The Digital Operational Resilience Act for Financial Services: A Comparative Gap Analysis and Literature Review

Anita Neumannová[1](✉), Edward W. N. Bernroider[1], and Christoph Elshuber[2]

[1] Institute for Information Management and Control, Vienna University of Economics and Business (WU Vienna), Welthandelsplatz 1/D2/C, 1020 Vienna, Austria
{anita.neumannova,edward.bernroider}@wu.ac.at

[2] NTT DATA Deutschland GmbH, Hans-Döllgast-Straße 26, 80807 Munich, Germany
christoph.elshuber@nttdata.com

Abstract. Regulatory bodies, driven by enhanced speed of digital transformations, seek to strengthen the resilience of information and communication technologies (ICT) to ensure their operational integrity. As a result, The Digital Operational Resilience Act (DORA) was recently proposed to unify and enhance ICT risk management of financial institutions by recommending stricter rules. ICT risk management has to date been mainly governed by ISO 27001:2013 standard in the context of information security governance. Based on qualitative content analysis, we firstly mapped ISO 27001:2013 to DORA and identified nine gaps in ISO 27001:2013 in relation to six general DORA requirements. While we find sufficient support in academic literature for six of the nine extensions suggested by DORA, three areas seem less supported: Threat-led penetration testing, major incident management, and ICT third-party risk management. We argue that these topics should serve academic interest to further our understanding of digital operational resilience in theory and practice.

Keywords: Digital Operational Resilience · DORA · ISO 27001:2013 · Mapping analysis · IT risk management

1 Introduction

To account for the increased number of digital transformations and to ensure the secureness of financial industry, European policy makers have recently introduced the Digital Operational Resilience Act (DORA) for financial services [1]. European policy makers have long been aiming to unify regulations in financial institutions, especially those connected to information and communication technologies (ICT) risks (e.g., digital operations) [2]. ICT risk and security standards are embedded in existing information technology (IT) governance frameworks (e.g., ITIL, COBIT) or certification standards (e.g., ISO) [3, 4 5], which are utilized by numerous financial institutions. Nevertheless, the extant IT governance frameworks or standards have varying focuses [6, 7], which

M. Papadaki et al. (Eds.): EMCIS 2022, LNBIP 464, pp. 570–585, 2023.
https://doi.org/10.1007/978-3-031-30694-5_40

complicates the assessment of DORA's impact on the ICT risk management rules in financial institutions.

According to academic literature, IT governance can either prescribe strategies connected to leadership involvement [7, 8] or can set specific process steps to guard operations [6, 9]. DORA unifies regulations connected to ICT risk management, cybersecurity, third-party risk exposure, and brings to the forefront the need for leadership involvement to portray resilience. Albeit DORA is primarily focused on securing the digital operations of financial institutions, its integration of leadership involvement provides the most comprehensive directive on ICT risks to date.

Financial institutions, to safeguard digital operations, are known to possess the ISO 27001:2013 certification which specifically addresses ICT risk management [10], and which has been used as a baseline for DORA's requirements [11]. Nevertheless, ICT risk management and its specifics have been scarcely addressed as attributes of resilience by the information systems (IS) literature [12]. Consequently, more research is warranted to show how well DORA relates to both, current standards in practices and known attributes of resilience in the IS literature. We seek to uncover DORA's relation with ISO 27001:2013 and examine its requirements from the perspective of prior resilience focused studies. In order to do so, we seek to address the following research questions:

RQ1: *How do ICT risk management requirements of DORA compare to ICT security management standards of ISO 27001:2013?*

RQ2: *How are (if any) extended DORA requirements supported by IS literature on digital resilience?*

To answer these questions, firstly, we extended a mapping method previously used in a similar context [13, 14, 15] by implementing a comparative qualitative content analysis from medical studies [16] in order to map DORA's requirements to ISO 27001:2013. Secondly, we have aligned DORA's requirements to resilience attributes considered in prior IS literature. Our findings are relevant to both academia and practice in relation to ICT risk management and IT auditing, especially to those trying to understand implications and the rationale of new policy measures to safeguard the ICT of financial institutions.

2 Conceptual Background

2.1 Digital Operational Resilience Act (DORA)

The need to strengthen the resilience of firms has been a focal point of discussions not only among academia, but also practitioners and policy makers [17, 18]. Policy makers and practitioners mainly attribute resilience to ICT security standards (e.g., ICT risk management principles) [1, 19, 20]. Within the financial industry, the directives partly addressing ICT risk management can be traced back to the 2008 due to the derailing events of 2008 Financial Crisis. The financial crisis underlined the need to strengthen the financial standing of numerous countries which resulted in ongoing regulatory advances aiming to strengthen resilience of financial institutions. Albeit, as became highly visible, these regulations omitted the digitalization advances and only focused on operational resilience – not the specifics of ICTs and risks associated with their implementation [2]. The crisis driven by Covid-19 pandemic shed light onto the risk aspects concerning digital transformations or digital operations in the financial industry, as the switch to fully remote work opened doors to numerous cyber-attacks as well as increased ICT vulnerabilities [21]. This impacted the stability and integrity of the European financial industry, prompting the European Union (EU) to establish detailed and comprehensive framework to maintain operational resilience of ICT – i.e., Digital Operational Resilience Act (DORA) [1].

