, 2, 7 to 11, 13, and 14 are not reported in the MSECO literature. Control 3 is shown by Williams and Mahmoud [26]. The authors argue that user registration may make the organization lose customers; thus, they reflect upon other means of relationship between enterprise and customer. Control 4 is tackled by Jaramillo et al. [27] and describes how important it is to provide employees with secure devices in organizations as a means to improve data security and access, among others. Control 5 is pointed by Acar et al. [16] as a challenge entitled "Permission Comprehension and Attention by End Users". The authors argue that it is the user's responsibility to take care of the applications. Control 6 is shown by Watanabe et al. [28], in which they explore some vulnerabilities in mobile applications, finding that secret token to authentication supports secure passwords. Control 12 is presented in Campbell et al. [29] and Samonte et al. [30], who discuss the importance of employees to get a username and a password to use an enterprise system.

The sixth section is named "Cryptography" and is composed of 2 controls (see Table VI). Control 1 is presented by Oltrogge et al. [31], in which the authors explain the importance of the use of cryptography API's to applications with important data. It is also discussed by Devine [32]. The author reports that 44% of the vulnerabilities of external attacks on Android applications stem from cryptography issues. Control 2 is also reported by Oltrogge et al. [31], in which the authors discuss the importance of choosing a good key to encrypt data.

The seventh section, "Physical and environmental security", which is composed of 15 controls as presented in Table VII, had only one of its controls reported in literature–Control 1. This control is discussed by Jaramillo et al. [27] in a study in which the authors explain the distinct kind of securities in an organization, including physical security.

Table VI
SECTION VI - CRYPTOGRAPHY

Control	Citation
1) Policy on the use of cryptographic controls	Oltrogge et al. [31] Devine [32]
2) Key management	Oltrogge et al. [31]

Table VII
SECTION VII - PHYSICAL AND ENVIRONMENTAL SECURITY

Control	Citation
1) Physical security perimeter	Jaramillo et al. [27]
2) Physical entry controls	-
3) Securing offices, rooms and facilities	-
4) Protecting against external and environmental threats	-
5) Working in secure areas	-
6) Delivery and loading areas	-
7) Equipment siting and protection	-
8) Supporting utilities	-
9) Cabling security	-
10) Equipment maintenance	-
11) Removal of assets	-
12) Security of equipment and assets off-premises	-
13) Secure disposal or reuse of equipment	-
14) Unattended user equipment	-
15) Clear desk and clear screen policy	-

Table VIII
SECTION VIII - OPERATIONS SECURITY

Control	Citation
1) Documented operating procedures	-
2) Change management	Pettersson et al. [33]
3) Capacity management	-
4) Separation of development, testing and operational environments	-
5) Controls against malware	-
6) Information backup	Chin et al. [34]
7) Event logging	-
8) Protection of log information	-
9) Administrator and operator logs	-
10) Clock synchronization	-
11) Installation of software on operational systems	Siegfried et al. [35]
12) Management of technical vulnerabilities	-
13) Restrictions on software installation	-
14) Information systems audit controls	Acar et al. [16]

The eighth section is named "Operations security" and comprises 14 controls in total. As indicated in Table VIII, only 4 of these 14 controls were cited in literature as follows. Control 2 is discussed by Pettersson et al. [33]. The authors argue that it is essential to an ecosystem life cycle to deal with change management. Control 6 is presented by Chin et al. [34], whose work explain data loss or lack of backup as one of the most critical factors to users or companies. Control 11 is part of Siegfried et al. [35] study. The authors explain about the installation of applications on operating systems, focusing on metrics to understand the target audience of an application. Control 14 is introduced by Acar et al. [16], in which presents AndroidLeaks, an analysis tool for a manual security audit.

