Towards a Classification of IT Control Areas for Government Digitalization

Maria Haasnoot(✉), Marijn Janssen, and Nitesh Bharosa

Technical University of Delft, Delft, Netherlands
m.a.haasnoot@tudelft.nl

Abstract. Governments struggle to exercise control over their digitalization efforts, often with many risks and uncertainties. Literature on IT control provides a fragmented understanding of government-specific digitalization areas. This paper systematically identifies and analyzes different areas of IT control through a systematic literature review, resulting in a novel classification. The literature review reveals that the current classifications of IT controls are fragmented, lack coherence, are incomplete, and depend on the research field and the language in which the data was collected. The novel classification presented in the paper focuses not only on technology, but also on the whole domain of digitalization, including the arrangements of organizations and projects, data management, agreements with other organizations, and the achievement of political ambitions and goals. This paper gives insights into the areas of control and argues that more research is needed to understand differences among government IT control approaches.

Keywords: IT control · IT controlling · Government · Digitalization · Classification · Systematic Literature Review

1 Introduction

The current focus on integrating digital technologies like AI, Algorithms, IoT, and data-driven decision-making in organizations underscores a continuing impact of IT on public organization processes and functions. However, the implementation and use of IT come with risk and uncertainty, even with failure [1, p. 4, 2, 3, pp. 24–25]. This calls for control over IT and digital technologies. Literature on IT control, best practice frameworks on IT governance, or IT auditing provides some guidance, but is often limited to IT general and application controls [4, p. 23]. However, digitalization in government demands a broader scope, because of the need for additional types of control in domains like IT-innovations, digitalization, IT projects, data, and algorithms. Also, as IT develops at a tremendous pace, new types of IT-related controls are constantly emerging, such as Zero Trust Architecture controls [5], AI-driven Anomaly Detection [6], Cloud Security controls [7], or DevOps controls [8]. In the future, there will be more new types of IT controls, also specific to governments; therefore, a clear classification can help specify the (new) types of IT controls and apply them efficiently and effectively. This goes beyond "classic" IT risks such as cybersecurity, access management, or data quality.

Published by Springer Nature Switzerland AG 2026
A. Achilleos et al. (Eds.): I3E 2025, LNCS 16079, pp. 41–54, 2026.
https://doi.org/10.1007/978-3-032-06164-5_4

Compared to the private sector, governments also face IT risks regarding non-compliance with laws and regulations or wasting public funds [9, pp. 16–17]. IT control is therefore "even more important in the public sector than in the private sector" [10] because of its unique characteristics like "the environmental factors, … in organization-environment transactions… and in internal structures and processes" [11, 12], risk-averse culture, and high accountability norms for IT-spending and value and creating social value [9, pp. 16–17].

Given this broad field, this calls for insight into the IT control areas for government. Our main research objective is to develop a *classification of IT control areas for the government.* This can help governments control digitalization initiatives better. In the literature, there are different classifications of IT-controls according to a goal of control, types of risks, or layering of IT systems of organizational structure, but none are specific for the government. Our classification is derived from the risks specific to the government in achieving its objectives.

The paper is structured as follows: The following section provides a theoretical background on IT control, followed by the research methodology, which describes the process of arriving at an overview of controls on digitalization. Then the study is presented, followed by a discussion of our results and the conclusion.

2 Theoretical Background: The Evolution of IT Control

Control theory has evolved over the past 50 years [13]. Control transformed from a bookkeeping function, 'bean counter,' looking back in administration (Hopper 1980, see Table 1 [13, p. 24]), to a 'business partner' looking at the now and future [1, 14]. Nowadays, control also deals with the implementation and risks of IT. Webster's New Collegiate Dictionary (1967) defines control as "to exercise restraining or directing influence over: regulate." [15], a definition widely supported by the scientific community. Over the years, various forms of sub-areas of control have been developed, such as financial, management, business, strategic, internal, and IT control, each with specific definitions. Several theoretical and best-practice models of controls, such as COSO, Sarbanes-Oxley Act (SOX), COBIT, ISO27001, and NIST, permeate the academic field.

With the rise of IT, there was a need to introduce separate controls for Information Technology [3, p. 2]. The literature distinguishes IT control from IT controlling. The word 'IT control' originates from practice and has evolved into frameworks, such as ITIL, COSO, and COBIT [16, 17]. IT control consists of IT general controls and application controls [16, p. 10]. Hamdan gives the follow definition:"IT control is defined as a manual or automated process designed by, or under the supervision of, the company's principal executive and principal IT officers, or persons performing similar functions, and effected by the company's board of directors, management, and other personnel, to provide reasonable assurance regarding the reliability of financial information and transactions and the continued proper operation of the information systems that capture, process and generate them" [18, p. 2]. Chan et al. point out that IT control processes "ensure that the company's IT sustains and extends the company's strategies and objectives." [19, p. 226].