The general aim of DORA is to ensure consistency in ICT risk management throughout the financial industry and to introduce the concept of digital operational resilience (DOR). As a result, its implications will not only affect large incumbents, but also high-tech growing enterprises (i.e., FinTechs) and their partners [1, 20]. Nevertheless, DORA's diverse requirements do not include the focus on microenterprises, which are, for this purpose, defined as firms employing less than 10 employees, and whose annual turnover or balance sheet does not exceed EUR 2 million [22]. The implementation of DORA is intended to improve and standardize ICT risk management, ICT-related incident reporting, in-depth auditing of ICT systems, and the oversight of critical third-party ICT risks [20]. Additionally, it strives to raise awareness of cyber risks and ICT-related incidents among upper management and supervisory authorities [2].

To ensure digital operational resilience (DOR), DORA stands on six main pillars with each having its own requirements towards financial institution (please see Table 1). Albeit, in its current draft DORA stands on five pillars, we list ICT governance separately to emphasize its importance for resilience [23, 24]. Firstly, DORA explicitly defines the requirements on the management body regarding ICT risks management. The internal governance and control frameworks have to be deployed and the management body shall be accountable for defining, approving and monitoring all arrangements regarding the ICT risk management framework. Moreover, DORA calls for state-of-the art ICT systems, asset inventory and initial audits to ensure the protection and prevention of ICT risks. It further stipulates the need to map the risks both internally and with external service providers. Next, DORA defines processes for ICT incident management. It distinguished two types of incidents (normal and major), and further defines steps on reporting major incidents to government, media, and partners, as well as their supervisory feedback. DORA further underlines the need for regular testing of performance, ICT tools and systems to increase resilience of financial institutions. It states the requirements on threat-led penetration testing and adds advanced testing as an additional part financial institutions have to account for. DORA greatly calls for the assessment of outsourcing agreements and sets their key contractual provisions. In lieu, it provides a framework for critical ICT third-party providers' assessment which is to be defined and implemented by European policy makers. Lastly, it describes information sharing agreements with competitors and partners in regard to cyber intelligence and threats. Altogether these requirements portray DORA's explicit operational demands to ensure ICT risk management of financial institutions.

2.2 Information Security Management Systems (ISMS) – ISO 27001:2013

The regulatory directives governing ICT security or risk management (e.g., DORA) are known to draw information from existing certification standards such as the international standards organization (ISO) [11] or the popular IT governance frameworks of ITIL or COBIT [3, 25]. With respect to operation secureness and resilience, ISO offers numerous

Table 1. DORA's main requirements

Requirement	Aim	DORA Articles
R1: ICT governance	To set requirements on internal governance and control decisions	Art. 4
R2: ICT risk management	To provide boundary conditions to prevent ICT risk exposure and ensure recovery methods	Art. 5–14
R3: ICT-related incidents management, classification and reporting	To prescribe adequate incident response and communication management	Art. 15–20
R4: Digital operational resilience testing	To set controls for regular audits, performance test and penetration tests	Art. 21–24
R5: Managing of ICT third-party risk	To lessen external risk exposure and assess contractual provisions on ICT third-party providers	Art. 25–39
R6: Information-Sharing Agreements	To prescribe regulations on information exchange regarding cyber threats and intelligence	Art. 40

certification choices firms and financial institutions can choose from. Firstly, the choice can range from business capacity management (e.g., ISO 22301:2019), resilience management (e.g., ISO 22313:2020) or even ICT risk management (e.g., ISO 27005). The most comprehensive measure on ICT risk management and operation secureness, however, comprises of ISO 27001:2013 [26]. This certification encompasses every section of information security related measures and has been known to be widely used across numerous financial institutions [27].

Prior to DORA's introduction, the European Banking Authority (EBA) within its final report on ICT risk management, in addition, proposed to tailor ISO 27001:2013 as a baseline on ICT risk management [11]. We, therefore, suggest that the possession of ISO 27001:2013 can be viewed as a standard for ICT risk management of EU financial institutions and shall be contextually comparable to the requirements of DORA. Nevertheless, academic circles argue ISO guidelines are generic in scope and based on universal principles to make them applicable to a wide set of organizations. They are not context-specific and, consequently, cannot account for all aspects and needs of various financial institution [28]. Altogether, it is imperative to understand the support among ISO 27001: 2013 guidelines and DORA's requirements, as DORA is contextually specific to the needs of digitalization advances and their secureness in the financial industry.

2.3 Resilience in the IS Literature

Notwithstanding, academics underline resilience as a research concept has been highly fragmented across various research domains, portraying its multidisciplinary aspect [12].

Research on resilience was further influenced by different levels of analysis, consideration of regulatory requirements [29]. Presently, due to the strain on ICT in numerous organizations driven by Covid-19 pandemic and with the introduction of DORA, a new definition emerged – digital operational resilience (DOR). According to policy makers, DOR is defined as "*the ability of (a financial entity) to build, assure and review its operational integrity from a technological perspective*" [1]. Arguably, this new definition brings to the forefront the need to both safeguard and utilize IS to ensure the resilience of the organization as a whole.