The ninth section named "Communications security" is

Table IX
SECTION IX - COMMUNICATIONS SECURITY

Control	Citation
1) Network controls	-
2) Security of network services	-
3) Segregation in networks	-
4) Information transfer policies and procedures	-
5) Agreements on information transfer	Hatamian et al. [36]
6) Electronic messaging	-
7) Confidentiality or nondisclosure agreements	-

organized into 7 controls as presented in Table IX. Control 5 is the only one cited in the MSECO literature. The study by Hatamian et al. [36] explains that to safely transfer data it is important to record the transferred information and the people who share or get access to this data.

The tenth section, entitled "System acquisition, development, and maintenance", is composed of 13 controls as presented in Table X. Over half of these 13 controls (7 of them) have no evidence in literature, which are: Controls 2 to 7, and 11. Control 1 is presented by Acar et al. [16], in which the authors explain that in access control it is important to analyze the security requirements that support identifying risks. In addition, França et al. [37] argue that analysis of security requirements is a social activity since people are those who participate in these ecosystems. Control 8 is shown in Xu et al. [20] study, whose authors explain that a webview application for mobile needs to have the same cautions that a common application in a web browser has. Control 9 is discussed by Krupskiy et al. [15]. The authors report that the xCode development environment is most secure than other environments. Control 10 is evidenced in Castle et al. [14] study, in which one of the respondents of the conducted interviews works as an outsourced member similar to most of other application developers settings. Control 12 is discussed by Samonte et al. [30]. The authors explain the importance of testing applications. They argue that this importance comes not only to secure data but also to understand the differences in the applications in distinct devices.

The eleventh section refers to "Supplier relationships" and is composed of 5 controls as presented in Table XI. Controls 2, 4, and 5 were not reported. Control 1 is cited by Basole et al. [38], whose study reports that Apple and Samsung have changed many times their relationship with application suppliers over the years, which may change the ecosystem operating rules, or in some cases generate or correct vulnerabilities. Control 3 is mentioned by Gamba et al. [17] study, in which the authors inform that the supplier chain in the Android open-source model supports transparency.

The twelfth section of ISO 27001 is named "Information security incident management". Out of its 7 controls as listed in Table XII, only Control 1 was found in literature. The study by Fontao et al. [39] discuss that among the evangelists' responsibilities and procedures is the concern with security.

The thirteenth section "Information security aspects of business continuity management" contains 4 controls. These are listed in Table XIII in which one can see that only Control 4 was cited by MSECO literature. Both the studies by Seidl et al. [40] and by Roshan et al. [41] report on the importance of information processing facilities.

Table X
SECTION X - SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

Control	Citation
1) Information security requirements analysis and specification	Acar et al. [16] França et al. [37]
2) Securing application services on public networks	-
3) Protecting application services transactions	-
4) Secure development policy	-
5) System change control procedures	-
6) Technical review of applications after operating platform changes	-
7) Restrictions on changes to software packages	-
8) Secure system engineering principles	Xu et al. [20]
9) Secure development environment	Krupskiy et al. [15]
10) Outsourced development	Castle et al. [14]
11) System security testing	-
12) System acceptance testing	Samonte et al. [30]
13) Protection of test data	-

Table XI
SECTION XI - SUPPLIER RELATIONSHIPS

Control	Citation
1) Information security policy for supplier relationships	Basole et al. [38]
2) Addressing security within supplier agreements	-
3) Information and communication technology supply chain	Gamba et al. [17]
4) Monitoring and review of supplier services	-
5) Managing changes to supplier services	-

Table XII
SECTION XII - INFORMATION SECURITY INCIDENT MANAGEMENT

Control	Citation
1) Responsibilities and procedures	Fontao et al. [39]
2) Reporting information security events	-
3) Reporting information security weaknesses	-
4) Assessment of and decision on information security events	-
5) Response to information security incidents	-
6) Learning from information security incidents	-
7) Collection of evidence	-