IT control often embraces a risk approach, where the IT controls are focused on mitigating and measuring IT risks. This aligns with Soin and Collier that "risk-based

control needs to be put in place to help ensure, as far as possible, that organizational objectives are achieved." [20, p. 2]. This is visible in new areas like cloud computing and AI algorithms and aligns with the public sector's risk-averse culture.

'IT-controlling' is mainly used in Germanic languages to emphasize the increasingly deeper embedding of IT in the organization with business perspectives [1, p. VII]. Gadatsch tells us that the difference with IT control is that *IT control focuses on the operational management of IT processes and risk management, while IT controlling is concerned with financial management, planning, and value measurement of IT within the broader business strategy* [3, p. 23, 3, p. 2].

With the complexity of IT, new types of control appeared, such as data-processing controlling, electrical data processing controlling (EDP-controlling), Information Processing Controlling (IP-Controlling), Information System Controlling (IS-Controlling), and Information Technology Controlling (IT-Controlling). Some of these controls are already outdated and no longer used in practice [3, p. 12]. A new control area is emerging due to digitalization, resulting in an explosion of big data and the introduction of algorithms for processing this data.

In recent years, the control function is also being digitalized, where the controller uses digital opportunities to create value. This is named "Digital Controlling" by Keimer & Egle [1, p. 7] and talks about the five domains of data, technologies, processes, methods, and competencies that the controller must be able to use. Gadatsch calls this type of control "smart controlling". "The term 'Smart Data' is associated with the innovative character of Big Data, which is primarily linked to the development of new business forms and models." [3, p. 25]. Control is evolving into smart IT controlling from using "smart data associated with the innovative character of Big Data, primarily linked to the development of new business forms and models." [3, p. 25].

In the Netherlands, IT control has further evolved into, e.g., iControl (Dutch government) and Smart IT controlling [21], as well as control of information provision [22]. The leading "i" in iControl refers to "informatization" as the next step after digitization. This is a new term, like "iOverheid", "iSamenleving", "iPlatform", which were introduced in the Dutch government documents in 2011 [23, 24, pp. 273–282]. The term "iGovernment" is also used in UK literature [25]. Overall, iControls shows that information is fragmented and lacks coherence.

The literature shows that various names are used and that there is digitalization development that changes IT control. New areas are coming into existence that are not covered by existing classifications. The evolution of IT-control and the variations of names given to IT-control are included in our Systematic Literature Review in the next section.

3 Research Methodology

This research aims to create a classification of IT control for the government. For this, a Systematic Literature Review (SLR) is conducted in which known areas of IT control are reviewed. We develop the classification of IT control areas by identifying the risk areas to which the IT controls are directed. This systematic literature review is conducted using the steps of Snyder [26]: 1) design, 2) conduct, 3) analysis, and 3) writing the review. The Prisma 2020 method checklists have been followed and fulfilled [27].

In the *design phase*, we formulated the problem statement and purpose detailed in our introduction. We defined our search terms as combinations of 'IT' or 'digitalization' and 'controlling' or 'control' to keep our search broad. Google Scholar and Scopus were selected as databases. Scopus offers the possibility to filter very specifically and thus provides reliability and quality of sources. Google Scholar includes completeness and broad coverage. Together, they provide a strong and complete literature study in which they complement each other well [28]. We limited our scope to 25 years since IT (IT governance, IT projects, IT investments, etc.) is a relatively young and rapidly developing domain.

In the *conduct phase*, we executed the search and fine-tuned the search terms and filters to obtain a suitable dataset. The fine-tuning was tested by checking for the inclusion of expected articles. In Scopus, we limit ourselves to English articles, conference papers, and articles. In the absence of a research area for the government, we opted for the research areas 'Computer Science', 'Business Management and Accounting', and 'Economics, Econometrics, and Finance'. In the Google Scholar database, we encountered that the search phrase constructions were less advanced than Scopus, which made a more extensive set of search phrases necessary. We refined this search by excluding all patents and citation records and limiting the search to the keywords and title. Here, we checked if the expected papers were present in the results. Table 1 gives a summary of the inclusions and exclusions.