According to DORA, in crisis situations IS and their operability need to be safeguarded through ICT risk management and IT governance [19] to portray DOR. Two topics which have rarely been emphasized in prior resilience literature in the IS research [12, 23]. For instance, Sarkar et al. [8, 23] aimed to link IT governance to resilience, however, their focus has been on leadership involvement and commitment as opposed to specific operational secureness practices which are the core of DORA. The focus on securing or recovering operations and their connection to resilience can be, to a certain degree, visible in the research of business continuity plans (BCP) and disaster recovery plans (DRP) [30, 31]. Albeit both Baham et al. [30], Sakurai and Chughtai [31] underline BCP and DRP mainly address the recovery of complex IS as opposed to ensuring their operability. Consequently, this opens questions regarding resilience attributes postulated by academics and their coverage of DORA's requirements.

3 Methodology

An effective approach to capture and compare two texts, especially frameworks, is through a mapping method [13, 14]. These methods are derived from the principles of qualitative content analysis to allow for "*rendering the rich meaning*" [32] and enable document observation to make inferences [33]. To ensure reliability of our analysis, we have followed content analysis standards offered by IS research [34, 35], which we enriched by considering comparative content analysis in healthcare research [16, 36]. These additions include the closeness of content and its interpretation among two or more texts [37]. The closeness of content is either manifested (text closeness in wording or interpretation) or latent (describes distance from the text while still rendering close interpretation) [36, 37].

Overall, comparative content analysis should stand on procedural steps which ensure its reliability [38, 39]. Following Nasir [34], firstly, we have chosen the texts to be examined (DORA and ISO 27001:2013). Secondly, we have selected the units of analysis. In DORA, we have identified single articles (4–40) which address ICT security management and in ISO 27001:2013 we have utilized its division into single controls and annexes. Thirdly, we have identified the theme categories. The themes have been determined by the titles of selected DORA's articles. Next, we have pinpointed key aspects of each DORA article and searched for these key aspects within ISO 27001:2013 [35]. Following Barello et al. [16], we have firstly compared the manifested key aspects (i.e., searching for exact wording comparison) before proceeding to search for latent content (i.e., searching for the synonyms of key aspects). This is a step visible in mapping analyses of IT Governance frameworks [14], and which allowed us to render a richer meaning as not every definition, description and interpretation is identical in each of the texts. For example, considering third-party risk exposure, DORA classifies this as “*third-party or external vendors*”, whereas ISO uses the terminology of “*suppliers or supplier services*”. Following, we have categorized each DORA article dependent on the level of support by ISO 27001:2013 controls. When a majority of DORA’s key aspects have been supported, we identified the article as largely covered, when part of the DORA’s article key aspects could not be mapped, we have classified this article as partly covered, and when no ISO 27001:2013 controls could be mapped to key aspects, we have classified this article as not covered by ISO 27001:2013. Next, we have determined differences among the two texts by inferring which DORA’s key aspects were only partly, or not at all supported by ISO 27001:2013 controls. As a last step, the differences were summarized into overall gaps.

To purport and justify our findings in relevance to extant resilience attributes in IS literature, we have surface-searched for peer-reviewed articles, which addressed resilience as well as the identified differences per each gap. Following prior non-exhaustive literature reviews in the IS research [40, 41], we have focused on the following major IS journals and IS conferences: BISE, CAIS, EJIS, ISJ, ISR, JAIS, JIT, JMIS, JSIS, MISQ, MISQe, PAJAIS, AMCIS, ECIS, HICSS, ICIS, PACIS [12, 41]. To assess these outlets, we have queried AIS electronic library and EBSCO Business Premier databases, and searched for the following phrases: “resilient OR resiliency OR resilience” (abstract) AND “*identified difference*” (all text) [12, 41]. We have accumulated number of results for each query as hits and assessed them for final consideration per each gap (please see Table 2). Firstly, we have excluded short-papers, research-in-progress papers, as well as articles stating matters or opinions [41]. Subsequently, we focused on articles on resilience, and which addressed, even if marginally, the differences our prior mapping analysis has identified. Altogether, as some of the final articles addressed more than one gap, we have collected 18 articles spread among 8 outlets out of the 17 given above for our subsequent analysis (please see Table 3).

Table 2. Literature search

Gap	Search Term	Hits	Final
G1	Leadership involvement	33	10
	Leadership commitment	21	
G2	Risk identification	27	9
	Risk mapping	29	
G3	Back-up policy	13	5
G4	Incident review	27	6
	Incident documentation	21	

(*continued*)

Table 2. (*continued*)

Gap	Search Term	Hits	Final
G5	Incident communication	27	5
	External communication	48	
G6	Major incident	24	0
G7	Penetration test	8	1
G8	Third-party risk	22	0
	Outsourcing risk	10	
G9	Information sharing	90	3

Table 3. Number of relevant articles per outlet

<table>
<tr><th colspan="6">Journals</th></tr>
<tr><td colspan="2">CAIS</td><td colspan="2">ISJ</td><td colspan="2">MISQ</td></tr>
<tr><td colspan="2">2</td><td colspan="2">1</td><td colspan="2">2</td></tr>
<tr><td colspan="3">MISQe</td><td colspan="3">PAJAIS</td></tr>
<tr><td colspan="3">2</td><td colspan="3">1</td></tr>
<tr><td colspan="6">BISE, EJIS, ISR, JAIS, JIT, JMIS, JSIS</td></tr>
<tr><td colspan="6">0</td></tr>
</table>