The fourteenth and final section of ISO 27001 is named "Compliance" and is organized into 8 controls. Table XIV shows that half of the controls–1, 3, 5, and 8 were not discussed in the literature. Control 2 is reported in 4 studies. Teixeira et al. [42] explain that open source does not ensure a property right, but brings transparency and collaborative benefits. Schlagwein et al. [43] explains that owners can keep the property of their rights and change terms to an open access option. Ceccagnoli et al. [44] investigate the strategies

Table XIII
SECTION XIII - INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

Control	Citation
1) Planning information security continuity	-
2) Implementing information security continuity	-
3) Verify, review and evaluate information security continuity	-
4) Availability of information processing facilities	Seidl et al. [40] Roshan et al. [41]

Table XIV
SECTION XIV - COMPLIANCE

Control	Citation
1) Identification of applicable legislation and contractual requirements	-
2) Intellectual property rights	Teixeira et al. [42] Schlagwein et al. [43] Ceccagnoli et al. [44] Wong et al. [45]
3) Protection of records	-
4) Privacy and protection of personally identifiable information	Gamba et al. [17]
5) Regulation of cryptography controls	-
6) Independent review of information security	Siegfried et al. [35]
7) Compliance with security policies and standards	Oltrogge et al. [31]
8) Technical compliance review	-

of property rights to reach partnerships and better performance. Wong et al. [45] discuss legal and privacy issues of property rights. Control 4 is briefly discussed by Gamba et al. [17], in which the authors present personally identifiable information (PII) that could be used to identify the users that conducted suspicious activities. Control 6 is referred by Siegfried et al. [35]. The authors argue that independent reviews are valuable sources for quality evaluation. Control 7 is illustrated by Oltrogge et al. [31] study which reports that is necessary to ensure that the service infrastructure maintains the highest security standards.

V. DISCUSSION

The MSECO literature contains several studies (193 identified in our literature review), but only a few (32 of them) present the issue of organizational information security. Out of the 32 selected studies, 14 directly mention ISO 27001. Despite the little representativeness, all of them discuss topics related to at least one of the ISO 270001 controls, helping us to understand the extension and breadth of discussion on the matter in the MSECO literature.

Generally, we learned that only about one-third of the controls are reported (34 out of 114) and that only 2 out of the 14 sections had at least one study discussing each one of the respective controls. Moreover, we found that one section, “Asset management”, has no reported evidence whatsoever.

An in-depth look reveals that the research community is concerned with issues related to information security policies (Section I), the definition of information security roles and responsibilities, privacy issues and the impact of lack of privacy as well as with the accountability for suspicious behavior when using mobile applications (Section II).

Discussions around which kind of responsibilities outsourced developed have towards information security in MSECO is also out there (Section III). This brings implications to software development practices to say the least. We could open the discussion of how we are preparing young developers to concern about such issues and how such standards are part of undergraduate curricula.

Some studies debate that required user identification information may impose to users and led a company to lose them, having these migrating to other ecosystems. Related topics discuss on the design of secure authentication procedures that inherit limitations from MSECOs (Section V), on the need for implementing such procedures, for instance, adding cryptography to APIs (Section VI), or debate about which kinds of security concerns should one have (Section VII).

The security of information along the operation of the business is essential because the company cannot allow weaknesses that can lead to data loss, especially in applications that are in operation (Section VIII). In addition, communication security needs to be carefully evaluated, as a secure channel for data transmission is required, thus avoiding possible external attacks (Section IX).

All used applications in an organization must be analyzed from their requirements, development and pass a set of tests to ensure that the application is safe to use (Section X). Often the company's applications are used by third parties, which means that they need to be reliable suppliers whom to buy from and that follow what is agreed with the contracting company (Section XI).

In a company information incident, it is critical that the company be able to quickly analyze impact and correct it as quickly as possible. To avoid an incident, it is ideal to establish responsibilities for company employees regarding the use of applications. (Section XII).

Information security needs to adapt to the business and its rules without disrupting the workflow of the organization that implements it (Section XIII). Compliance with security rules must also occur, making company employees clearly understand security rules, and how to protect company property (Section XIV).