Table 1. Inclusion and exclusion criteria

Scopus		**Google Scholar**	
Inclusion		***Exclusion***	
Search Area	Computer Science	*Search Time range*	<2000
	Business Management and Accounting	*Language*	Not English
	Economics, Econometrics and Finance	*Document type*	Patents
Document type	Conference paper		Citation records
	Article,		
Exclusion			
Search Time range	<2000		
Language	Not English		

The results from Scopus could easily be exported; for Google Scholar, a separate tool, Publish Or Perish[1], was needed, resulting in meta-information for 140 documents for Scopus and 382 documents for Google Scholar. These results were combined in one document (spreadsheet) for further analysis. In the *third phase, analyses*, the document meta-information was analyzed for its relevance based on the document information about the scientific domain, journal, title, and abstract. For example, an exclusion based on the title was "…four-stroke engine and its control system" and based on the journal was "Textile Month". As a final step, duplicates between Google Scholar and Scopus were identified, resulting in 223 documents (Table 2).

[1] https://harzing.com/resources/publish-or-perish.

Table 2. Results of SLR

Scopus		
Search term	IT PRE/1 controls	106
in Article title	"IT controlling"	16
OR in Keywords	controlling AND digitalization	15
	control PRE/1 digitalization	3
Nr of documents		**140**
Duplicates		-5
Not relevant (and not duplicate)		-30
To assess		**105**

Scopus + Scholar	
Total	249
Duplicates Scopus and Scholar	-26
To assess	**223**

Google Scholar		
Search terms	allintitle: "IT controls"	106
	allintitle: "IT * controls"	58
	allintitle: "IT * * controls"	57
	allintitle:"IT controlling"	129
	allintitle:"controlling digitalization"	2
	allintitle:"controlling * digitalization"	3
	allintitle:"controlling * * digitalization"	6
	allintitle:"control * digitalization"	21
Nr of documents		**382**
Duplicates		-98
Not relevant (and not duplicate)		-140
To assess		**144**

The next step was to download all the documents. The distribution of the documents over the years is shown in Fig. 1, showing a continuous stream of publications over time. While most articles focus on "classical" IT controls, less attention is paid to more recent developments, such as IT controls regarding data, algorithms, AI, IoT, and innovations.

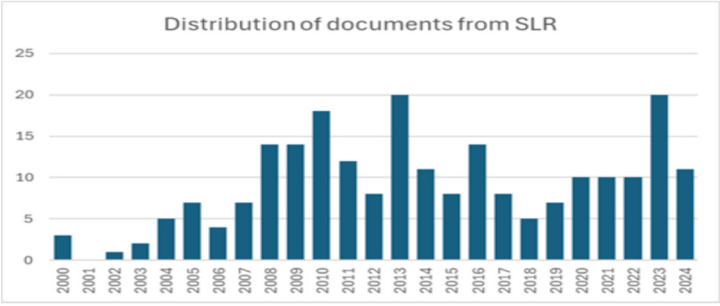

Fig. 1. Distribution of documents on IT controls between 2000 and 2024

Reading these documents, two papers were not academic, and seven were not written in English. We extracted papers that dealt with controls in the public sector by searching all documents for 'public sector', 'ministry' or 'government', resulting in 33 papers: some discussed the public sector as a case study, and some discussed specific controls in the public sector alongside the private sector. Only 5 of these 33 papers mentioned the public sector or government in the title.

Besides the papers, we found three books providing an overview of many controls and explaining the evolution of digitalization controls from IT-cost control to IT-controlling to Smart IT-controlling [3, p. 26]. The book by J. Kyriazoglou, "IT Strategic and Operational Controls", gives an overview of the IT controls [16]. The other two books introduce types of control named in the German-language countries "Controlling": IT-controlling or control Digitalization, Smart IT-Controlling or Digital Controlling. The difference between these types of control is analyzed in the next section. A book by Keimer &

Ulrich [1] was not part of our SLR results since the selected keywords were not part of its title, so it was added to our SLR data given its relevance.Each document was analyzed, and texts about control roles and controlling areas were coded using open coding. Codes were created by searching for 'control' in each document. In some cases, the distinction between control instruments and control roles was unclear; where the distinction was clear, only the control roles were coded. This resulted in more than 200 codes, and after axial coding to identify relations between the codes, 173 merged codes remained.

In the last phase of Snyder [26], *structuring and review,* the classification of the risks to controls was determined. Using control definitions obtained from the SLR, we selected the controls with a mitigating effect for each risk domain. This was verified by an independent expert in IT control in government and is described in the next section.

4 Classification of IT Controls

Our aim is to develop a classification of IT controls that supports government objectives. In our SLR, we found control names based on a variety of underlying classifications: this can be a process-based classification in which change management and system development have a place (e.g. [29]), or a classification related to business objectives, like quality control and regulatory controls (e.g. [30]). A classification based on the goal of control is also prevalent, such as *detective*, *corrective,* and *preventive* [32, 33], which are useful in discussing security controls and stem from internal control literature. Another classification of controls exists that is reminiscent of the organizational components that Mintzberg describes [34], such as *operational controls* and *strategic controls.* Also, a distinction between *technological* and *behavioral controls* in preventing IT incidents can be found [35]. However, all these classifications are not specific to the public sector.