<table>
<tr><th colspan="3">Conferences</th></tr>
<tr><td>AMCIS</td><td>HICSS</td><td>ICIS</td></tr>
<tr><td>4</td><td>2</td><td>4</td></tr>
<tr><td colspan="3">ECIS, PACIS</td></tr>
<tr><td colspan="3">0</td></tr>
</table>

4 Findings

Albeit ISO 27001:2013 is a widely used certification ensuring the ICT security standards of financial institutions, certain DORA's requirements are either partly or not supported by ISO 27001:2013 controls. Overall, we have identified 37 articles (Art. 4–40) in DORA that prescribe its requirements towards ICT risk management of financial institutions. Firstly, out of the 37 Articles, 16 were focused on stating regulations to ESA, EBA, and EU Commission (Articles 14, 18–20, and 28–39). These articles we have omitted from our analysis, as our focus does not comprise of requirements towards policy makers. Secondly, our findings indicate the support of DORA's articles in ISO 27001:2013 is the following: 7 articles were largely mapped (Art. 5–6, 8–10, 21–22), 7 articles were partly mapped (Art. 4, 7, 11–13, 15, 25) and 7 articles could not be mapped (Art. 16–17, 23–24, 26–27, 40) to ISO 27001:2013 controls and annexes. This is mainly driven by abstractedness in the ISO 27001:2013 language when compared to the detailed and descriptive one of DORA. The 14 articles (67% of analyzed articles) that were partly or not mapped to ISO 27001:2013 controls overall culminated in 9 gaps (please see Table 4): Leadership and commitment (Art 4.), Risk mapping and identification (Art. 7), Backup recovery times and policies (Art. 11), ICT incident review and documentation (Art. 12), External incident communication (Art. 13 and Art.15), Major ICT incident (Art. 16–17), Threat-led penetration testing (Art. 23–24), ICT third-party risk assessment (Art. 25–27) and Information-sharing arrangements (Art. 40).

Firstly, the gap on leadership and commitment stems from ISO's 27001:2013 marginal demands to leadership accountability. Even though ISO 27001:2013 controls 5, 9.3, and annex A.7.2.1 require the leadership commitment to a certain degree, majority of other controls prescribe accountability to the organization as opposed to leadership (e.g., controls 6, 7, and 8.1). Next, ISO 27001:2013 controls 4, 6.1.1-.1.2, and 8.2 are not explicit about the timing of internal risk reviews, the mapping of external risk, and the involvement of third-party service providers. This culminates in a gap in risk mapping and identification. The gap on backup recovery times and policies stems from insufficient information on precise incident recovery times, and the handling of third-party service providers in ISO 27001:2013 annexes A.9.1, A.12.2-.3, A.17.2. ICT incident review and documentation discrepancies result from ISO 27001:2013 limited support in controls 9.1, 9.3, 10, and annexes A.12.6.1, A.16.1.6-.7 of post ICT incident reviews, the mapping for future risks, and the specific documentation requirements. Apart from that, ISO 27001:2013 does not ask for communication plans and policies to be aligned both internally and with external partners resulting in a gap on external incident communication. Albeit the external incident communication is partially addressed in ISO 27001:2013 control 7.4 and annex A.16, neither mentions the involvement of governing bodies, media, and external partners. Moreover, ISO 27001:2013 does not define and distinguish major incident in annex A.16. The same applies to threat-led penetration testing which is not supported by a single control or annex. Albeit ISO 27001:2013 marginally addresses ICT third-party risk assessment in controls 4.2, 8.1, and annexes A.14.2.7, A.15, it does not contextually specify the needs or risks associated with "third-party" service providers, does not depict third-party risk assessments or third-party contractual agreements. Lastly, no control or annex in ISO 27001:2013 supports the requirements for information sharing arrangements which culminates in the last observed gap. Our findings overall distinguish DORA's requirements as more complex and explicit when mapped with ISO 27001:2013 controls and annexes.

As a last step, we mapped the uncovered nine gaps of ISO 27001:2013 in relation to DORA to extant resilience attributes within selected IS articles. Our findings indicate that six (G1–5, 9) of the gaps have been addressed by IS research, whereas three (G6–8) were hardly portrayed (please see Table 5): major ICT incidents, threat-led penetration testing, and third-party risk assessment. These three gaps clearly lack academic support and warrant the most attention by IS research according to our analysis. Firstly, albeit Green et al. [42] underlie the need of adequate testing of ICT, they do not stipulate advanced tests or threat-led penetration tests ensure resilience (G7). Secondly, although information on incident management, reporting or communication is addressed within the uncovered articles, neither defines the difference nor distinguishes between major and minor incident resulting in no identified article covering major incidents (G6). The same applies to the gap on third-party risk assessments (G8).