VI. VALIDITY THREATS

This study had some limitations, such as:

- Some studies may not be indexed in the selected libraries. However, to mitigate this, we followed the Petersen et al. [12] recommendations of digital libraries and conducted a snowballing process.
- The data extraction process followed a manual process but we double-check every step to not forget anything present on the identified studies.

VII. CONCLUSION

The MSECO literature continues to have several opportunities for scientific and practical contributions, including topics such as information security that are widely explored. In this study, we investigated the topic of organizational information security in light of ISO 27000. We looked specifically into ISO 27001 and its sections and controls. We found that only 34 of 114 controls presented in ISO 27001 are presented in MSECO literature and some sections of ISO 27001 are not explored at all (e.g., Asset management) or less explored than others (e.g., Communications Security, Information security incident management, and Information security aspects of business continuity management). This provides us with evidence that the topic of organization information security still has several opportunities of future studies to investigate these unexplored controls (as comparing this results with General Data Protection Regulation - GDPR). Thus, we would like to recommend that researchers wishing to contribute to the MSECO literature can further explore the topic of organizational information security.

Appendix

Table XV presents the 32 publications about organizational information security in light of ISO 27001 present in MSECO.

References

[1] L. A. Gordon, M. P. Loeb, and L. Zhou, "The impact of information security breaches: Has there been a downward shift in costs?," *Journal of Computer Security*, vol. 19, no. 1, pp. 33–56, 2011.

[2] R. Werlinger, K. Hawkey, and K. Beznosov, "An integrated view of human, organizational, and technological challenges of it security management," *Information Management & Computer Security*, 2009.

[3] J. Bosch and P. Bosch-Sijtsema, "From integration to composition: On the impact of software product lines, global development and ecosystems," *Journal of Systems and Software*, vol. 83, no. 1, pp. 67–76, 2010.

[4] A. d. L. Fontao, R. P. dos Santos, and A. C. Dias-Neto, "Mobile software ecosystem (mseco): A systematic mapping study," in *Proceedings of the IEEE Annual Computer Software and Applications Conference*, pp. 653–658, IEEE, 2015.

[5] P. R. Campbell and F. Ahmed, "A three-dimensional view of software ecosystems," in *Proceedings of the European Conference on Software Architecture: Companion Volume*, pp. 81–84, ACM, 2010.

[6] G. Disterer, "Iso/iec 27000, 27001 and 27002 for information security management," *Journal of Information Security*, vol. 4, no. 1, pp. 92–100, 2013.

[7] J. Hunker and C. W. Probst, "Insiders and insider threats-an overview of definitions and mitigation techniques," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 2, no. 1, pp. 4–27, 2011.

[8] C. Steglich, S. Marczak, C. R. de Souza, L. P. Guerra, L. H. Mosmann, M. Perin, *et al.*, "Social aspects and how they influence mseco developers," in *Proceedings of the International Workshop on Cooperative and Human Aspects of Software Engineering*, pp. 99–106, IEEE, 2019.

[9] C. Steglich, S. Marczak, L. P. Guerra, L. H. Mosmann, M. Perin, F. Figueria Filho, and C. De Souza, "Revisiting the mobile software ecosystems literature," in *Proceedings of the Workshop on Distributed Software Development, Software Ecosystems and Systems-of-Systems*, pp. 50–57, IEEE, 2019.

[10] L. Reinfelder, Z. Benenson, and F. Gassmann, "Differences between android and iphone users in their security and privacy awareness," in *Proceedings of the International Conference on Trust, Privacy and Security in Digital Business*, pp. 156–167, Springer, 2014.

[11] T. Watanabe, M. Akiyama, F. Kanei, E. Shioji, Y. Takata, B. Sun, Y. Ishi, T. Shibahara, T. Yagi, and T. Mori, "Understanding the origins of mobile app vulnerabilities: A large-scale measurement study of free and paid apps," in *Proceedings of the International Conference on Mining Software Repositories*, pp. 14–24, IEEE, 2017.