Due to the unique IT risks the government faces, as mentioned in the introduction, this research uses a risk-oriented approach to classify IT controls for the government. Our classification provides insight into which IT controls contribute to mitigating risks in achieving government objectives and responsibilities. This makes our classification unique for the government and can be applied in practice. In the literature, we have not yet encountered comparable or more suitable classifications. Several best practice frameworks have been developed from which IT controls have emerged: COBIT, NORA, ISO 27100, ITIL, BiSL, etc. However, they are not specific to the government, nor are they developed to tackle government-specific risks, and they do not cover all risks, such as those associated with large IT projects. An exception is perhaps COBIT, in which risk management is a central component if its framework. However, COBIT does not take public values into account which are key for governments.

The public sector has a number of specific responsibilities, goals, regulations, and obligations that the private sector does not have, including weighty accountability (towards politics), political objectives that are not fixed, frameworks around the handling of public data, national security, and realizing political agreements to which costs are subordinate [36, p. 12, 37 p. 10]. These specific responsibilities result in specific IT risks and set specific requirements for the necessary IT controls. In addition, governments often encounter a high complexity of IT, resulting from the many developments, highly interconnected IT landscapes, legacy systems, fragmentation of data sources, and

sensitive and personal data. This results in the need to tightly organize IT controls. Based on the typical areas of interest as identified by two European audit offices [9, pp. 16–17, 38], we selected the following risk domains to classify the IT control areas:

1. Non-compliance with laws and regulations: "Failure to comply with regulations, including on workplace safety, safeguard measures on the environment" [9, pp. 16–17];
2. Insufficient integration between IT and policy: "Anything that jeopardizes attainment of departmental objective or service delivery for citizens (i.e., their statutory mandates, etc.") [9, pp. 16–17];
3. Inefficiency and waste of public resources: "Failure to guard against mismanagement, impropriety or waste" [9, pp. 16–17];
4. Insufficient management of IT projects: "An inability to respond to the changed operating environment and hence the risk of missing an opportunity (better known as "decision regret") [9, pp. 16–17];
5. Non-compliance with IT continuity, security, and privacy (cyber-attacks and data leaks, algorithms): "Failure to comply with regulations, including workplace safety, cybersecurity, safeguard measures on the environment, etc.") [9, pp. 16–17];
6. Fragmentation of legacy systems: heterogeneous legacy systems storing data in different ways and formats [39, p. 151];
7. Risks regarding management of government data: poor data quality, and Open government data [40, p. 35].

This classification of IT control areas is presented in Table 3. Each area has a risk classification based on the previous risks, numbered 1 to 7. Table 3 shows whether the public sector needs in each risk area (columns) receive sufficient attention or whether there are still (risk) areas specific for a government that could receive more attention through research into IT control. The IT control areas (rows) in Table 3 are based on a systematic literature study [16]. Overlapping categories have been merged after careful analysis to avoid redundancy. Overarching categories such as 'Management Control' and 'Digital Controlling' have been omitted because they are too broadly defined and do not provide sufficient distinctiveness for our analysis.

The assignment of risk domains to each area of IT control was based on literature, specifically the definitions of the IT controls found in the SLR, and the nature of the risks. This was verified by an independent expert in IT control in government. For example, the risk "Non-compliance with laws and regulations" means that the government must comply with laws and regulations, such as laws about transparency and accountability to society, and adherence to archiving regulations regarding government documents. This involves risks such as loss of government documents and workflow data (e.g., due to poor backup or hardware problems), lacking access management (e.g. becoming public of confidential documents), no audit trail (no proof of who did what), loss of integrity of documents (e.g. due to editing without logging) or insufficient information classification (making sensitive in-formation public). From the control area definitions in the SLR literature, we identified the controls corresponding to these risks regarding "Non-compliance with laws and regulations": Application controls, Data Centre Operational and Support Controls, IT Cloud Control, IT internal controls, IT security controls and IT Strategy controls. This mapping of the controls and risks is explained in Table 3. The