Table 4. ISO 27001:2013 support of DORA requirements

DORA		**ISO 27001**	
Requirement	**Key Area**	**Support**	**Gaps**
ICT governance **(R1)**	Art. 4: Governance and organization	5.1; 5.2; 5.3; 6.1; 6.2; 7.1; 7.2; 7.3; 7.4; 8.1; 9.2; 9.3; A.5.1; A.6.1; A.7.2.1; A.18.2.2	Leadership involvement and commitment **(G1)**
ICT risk management **(R2)**	Art. 7: Identification	4.1; 4.2; 6.1.1; 6.1.2; 8.2; 9.1; 9.2; A.8.1.1; A.8.2; A.15.1.2; A.15.2.1; A.18.1.1; A.18.2.3	Risk mapping and identification **(G2)**
	Art. 11: Backup policies and recovery methods	A.9.1; A.12.2; A.12.3; A.17.2	Back-up recovery times and policies **(G3)**
	Art. 12: Learning and evolving	9.1; 9.3; 10; A.12.6.1; A.16.1.6; A.16.1.7; A.17.1.3	ICT incident review and documentation **(G4)**
	Art. 13: Communication	7.4; A.15.1.3; A.16	External incident communication **(G5)**
ICT-related incidents **(R3)**	Art. 15: ICT-related incident management process	A.16	
	Art. 16: Classification of ICT-related incidents	n/a	Major ICT incidents **(G6)**
	Art. 17: Reporting of major ICT-related incidents	n/a	
DOR testing **(R4)**	Art. 23: Advanced testing of ICT tools, systems and processes based on threat led penetration testing	n/a	Threat-led penetration testing **(G7)**
	Art. 24: Requirements for testers	n/a	
Managing of ICT third-party risk **(R5)**	Art. 25: General principles	4.2; 8.1; A.6.1.3; A.13.1.2; A.13.2.2; A.13.2.4; A.14.2.7; A.15; A.18.1.1	Third-party risk assessment **(G8)**

(*continued*)

Table 4. (*continued*)

DORA		**ISO 27001**	
Requirement	**Key Area**	**Support**	**Gaps**
	Art. 26: Preliminary assessment of ICT concentration risk and further-outsourcing arrangements	n/a	
	Art. 27: Key contractual provisions	n/a	
Information-Sharing Agreements **(R6)**	Art. 40: Information-sharing arrangements on cyber threat information and intelligence	n/a	Information-sharing arrangements **(G9)**

Table 5. Mapping of gaps to existing resilience literature in IS

Gaps									
Articles	**G1**	**G2**	**G3**	**G4**	**G5**	**G6**	**G7**	**G8**	**G9**
[43]	x	x	x	x					
[44]		x							
[45]					x				
[42]		x	x	x	x		x		x
[46]	x								
[47]		x	x		x				x
[48]	x								
[49]	x			x					x
[50]	x								
[51]		x		x					
[52]		x		x					
[53]		x			x				
[54]	x		x						
[8]	x	x							
[23]	x								

(*continued*)

Table 5. (*continued*)

Gaps									
Articles	**G1**	**G2**	**G3**	**G4**	**G5**	**G6**	**G7**	**G8**	**G9**
[55]	x								
[56]	x	x	x	x					
[57]					x				

5 Discussion, Limitations and Future Research

In this study we have provided a mapping analysis of DORA to ISO 27001:2013, and subsequently to attributes of resilience addressed by the IS literature. Understanding the regulatory extensions made by DORA is important, as its implementation will have a profound impact on numerous financial institutions and their partners. Firstly, our comparative review makes clear that the possession of ISO 27001:2013 certification or the aim to obtain it, cannot be seen as equivalent in terms of complying with DORA as their discrepancies look substantial given the gaps identified. The mapping analysis portrays that 33% of DORA's analyzed articles are partly covered within the ISO 27001:2013, and 33% of DORA's articles cannot be clearly linked to a single ISO 27001:2013 control or annex. Overall, we have identified nine gaps, which should be of interest to practitioners analyzing financial institutions preparedness for DORA. The majority of the identified difference leading to the gaps appear to stem from the lacking presence of a detailed leadership involvement in ISO 27001:2013 controls and annexes (e.g., G1–3, 5, 8–9) [6, 13].

Secondly, we have reflected on the coverage of the identified gaps of ISO 27001:2013 in relation to DORA in resilience focused IS literature. Results show that differences leading to six of the gaps (G1–5, 9) have been at least discussed in some way among IS academics as resilience attributes. Leadership involvement and commitment (G1) is connected to the presence of leadership-focused IT government frameworks [54, 56] or cyber-security cultures [49]. Leadership involvement can further ensure both risk identification and mapping (G2) as well as strengthened back-up policies (G3) [8, 43, 54]. In addition, back-up policy requirements as well as risk identification are implemented through agile principles [44], cybersecurity assessments [42] or BCP/DRP [53], whereas risk mapping steps are attributed to the usage of combined IT governance frameworks [47]. Apart from that, Park et al. [51] state incident tracking software enables future ICT incident reviews, whereas Baham et al. [43] stress the importance of proper ICT incident documentation to portray resilience (G4). IS researchers address external incident communication (G5) through communication protocols [58], DRP [43, 53], situational-crisis communication theory [57], or information secureness [59]. Lastly, Marotta and Pearlson [49] position information sharing (G9) as important trust-building procedure leading to cyber-resilience, and Green et al. [42] addressed both benefits and risk associated with information sharing among competitors, as well as to government. Consequently, this support by prior IS research also justifies the presence of these six extended requirements in DORA to portray DOR (in relation to ISO 27001:2013), and in this sense provides further motivation for practitioners applying DORA respectively.