[12] K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update," *Information and Software Technology*, vol. 64, no. 1, pp. 1–18, 2015.

[13] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proceedings of the International Conference on Evaluation and Assessment in Software Engineering*, p. 38, Citeseer, 2014.

[14] S. Castle, F. Pervaiz, G. Weld, F. Roesner, and R. Anderson, "Let's talk money: Evaluating the security challenges of mobile money in the developing world," in *Proceedings of the Annual Symposium on Computing for Development*, p. 4, ACM, 2016.

[15] A. Krupskiy, R. Blessinga, J. Scholte, and S. Jansen, "Mobile software security threats in the software ecosystem, a call to arms," in *Proc. of the Int'l Conference of Software Business*, pp. 161–175, Springer, 2017.

[16] Y. Acar, M. Backes, S. Bugiel, S. Fahl, P. McDaniel, and M. Smith, "Sok: Lessons learned from android security research for appified software platforms," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 433–451, IEEE, 2016.

[17] J. Gamba, M. Rashed, A. Razaghpanah, J. Tapiador, and N. Vallina-Rodriguez, "An analysis of pre-installed android software," *arXiv*, vol. 1, pp. 1–17, 2019.

[18] H. Lee, S. Kang, and M. Kim, "An efficient application-device matching method for the mobile software ecosystem," in *Proceedings of the Asia-Pacific Software Engineering Conference*, vol. 1, pp. 175–182, IEEE, 2014.

[19] B. Liu, J. Lin, and N. Sadeh, "Reconciling mobile app privacy and usability on smartphones: Could user privacy profiles help?," in *Proceedings of the International Conference on World Wide Web*, pp. 201–212, ACM, 2014.

[20] M. Xu, C. Song, Y. Ji, M.-W. Shih, K. Lu, C. Zheng, R. Duan, Y. Jang, B. Lee, C. Qian, *et al.*, "Toward engineering a secure android ecosystem: A survey of existing techniques," *ACM Computing Surveys*, vol. 49, no. 2, p. 38, 2016.

[21] P. Andriotis and T. Tryfonas, "Impact of user data privacy management controls on mobile device investigations," in *Proceedings of the International Conference on Digital Forensics*, pp. 89–105, Springer, 2016.

[22] D. Barrera and P. Van Oorschot, "Secure software installation on smartphones," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 42–48, 2010.

[23] B. Bergvall-Kåreborn and D. Howcroft, "The apple business model: Crowdsourcing mobile applications," *Accounting Forum*, vol. 37, no. 4, pp. 280–289, 2013.

[24] M. de Reuver, "Governance of mobile service innovation after the walled gardens," *info*, vol. 13, no. 1, pp. 43–60, 2011.

[25] A. Miclaus, W. Clauss, E. Schwert, M. A. Neumann, F. Mütsch, T. Riedel, F. Schmidt, and M. Beigl, "Towards the shop floor app ecosystem: Using the semantic web for gluing together apps into mashups," in *Proceedings of the International Workshop on the Web of Things*, pp. 17–21, ACM, 2016.

[26] G. Williams and A. Mahmoud, "Modeling user concerns in the app store: A case study on the rise and fall of yik yak," in *Proceedings of the International Requirements Engineering Conference*, pp. 64–75, IEEE, 2018.

[27] D. Jaramillo, R. Newhook, and R. Smart, "Cross-platform, secure message delivery for mobile devices," in *Proceedings of the IEEE Southeastcon*, pp. 1–5, IEEE, 2013.

[28] T. Watanabe, M. Akiyama, F. Kanei, E. Shioji, Y. Takata, B. Sun, Y. Ishi, T. Shibahara, T. Yagi, and T. Mori, "Understanding the origins of mobile app vulnerabilities: A large-scale measurement study of free and paid apps," in *Proceedings of the International Conference on Mining Software Repositories*, pp. 14–24, IEEE Press, 2017.