Table 3. Classification of IT-control areas for government digitalization

Areas of IT control from SLR Detailed overview on request	**Definition of control areas**	**Government risk domains**							**Explanation** Numbers refer to relevant risk domains	**References** (IT controls)
		1 Law & Regulation	**2 Integration IT & policy**	**3 Public resources**	**4 IT projects**	**5 Continuity & Security**	**6 Legacy**	**7 Data**		
Application Controls Application systems development process controls, End-user computing controls, IT application change controls, IT application database controls, IT application testing controls.	"IT application controls are those controls that are appropriate for transaction processing by individual computerised subsystems, such as financial accounting, personnel administration, customer sales, inventory control, payroll or accounts payable, etc. and individual computer programs." [16, p. 480]	x				x		x	Applications must comply with laws based on privacy and algorithm risks (1), are subject to hacking (5) and are primarily intended within the government for processing data from the company or for internal business operations (7).	[16] [32] [41] [42] [30] [19] [4] [31]
Data Centre Operational and Support Controls Back-up control, Computer controls and hardware controls, Data control, Hardware maintenance controls, IT contingency planning and disaster recovery controls, Network control and Recovery controls.	"Controls at this level ensure that the IT facilities and equipment can remain in good operational status, and ensure the safe and successful operation of the IT infrastructure and systems for serving the business purposes of the organisation." [16, p. 360]	x				x		x	Continuity of government IT is essential for society (5). Citizens' data must be secure (7) and compliance with laws and regulations is expected (1).	[16] [32] [41] [42] [30] [4] [31] [33]
Enterprise Architecture (EA) Controls EA description controls, EA business related controls, EA development roles.	"Enterprise Architecture controls enable and support the alignment of IT (infrastructure and systems) with the business functions of the organization, and support the successful execution of the daily activities and operational transactions of the IT systems." [16, p. 139]		x				x		An architecture ensures the integration of IT with policy and business objectives (2). In addition, legacy is an important point of attention in the further development of architecture (6).	[16] [43] [44]
IT Cloud Control IT-controls in a Cloud based environment, Financial controls, User controls, Security controls for cloud applications, Encryption controls, Change controls, Performance management controls, Reconciliation controls,	Controls to "manage all potential critical, legal, and compliance-related risks associated with the cloud. ", ensure "compliance with internal as well as external policies, regulations, and accountability mechanisms", "evaluate cloud vendors to ensure deployment of security mechanisms", and "monitoring the vendor against the SLAs, and rating their performance" [45, p. 22]	x				x		x	Placing data in the cloud entails risks of data leaks (7), control over backups and continuity is relinquished (5) and that is why there are laws about what can and cannot be done in the cloud (1).	[3] [7] [46] [47]

(*continued*)

Table 3. (*continued*)

Areas of IT control from SLR Detailed overview on request	**Definition of control areas**	**Government risk domains**							**Explanation** Numbers refer to relevant risk domains	**References** (IT controls)
		1 Law & Regulation	**2 Integration IT & policy**	**3 Public resources**	**4 IT projects**	**5 Continuity & Security**	**6 Legacy**	**7 Data**		
IT Internal Controls Security Internal Controls, IT-control over availability, continuity, and integrity	"Internal controls are ways, checks and balances, to provide assurance that things go as intended where procedures, regulations and laws are followed, transaction are properly documented, fraud, waste and abuse are minimised, unapproved transactions are not processed and desired outcomes are achieved" [48, p. 65]	x		x				x	According to the definition, internal control ensures compliance with laws and regulations, minimizes inefficient use of social resources, and ensures that internal business data is reliable.	[33] [41] [32] [18] [42] [30] [19] [49] [50] [31] [35] [46] [4]
IT Security Controls IT Access controls, Biometric control, Cryptography controls, IT Entry-Level Controls, Login control, Password controls, Segregation of duties control.	"The purpose of IT security controls is to ensure that all IT assets, systems, facilities, data and files are protected against unauthorized access, potential damage and improper or illegal use, and that they are operable, safe and secure at all times." [16, p. 303]	x				x	x	x	The government has laws and regulations (1) to guarantee the continuity of government processes for citizens (5) and to protect data (7). Legacy brings with it many security risks (6)	[16] [33] [32] [42] [49] [4] [35] [41] [31] [41]
System Development Controls Audit controls, Audit trail log file controls, Full control lifecycle, IT project control, Portfolio controlling, Program Development controls, System Controls, System Development Controls, System development quality controls, Systems development personnel controls, Change management control, source code controls.	"System Development Controls establish a good operating environment for the development of IT systems and ensure the successful testing and preparation of these systems for serving the business purposes of the organization. They also facilitate and support the successful execution of the daily activities and operational transactions of the IT systems." [16, p. 246]				x				Ensures a development environment that allows the government to keep pace with political and societal demands, and to ensure projects are implemented effectively (4)	[41] [16] [51] [3] [49] [4] [33] [41] [49] [31]
IT Organization Control IT department functional description controls, IT Governance control, IT process controls, IT vision, mission and values statements, Monitoring and review controls.	"IT organization controls establish the good operating environment for IT (infrastructure and systems) and ensure the successful execution of the daily activities and operational transactions of the IT systems of the organization." [16, p. 25]								These controls provide the foundation and organizational environment for the other controls to function properly. Therefore, they do not directly mitigate risks.	[33] [31]