Notwithstanding, we also contribute by explicating three gaps (G6–8) that were hardly addressed in the considered IS literature related to resilience, which may be contemplated in scoping risk-based control-coverage decisions. Simultaneously, our finding calls for future research to gain more evidence to understand the role of these gaps for achieving DOR. Albeit incident management has been addressed by various academic circles, and has been connected to both firm's absorptive capacity [60, 61], as well as to technical debt [62, 63], the distinction between major and minor incidents (G6) does not appear to be broadly addressed in the IS literature on resilience. This is intriguing as existing IT governance frameworks (i.e., ITIL and COBIT) do distinguish among different incident types [5] indicating relevance for DOR of firms. A promising research area could delve deeper into how specific types of ICT incidents (stemming from DORA, ITIL or COBIT) affect firms and which specific steps firms apply in order to withstand them. Secondly, support in academic literature seems to be lacking in terms of the strengthened demand on the management of third-party risk exposure (G8). Under DORA, external partners, cloud vendors especially, should be heavily guarded [20]. A research area not broadly discussed within our subsequent analysis. Risks associates with third-party involvement are primarily found in research focusing on outsourcing strategies [64], or digital innovations and IS project risks [65]. Future research could perform a more detailed and comprehensive literature review and uncover ingrained stipulations on third-party risk management in connection to DOR. Lastly, threat-led penetration testing (TLPT) or advanced testing (G7) has received more attention by practice-oriented research as opposed to academic research. Even though consulting companies address TLPT as a source of lessened ICT risk exposure [66], our subsequent analysis could not find an IS article specifically connecting TLPT to resilience of firms. Future IS research should include these perspectives and specify under which conditions advanced testing or TLPT is imperative for DOR.

6 Conclusion

This paper illustrates differences of what DORA requires in addition to a widely used ICT risk management standard (ISO 27001:2013) through a comparative qualitative content analysis. The comparative analysis identified nine gaps which arose due to ambiguous language of ISO 27001:2013, and the strengthened focus on ICT secureness and third-party risk assessment of DORA. The identified gaps have been subsequently related to prior work in IS with a literature review. Our findings support the view that DORA will demand strengthened controls for financial institutions in terms of ICT risk management based on the applied ISO benchmark. However, some of these demands are barely supported by extant IS literature on resilience, which not only questions the validity of the regulatory extensions in DORA from an academic standpoint, but also calls for future research to better substantiate these extensions. The strengthened demands on threat-led penetration testing (TLPT), third-part risk assessment and the division among major vs. minor incident from DORA should receive further support from academic research. On this basis, we suggest that future IS research should strive to examine the roles of these three gaps in both academic and practical settings. In particular, academics could examine the effectiveness of differentiated approaches for handling different types of ICT incidents, the role of third-party exposure in outsourcing strategies or conduct more empirical research on the role of penetration tests in support of DOR. Further comparative work could include other frameworks such as the CERT-RMM model focusing particularly on ICT operational resilience of diverse enterprises.

References

1. European Commission: Proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, COM/2020/595 final, 2020/0266 (COD) (2020). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595. Accessed 03 Oct 2022
2. Kun, E.: From Operational Risk to Systemic Risk: The EU's Digital Operational Resilience Act for Financial Services (DORA) (2021). https://www.law.kuleuven.be/citip/blog/from-operational-risk-to-systemic-risk/. Accessed 03 Oct 2022
3. Vilarinho, S., da Silva, M.M.: Risk management model in ITIL. Sociotechnical Enterprise Information Systems Design and Integration, pp. 207–214. IGI Global (2013)
4. Bradley, R.V., Byrd, T.A., Pridmore, J.L., Thrasher, E., Pratt, R.M., Mbarika, V.W.: An empirical examination of antecedents and consequences of IT governance in US hospitals. J. Inf. Technol. **27**, 156–177 (2012)
5. Pereira, R., Silva, M.M.D.: A literature review: IT governance guidelines and areas. In: Proceedings of the 6th International Conference on Theory and Practice of Electronic Governance), pp. 320–323. Association for Computing Machinery, Albany, New York, USA (2012)
6. Kumsuprom, S., Corbitt, B., Pittayachawan, S.: ICT risk management in organizations: case studies in Thai business. In: ACIS 2008 Proceedings, 98 (2008)
7. O'Donohue, B., Pye, G., Warren, M.: Improving ICT governance in Australian companies. In: ACIS 2006 Proceedings, 53 (2006)
8. Sarkar, A., Wingreen, S.C., Ascroft, J.: Top management team decision priorities to drive IS resilience: lessons from jade software corporation. In: AMCIS 2016 Proceedings, 10 (2016)
9. Jafarijoo, M., Joshi, K.: IT governance: review, synthesis, and directions for future research. In: AMCIS 2021 Proceedings, 5 (2021)
10. So, I.G., Setiadi, N.J., Papak, B., Aryanto, R.: Action design of information systems security governance for bank using COBIT 4.1 and control standard of ISO 27001. Adv. Mater. Res. **905**, 663–668 (2014)
11. European Banking Authority: Final report on EBA Guidelines on ICT and security risk management, EBA/GL/2019/04 (2019). https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management. Accessed 03 Oct 2022
12. Weber, M., Hacker, J., vom Brocke, J.: Resilience in information systems research-a literature review from a socio-technical and temporal perspective. In: ICIS 2021 Proceedings, 3 (2021)
13. von Solms, B.: Information Security governance: COBIT or ISO 17799 or both? Comput. Secur. **24**, 99–104 (2005)
14. ITGI, OGC, Information Systems Audit and Control Association: Aligning COBIT, ITIL and ISO 17799 for Business Benefit: Management Summary (2005). http://www.itgi.org. Accessed 03 Oct 2022
15. Sheikhpour, R., Modiri, N.: An approach to map COBIT processes to ISO/IEC 27001 information security management controls. Int. J. Secur. Appl. **6**, 13–28 (2012)