[29] P. R. Campbell and F. Ahmed, "An assessment of mobile os-centric ecosystems," *Journal of theoretical and applied electronic commerce research*, vol. 6, no. 2, pp. 50–62, 2011.

[30] M. J. C. Samonte, J. P. R. Javier, L. M. Mataga, and T. T. Timbang, "Aquacloud: A saas disruptive innovation for enterprise business ecosystem," in *Proceedings of the International Conference on Internet and e-Business*, pp. 84–89, ACM, 2018.

[31] M. Oltrogge, E. Derr, C. Stransky, Y. Acar, S. Fahl, C. Rossow, G. Pellegrino, S. Bugiel, and M. Backes, "The rise of the citizen developer: Assessing the security impact of online app generators," in *Proceedings of the Symposium on Security and Privacy*, pp. 634–647, IEEE, 2018.

[32] S. Mansfield-Devine, "Android architecture: Attacking the weak points," *Network Security*, vol. 2012, no. 10, pp. 5–12, 2012.

Table XV
MSECO STUDIES ABOUT ORGANIZATIONAL INFORMATION SECURITY IN LIGHT OF ISO 27001

Title	Citation
Let's Talk Money: Evaluating the Security Challenges of Mobile Money in the Developing World	Castle et al. [14]
Mobile Software Security Threats in the Software Ecosystem, a Call to Arms	Krupskiy et al. [15]
Sok: Lessons Learned from Android Security Research for Appified Software Platforms	Acar et al. [16]
An Analysis of Pre-installed Android Software	Gamba et al. [17]
An Efficient Application-Device Matching Method for the Mobile Software Ecosystem	Heuijin et al. [18]
Reconciling Mobile app Privacy and Usability on Smartphones: Could User Privacy Profiles Help?	Liu et al. [19]
Toward Engineering a Secure Android Ecosystem: A Survey of Existing Techniques	Xu et al. [20]
Impact of User Data Privacy Management Controls on Mobile Device Investigations	Andriotis and Tryfonas [21]
Secure Software Installation on Smartphones	Barrera and Van Oorschot [22]
The Apple Business Model: Crowdsourcing Mobile Applications	Kaareborn and Howcroft [23]
Governance of Mobile Service Innovation After the Walled Gardens	Reuver [24]
Towards the Shop Floor App Ecosystem: Using the Semantic web for Gluing Together apps into Mashups	Miclaus et al. [25]
Modeling User Concerns in the app Store: A Case Study on the Rise and Fall of Yik Yak	Williams and Mahmoud [26]
Cross-Platform, Secure Message Delivery for Mobile Devices	Jaramillo et al. [27]
Understanding the Origins of Mobile app Vulnerabilities: A Large-Scale Measurement Study of Free and Paid apps	Watanabe et al. [28]
An Assessment of Mobile OS-Centric Ecosystems	Campbell and Ahmed [29]
AquaCloud: A SaaS Disruptive Innovation for Enterprise Business Ecosystem	Samonte et al. [30]
The Rise of the Citizen Developer: Assessing the Security Impact of Online app Generators	Oltrogge et al. [31]
Android Architecture: Attacking the Weak Points	Devine [32]
On the Role of Software Process Modeling in Software Ecosystem Design	Pettersson et al. [33]
Measuring User Confidence in Smartphone Security and Privacy	Chin et al. [34]
Drivers of app Installation Likelihood–A Conjoint Analysis of Quality Signals in Mobile Ecosystems	Siegfried et al. [35]
Revealing the Unrevealed: Mining Smartphone Users Privacy Perception on app Markets	Hatamian et al. [36]
A Roadmap for Cloud SECO: EcoData and the New Actors in IoT Era	França et al. [37]
Understanding Business Ecosystem Dynamics: A Data-Driven Approach	Basole et al. [38]
Which Factors Affect the Evangelist's Support During Training Sessions in Mobile Software Ecosystems?	Fontão et al. [39]
Challenges and Solutions for Opening Small and Medium-Scale Industrial Software Platforms	Seidl et al. [40]
How Mobile Game Startups Excel in the Market	Roshan et al. [41]
Lessons Learned from Applying Social Network Analysis on an Industrial Free/Libre/Open Source Software Ecosystem	Teixeira et al. [42]
Openness in the Orchestration of Ecosystems: A Resource-Based Prspective	Schlagwein et al. [43]
Cocreation of Value in a Platform Ecosystem! The Case of Enterprise Software	Ceccagnoli et al. [44]
Mobile Environments and Innovation Co-creation Processes & Ecosystems	Wong et al. [45]