(*continued*)

Table 3. (*continued*)

Areas of IT control from SLR Detailed overview on request	**Definition of control areas**	**Government risk domains**							**Explanation** Numbers refer to relevant risk domains	**References** (IT controls)
		1 Law & Regulation	**2 Integration IT & policy**	**3 Public resources**	**4 IT projects**	**5 Continuity & Security**	**6 Legacy**	**7 Data**		
IT-Administration Control IT Cost & Budget Control, IT asset controls, IT investment control, IT personnel management controls, IT purchasing controls, control of IT standards, policies and procedures.	"IT administration controls are designed and deployed with the main purpose of facilitating and enabling the proper execution of all the other IT controls." "These are usually concerned with operational efficiency and with adherence to organizational policies and compliance rules and guidelines." [16, p. 84]			x	x				Ensures, among other things, that internal budgets are spent properly (3) and that all resources required by projects are made available (4).	[33] [30] [41] [31] [16] [51] [35]
IT Strategy Control Innovation controlling, IT strategic process controls, IT strategy implementation controls, IT value-based control.	"The purpose of IT strategic controls is to define and establish the future IT vision and mission for the IT efforts (infrastructure and systems) of the organization, and prepare the whole IT environment to accommodate such requirements and needs of the IT systems and IT operations of the organization." [16, p. 194]	x	x						The government strategy must be in line with current legislation and regulations (1) and support and enable new policies (2).	[51] [52]

table shows a classification of IT-control. Given the interpretive but inherent nature of this process, the assignment of risks to control areas should be seen as an illustrative example subject to our interpretation and potential bias as researchers. The assignments depend on many factors, including the specific implementation of the controls and the context of the government organization. Future empirical research is needed to validate this classification.

5 Discussion

What makes the development of the classification challenging is that IT control definitions are different and fragmented across different organizational and system levels (strategic, tactical, or operational). Most of the literature is focused on "classical" IT controls, but not many controls, such as IT controls regarding data, algorithms, AI, IoT, and innovations. In contrast, our classification captures these new control areas.

The existing literature shows different groups underlying the IT controls; some of the controls are outdated (as EDP-controlling [3, p. 12], IP-controlling [3, p. 12]), abstract (Computer control [42] or Strategic control [16, 51]), or too specific (IT Entry-Level controls [49], Time Out control [41]). Our SLR shows that various names for the same IT controls were found, some controls have different interpretations (e.g., Password control/Access control or Resource control/IT asset controls), while some with the same

name have a different scope (e.g., Change management with a security or application scope). Additional empirical research for a more in-depth classification could be useful for some controls, such as Open government data [40, p. 35].

This framework shows that risks associated with the Open Government Act (WOO), Archives Act, Digital Government Act, social services, and public information security and privacy risks (BIO, AVG) make unique demands on controls. IT controls are needed to comply with these acts and regulations. This results in a broadening of the focus of IT control from technical IT aspects to more strategic and complex areas, such as IT-governance, transparency of IT systems and data, and archiving. This aspect is underexposed in existing literature.

In different organizational contexts, each control is expected to be set up somewhat differently [53], with, for example, different choices in the level of responsibilities (operational, tactical, or strategic) or differences in objectives (preventive, corrective, and detective). These differences can lead to variability in mapping the controls to the risks. Further research is needed to account for this variability.

Our results show that there are many controls in the field of digitalization. On the one hand, this is positive and indicates scholarly interest. On the other hand, the controls overlap, their effectiveness is unknown, and they might be too complex for organizations to set up all the controls [50]. Organizations must, therefore, make choices and determine which controls are critical for their processes and are suitable to prevent unnecessary costs. A clear framework for selecting appropriate controls for government organizations is still lacking.

6 Conclusions

This paper seeks to provide an overarching classification of IT control areas for government. Drawing on literature, we developed the first government risk-based classification of controls. The classification consists of ten different areas ranked by their risks. Using this classification, public organizations can better control the various risk areas of IT. By linking controls to a government organization's risk and policy landscape, it is possible to prioritize the risks and mitigating measures. The classification also includes the areas related to compliance gaps within government organizations. Governments can use the classification to determine where IT controls are (still) missing or ineffective and empirically test and improve the effectiveness of the proposed classification. This helps not only with auditing or compliance but also with strategic decision-making about investments in digital infrastructure. This can help improve oversight, audits, investments in public IT environments, and reduce IT failures.