16. Barello, S., Graffigna, G., Vegni, E.: Patient engagement as an emerging challenge for healthcare services: mapping the literature. Nutr. Res. Pract. **2012**, 1–7 (2012)
17. Bhamra, R., Dani, S., Burnard, K.: Resilience: the concept, a literature review and future directions. Int. J. Prod. Res. **49**, 5375–5393 (2011)
18. Hillmann, J., Guenther, E.: Organizational resilience: a valuable construct for management research? Int. J. Manage. Rev. **23**, 7–44 (2021)
19. Leo, M.: Operational resilience disclosures by banks: analysis of annual reports. Risks **8**, 128 (2020)
20. Scott, H.S.: The EU's Digital Operational Resilience Act: Cloud Services & Financial Companies (2021). https://ssrn.com/abstract=3904113
21. Lallie, H.S., et al.: Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Comput. Secur. **105**, 1–20 (2021)
22. European Commission: Commission recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, 2003/361/EC (2003). https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:en:PDF. Accessed 03 Oct 2022
23. Sarkar, A., Wingreen, S.C., Ascroft, J.: Towards a practice-based view of information systems resilience using the lens of critical realism. In: Proceedings of the 53rd Hawaii International Conference on System Sciences, pp. 6184–6193 (2020)
24. McManus, S., Seville, E., Brunsden, D., Vargo, J.: Resilience management: a framework for assessing and improving the resilience of organisations. Resilient Organisations Research Report University of Canterbury, Civil and Natural Resources Engineering (2007)
25. Ivanov, M., Stefanov, B.: Approaching risk management in IT by implementing it in ITIL. Electrotech. Electronica **49**(9–10), 2–9 (2014)
26. ISO/IEC 27001:2013. https://www.iso.org/standard/54534.html. Accessed 03 Oct 2022
27. van der Stoop, T.: ISO 27001 in the banking industry: "One standard to rule them all" (2009). https://advisera.com/27001academy/blog/2019/11/25/iso-27001-for-banks-a-game-changing-security-investment/. Accessed 03 Oct 2022
28. Siponen, M., Willison, R.: Information security management standards: problems and solutions. Inf. Manage. **46**, 267–270 (2009)
29. Müller, G., Koslowski, T. G., Accorsi, R.: Resilience - a new research field in business information systems? In: Abramowicz, W. (ed.) BIS 2013. LNBIP, vol. 160, pp. 3–14. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-41687-3_2
30. Baham, C., Hirschheim, R., Calderon, A.A., Kisekka, V.: An agile methodology for the disaster recovery of information systems under catastrophic scenarios. J. Manage. Inf. Syst. **34**, 633–663 (2017)
31. Sakurai, M., Chughtai, H.: Resilience against crises: COVID-19 and lessons from natural disasters. Eur. J. Inf. Syst. **29**, 585–594 (2020)
32. Duriau, V.J., Reger, R.K., Pfarrer, M.D.: A content analysis of the content analysis literature in organization studies: research themes, data sources, and methodological refinements. Organ. Res. Methods **10**, 5–34 (2007)
33. Prasad, B.D.: Content analysis. Res. Methods Soc. Work **5**, 1–20 (2008)
34. Nasir, S.: The development, change, and transformation of management information systems (MIS): a content analysis of articles published in business and marketing journals. Int. J. Inf. Manage. **25**, 442–457 (2005)
35. Gallivan, M.J.: Striking a balance between trust and control in a virtual organization: a content analysis of open source software case studies. Inf. Syst. J. **11**, 277–304 (2001)
36. Graneheim, U.H., Lindgren, B.-M., Lundman, B.: Methodological challenges in qualitative content analysis: a discussion paper. Nurse Educ. Today **56**, 29–34 (2017)
37. Graneheim, U.H., Lundman, B.: Qualitative content analysis in nursing research: concepts, procedures and measures to achieve trustworthiness. Nurse Educ. Today **24**, 105–112 (2004)