[33] O. Pettersson, M. Svensson, D. Gil, J. Andersson, and M. Milrad, "On the role of software process modeling in software ecosystem design," in *Proceedings of the European Conference on Software Architecture: Companion Volume*, pp. 103–110, ACM, 2010.

[34] E. Chin, A. P. Felt, V. Sekar, and D. Wagner, "Measuring user confidence in smartphone security and privacy," in *Proceedings of the Symposium on Usable Privacy and Security*, p. 1, ACM, 2012.

[35] N. Siegfried, O. Koch, and A. Benlian, "Drivers of app installation likelihood–a conjoint analysis of quality signals in mobile ecosystems," in *Proceedings of the International Conference on Information Systems*, pp. 1–18, AISEL, 2015.

[36] M. Hatamian, J. Serna, and K. Rannenberg, "Revealing the unrevealed: Mining smartphone users privacy perception on app markets," *Computers & Security*, vol. 83, pp. 332–353, 2019.

[37] M. França, R. Santos, and C. Werner, "A roadmap for cloud seco: Ecodata and the new actors in iot era," in *Proceedings of the International Conference on Distributed Computing in Sensor Systems*, pp. 218–223, IEEE, 2015.

[38] R. C. Basole, M. G. Russell, J. Huhtamäki, N. Rubens, K. Still, and H. Park, "Understanding business ecosystem dynamics: A data-driven approach," *ACM Transactions on Management Information Systems*, vol. 6, no. 2, p. 6, 2015.

[39] A. Fontão, B. Estácio, J. Fernandes, R. P. dos Santos, and A. C. Dias-Neto, "Which factors affect the evangelist's support during training sessions in mobile software ecosystems?," in *Proceedings of the European Conference on Software Architecture: Companion Proceedings*, p. 22, ACM, 2018.

[40] C. Seidl, T. Berger, C. Elsner, and K.-B. Schultis, "Challenges and solutions for opening small and medium-scale industrial software platforms," in *Proceedings of the International Systems and Software Product Line Conference-Volume A*, pp. 153–162, ACM, 2017.

[41] M. Roshan Kokabha, V. Tuunainen, and R. Hekkala, "How mobile game startups excel in the market," in *Proceedings of the Hawaii International Conference on System Sciences*, p. 10, Scholar Space, 2019.

[42] J. Teixeira, G. Robles, and J. M. González-Barahona, "Lessons learned from applying social network analysis on an industrial free/libre/open source software ecosystem," *Journal of Internet Services and Applications*, vol. 6, no. 1, p. 14, 2015.

[43] D. Schlagwein, D. Schoder, and K. Fischbach, "Openness in the orchestration of ecosystems: A resource-based perspective," *Working Papers on Information Systems*, vol. 1, pp. 43–60, 2010.

[44] M. Ceccagnoli, C. Forman, P. Huang, and D. Wu, "Cocreation of value in a platform ecosystem! the case of enterprise software," *MIS quarterly*, vol. 36, no. 1, pp. 263–290, 2012.

[45] T. Y. Wong, G. Peko, D. Sundaram, and S. Piramuthu, "Mobile environments and innovation co-creation processes & ecosystems," *Information & Management*, vol. 53, no. 3, pp. 336–344, 2016.