IT control is a broad field, and with the current digitalization developments, new areas included in our classification have emerged. The literature shows different definitions of IT control, depending on the goal of control or the control area. Some literature remains shallow, whereas others describe control in more detail. This study reveals that IT control is an overarching concept consisting of several subareas with different meanings for IT control and IT controlling. Moreover, we identified a wide range of objectives, from control at the organization's strategic level to the technical or operational level of digitalization. However, the control literature has not addressed Zero Trust Architecture

Controls, AI-driven Anomaly detection controls, AI- or algorithm controls, or DevOps Controls. We recommend further research into these control areas. We also recommend to research whether the classification from the literature can be further expanded to include these new developments.

Disclosure of Interests. The authors have no competing interests to declare relevant to this article's content.

References

1. Keimer, I., Egle, U.: The Digitalization of Management Accounting: Use Cases from Theory and Practice. Springer, Germany (2023)
2. Kroker, K.: Die lange Liste schwieriger und gefloppter SAP-Projekte. (2018). https://www.wiwo.de/unternehmen/it/haribo-lidl-deutsche-post-und-co-die-lange-liste-schwieriger-und-gefloppter-sap-projekte/23771296.html
3. Gadatsch, A., Controlling, I.T.: From IT cost and activity allocation to smart controlling. This Springer Vieweg, Germany (2023)
4. Chan, W.H.B., Lao, S.K.: A study of the business value of IT general controls in China. J. Info. Technol. Manage. **20**(4), 22–36 (2009)
5. He, Y., Huang, D., Chen, L., Ni, Y., Ma, X.: A survey on zero trust architecture: challenges and future trends. Wireless Communications and Mobile Computing, pp. 1–13 (2022)
6. Goswami, M.J.: AI-based anomaly detection for real-time. Int. J. Res. Rev. Techniq. **3**(1), 45–53 (2024)
7. Soms, N., Oswalt, M.S., Santhosh, K.P.: A case study on cloud security controls. Int. J. Health Sci. **6**(S1), 11374–11380 (2022)
8. Wiedemann, A., Wiesche, M., Gewald, H., Krcmar, H.: Integrating development and operations teams: A control approach for DevOps. Inf. Organ. **33**, 1–17 (2023)
9. Bhatta, G.: Public sector governance and risks: a proposed methodology to do risk assessments at the program level. Asian Development Bank, Philippine (2008)
10. Beaumaster, S.: Local government IT implementation issues: a challenge for public administration. In: Proceedings of Hawaii International Conference on System Sciences. Hawaii (2002)
11. Rainey, H.G., Backoff, R.W., Levine, C.H.: Comparing public and private organizations. Public Adm. Rev. **36**(2), 233–244 (1976)
12. Boyne, G.: Public and private management: what's the difference?. Journal of Management, 97–122 (2002)
13. Rouwelaar, H.t.: Theoretical Review and Framework: the Roles of Controllers. The Nyenrode Research Group (NRG), 32 (2007)
14. Anthony, R.: Planning and control systems: a framework for analysis (1965)
15. Diemer, H.: Industrial organization and management. LaSelle Extension University, Chicago (1915)
16. Kyriazoglou, J.: IT Strategic and Operational Controls. IT Governance Publishing, United Kingdom (2010)
17. Liu, Q., Ridley, G.: IT Control in the Australian public sector: an international comparison (2005)
18. Hamdan, B.J.: Investigating the Relationship between Governance Mechanisms and the Disclosure of IT Control Weaknesses. In: Thirty Second International Conference on Information Systems. Shanghai (2011)