38. Insch, G.S., Moore, J.E., Murphy, L.D.: Content analysis in leadership research: examples, procedures, and suggestions for future use. Leadersh. Q. **8**, 1–25 (1997)
39. Krippendorff, K.: Content Analysis: An Introduction to its Methodology. Sage publications, Thousand oaks (2018)
40. vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., Cleven, A.: Standing on the shoulders of giants: challenges and recommendations of literature search in information systems research. Commun. Assoc. Inf. Syst. **37**(1), 205–224 (2015)
41. Kohn, V.: How the coronavirus pandemic affects the digital resilience of employees. In: ICIS 2020 Proceedings, 6 (2020)
42. Green, A.W., Woszczynski, A.B., Dodson, K., Easton, P.: Responding to cybersecurity challenges: Securing vulnerable US emergency alert systems. Commun. Assoc. Inf. Syst. **46**, 187–208 (2020)
43. Baham, C., Calderon, A., Hirschheim, R.: Applying a layered framework to disaster recovery. Commun. Assoc. Inf. Syst. **40**, 277–293 (2017)
44. Baskerville, R., Pries-Heje, J.: Achieving resilience through agility. In: ICIS 2021 Proceedings, 8 (2021)
45. Butler, B.S., Bateman, P.J., Gray, P.H., Diamant, E.I.: An attraction–selection–attrition theory of online community size and resilience. MIS Q. **38**, 699–729 (2014)
46. Heeks, R., Ospina, A.V.: Conceptualising the link between information systems and resilience: a developing country field study. Inf. Syst. J. **29**, 70–96 (2019)
47. Junglas, I., Ives, B.: Recovering IT in a disaster: lessons from hurricane katrina. MIS Q. Exec. **6**, 39–51 (2007)
48. Lacity, M.C., Reynolds, P.: Cloud services practices for small and medium-sized enterprises. MIS Q. Exec. **13**, 31–44 (2014)
49. Marotta, A., Pearlson, K.: A culture of cybersecurity at Banca Popolare di Sondrio. In: AMCIS 2019 Proceedings, 24 (2019)
50. Morisse, M., Prigge, C.: Design of a business resilience model for Industry 4.0 manufacturers. In: AMCIS 2017 Proceedings, 4 (2017)
51. Park, I., Sharman, R., Rao, H.R.: Disaster experience and hospital information systems. MIS Q. **39**, 317–344 (2015)
52. Rehm, S.-V., Georg Schaffner, L., Goel, L.: Framing dialogues on cyber-resilience on boards. In: ICIS 2021 Proceedings, 10 (2021)
53. Sakurai, M., Kokuryo, J.: Design of a resilient information system for disaster response. In: ICIS 2014 Proceedings, 5 (2014)
54. Sarkar, A., Traubinger, T.: IS Resilience decision priorities at german smes: a q-method approach. In: AMCIS 2021 Proceedings, 19 (2021)
55. Sarkar, A., Wingreen, S., Ascroft, J., Sharma, R.: Bouncing back after a crisis: lessons from senior management team to drive IS resilience. In: Proceedings of the 54th Hawaii International Conference on System Sciences, pp. 6712–6721 (2021)
56. Sarkar, A., Wingreen, S.C., Cragg, P.: CEO decision making under crisis: an agency theory perspective. Pac. Asia J. Assoc. Inf. Syst. **9**(2), 1–22 (2017)
57. Syed, R., Dhillon, G.: Dynamics of data breaches in online social networks: Understanding threats to organizational information security reputation. In: ICIS 2015 Proceedings, 14 (2015)
58. Carlo, J.L., Lyytinen, K., Boland, R.J.: Systemic risk, IT artifacts, and high reliability organizations: a case of constructing a radical architecture. All Sprouts Content **4**(2), 57–73 (2008)
59. Conklin, W.: Information sharing and emergency services: an examination using information security principles. In: AMCIS 2008 Proceedings, 12 (2008)
60. Grispos, G., Glisson, W.B., Storer, T.: Rethinking security incident response: the integration of agile principles. In: AMCIS 2014 Proceedings, 9 (2014)

61. Mehrizi, M.H.R., Nicolini, D., Mòdol, J.R.: How do organizations learn from information systems incidents? A synthesis of the past, present and future. MIS Q. **46**, 531–590 (2022)
62. Alves, N.S.R., Mendes, T.S., De Mendonça, M.G., Spínola, R.O., Shull, F., Seaman, C.: Identification and management of technical debt: a systematic mapping study. Inf. Softw. Technol. **70**, 100–121 (2016)
63. Nielsen, M.E., Østergaard Madsen, C., Lungu, M.F.: Technical debt management: a systematic literature review and research agenda for digital government. In: Viale Pereira, G. (ed.) EGOV 2020. LNCS, vol. 12219, pp. 121–137. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-57599-1_10
64. Beck, R., Schott, K., Gregory, R.W.: Mindful management practices in global multivendor ISD outsourcing projects. Scand. J. Inf. Syst. **23**(2), 5–28 (2011)
65. Hoermann, S., Schermann, M., Krcmar, H.: When to manage risks in IS projects: an exploratory analysis of longitudinal risk reports. In: Proceeding of 10th International Conference on Wirtschaftsinformatik, pp. 871–880 (2011)
66. Deloitte: Deloitte's Cyber Risk capabilities, Cyber Strategy, Secure, Vigilant, and Resilient. https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-risk-advisory-cyber-brochure.pdf. Accessed 03 Oct 2022