19. Li, C., Lim, J.-H., Wang, Q.: Internal and external influences on IT control governance. Int. J. Acc. Info. Sys. **8**, 225–239 (2007)
20. Soin, K., Collier, P.: Risk and risk management in management accounting and control. Management Accounting Research (2015)
21. Gadatsch, A., Krupp, A., Wiesehahn, A.: Smart Controlling – Führungsunterstützung im digitalen. Controll Mag **4**, 72–75 (2017)
22. Kamer, T.: Parlementair onderzoek naar ICT-projecten bij de overheid, vergaderjaar 2014–2015, 33, 326, nr. 5. Tweede Kamer, Den Haag (2014)
23. WRR: iOverheid. Amsterdam University Press, Amsterdam (2011)
24. Prins, J., Broeders, D., Griffioen, H.: iGovernment: A new perspective on the future of government. Computer Law & Security Review **28**(3), 273–282 (2012)
25. Lessa, L., Negash, S., Belashew, M.: iGovernment: Working Paper Series ISBN: 978-1-905469-30-7, Institute for Development Policy and Management, SED: Centre for Development Informatics (2012)
26. Snyder, H.: Literature review as a research methodology: an overview and guidelines. J. Bus. Res. **1**(11), 333–339 (2019)
27. Page, M.J., et al.: The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ **372**(71), 1–9 (2021)
28. Falagas, M.E., Pisouni, E.I., Malietzis, G.A., Pappas, G.: Comparison of PubMed, Scopus, Web of Science, and Google Scholar: strengths and weaknesses. The FASEB Journal **22**(2), 338–342 (2007)
29. Berghout, E., Fijneman, R., Hendriks, L., De Boer, M., Butijn, B.-J.: Advanced Digital Auditing. Springer Nature (2023)
30. Limonad, L.: Controls in Business and IT - Formalization and Application. Vancouver (2013)
31. Collet, B.-J.: IT Controls Automation and Database Management: Defending Against the Insider Threat. In: Governance, Risk, and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices, pp. 325–342
32. Tarantino, A.: Governance, Risk, And Compliance Handbook Technology, Finance, Environmental, and International Guidance And Best Practices, In: Tarantino, A.P. (ed.) John Wiley & Sons, Inc., New Jersey (2008)
33. Mintzberg, H.: The five basic parts of the organization. Classics of Organization Theory **4**, 219–230 (1979)
34. Bauer, S.: The Role of Information Security Awareness for Promoting Information Security Policy Compliance in Banks (2016)
35. Budding, G.T., Wassenaar, M.C.: De veranderende rol van de public controller. Boom Bestuurskunde (2018)
36. Campbell, J., McDonald, C., Sethibe, T.: Public and Private Sector IT Governance: Identifying Contextual Differences. Australas. J. Inf. Syst. **16**(2), 5–18 (2010)
37. Dutch Court of Audit: Grip op digitalisering: Rode draden uit tien jaar Rekenkameronderzoek. Dutch Court of Audit, Den Haag (2020)
38. Bludova, T., Usherenko, S., Moskovchuk, A., Kaminska, I., Kyslytsyna, O.: Enterprise Risk Arising from Legacy Production Systems: A Probabilistic Perspective. EUREKA: Physics and Engineering **5**, 150–161 (2022)
39. Kucera, J., Chlapek, D.: Benefits and risks of open government data. J. Syst. Integr. **5**(1), 30–41 (2014)
40. Pathak, J.: Controls, Approach & IT Audit Judgment: A Case (2003)
41. Lee, L., Sawyer, R.: IT General Controls Testing: Assessing the Effectiveness of User Access Management, vol. 14, pp. 15–34 (2019)
42. Arriola, L., Markham, A.: Towards an enterprise architecture controlling framework. In: Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings (2018)

43. Wan, H., Johansson, B., Luo, X., Carlsson, S.: Realization of Enterprise Architecture (EA) Benefits. In: Practice-Driven Research on Enterprise Transformation: 6th Working Conference, PRET. Utrecht, The Netherlands (2013)
44. Khan, S., Nicho, M., Takruri, H.: IT controls in the public cloud: success factors for allocation of roles and responsibilities. J. Info. Technol. Case and Appl. Res. **18**(3), 155–180 (2016)
45. Shafaq, K., Nicho, M., Cooper, G.: A role allocation model for IT controls in a cloud environment. Rev. Bus. Info. Sys. **19**(1) (2015)
46. The Global Fund - Office of the Inspector General, "Audit Report - Cloud Computing at the Global Fund," The Global Fund - Office of the Inspector General. Geneva, Switzerland (2017)
47. Musa, N.: A conceptual framework of IT security governance and internal controls. In: 2018 Cyber Resilience Conference (CRC) (2018)
48. Acevedo, M.R., Ramírez, J.: IT Governance and Internal Controls to Comply with Laws and Regulations (2013)
49. Rezaei, N.: The Evaluation of Implementing IT Governance Controls. J. Appl. Bus. Fin. Res. **2**(3), 82–89 (2013)
50. Gadatsch, A.: IT Controlling – Concepts and Transformation into Practice, vol. 1, pp. 254–262. Springer Science and Business Media LLC (2009)
51. Veith, V., Leimeister, J.M., Krcmar, H.: Towards Value-Based Management of Flexible IT Environments (2007)
52. Chenhall, R.H.: Management control systems design within its organizational context: findings from contingency-based research and directions for the future. Acc. Organ. Soc. **28**, 127–168 (2003)