INTERNET OF THINGS GOVERNANCE FRAMEWORKS: A LITERATURE REVIEW

Timothy H. Speckman [1], Mariana Gerber[2], Dalenca Pottas[2]
[1]Durban University of Technology, Durban, South Africa, 4001
timothyS1@dut.ac.za
[2]Nelson Mandela University, Gqeberha, South Africa, 6001

ABSTRACT
The Internet of Things (IoT) has become a "buzz word", growing into an industry that is predicted to be worth $11 trillion by 2025. IoT devices are equipped with sensors that enable them to collect, transmit and process large volumes of data about their surroundings over the Internet, often without human intervention. Hence, these devices are often referred to as "smart" devices and are reported to bridge the gap between digital and physical worlds. The heterogeneity of the devices in the IoT and the volumes of data involved introduce inherent risk to any network housing such devices. A major concern is that ninety percent of the offerings currently in existence to address IoT related risk are repackaged general-purpose information technology (IT) security technologies, which unfortunately do not adequately address the IoT needs. Moreover, it is reported that the IoT requires new architectures and protocols compared to traditional computer networks, introducing a requirement for new standards, models and frameworks, not currently in existence to address several areas of the IoT. To this end, this article motivates towards the requirement of an IoT governance framework instead of traditional IT governance (ITG) frameworks. The authors of this article intended to explore the state of published literature on IoT governance frameworks. The objective was to establish whether IoT governance frameworks currently exist. Through a systematic literature review, it was established that scholars widely agree on the need for an IoT governance framework, however, one is currently not in existence. Therefore, considerations from the literature were presented as components to be included in an IoT governance framework. Limitations of this study were that technical works were not considered as the study focused on governance and not management.

Keywords: Internet of Things; IoT Governance; IT Governance; Heterogeneous Systems

1. INTRODUCTION
Since its inception, a growing trend has seen heterogeneous 'things' being connected to the Internet, giving birth to the term 'internet of things' or IoT, first used by Kevin Ashton in 1999 (Henriques et al., 2020). Broadly defined, the IoT is an interconnection of people, heterogeneous sensor-fitted devices, and the various protocols that allow these devices to communicate for data collection, transmission and processing over an internet (Yousuf & Mir, 2019). The global reach of IoT in forming people-to-people, people-to-things or things-to-things relationships has allowed digitisation to be extended into the physical world (CompTIA, 2016; Henriques et al., 2020; Talwana & Hua, 2016). Despite the foreseen benefits of the IoT, it is predicted that at least a quarter of all future cybersecurity attacks will be on IoT devices or systems. Thus, if not governed well, these devices and systems present immense risk to organisations, society and individual users (Arias, Wurm, Hoang, & Jin, 2015; Talwana & Hua, 2016). Al-aqrabi and Hill

(2018), Williams and McCauley(2017), Yousuf and Mir (2019), as well as CompTIA (2016), each present that IoT should be governed for several reasons.

First, each IoT sensor introduces a new vulnerability and is a potential point of entry to the entire computer network to which it is connected. Second, there is the rapid adoption of the IoT. The IoT is predicted to have a global economic value of $11 trillion by 2025; therefore, organisations are rapidly adopting it (CompTIA, 2016; Schinagl & Shahim, 2020). Third, IT professionals are ill-equipped to deal with IoT-related risk (CompTIA, 2016). Fourth, predictions estimate that IoT security will account for less than ten percent of the IT budget of most organisations in the future (Culot et al., 2019; Stout & Urias, 2016). Finally, it is reported that no framework of standards currently exists to adequately govern IoT investment and the resultant risk (Almeida et al., 2017; van Niekerk & Rudman, 2019). Considering the aforementioned, it was concluded that there is a lack of published literature on IoT governance mechanisms such as frameworks. Accordingly, this study's most important achievement and contribution are factors that must be incorporated into an IoT governance framework. Subsequent to this article, a conceptual model of the relationship between the factors and the layers of the IoT architecture was developed.

This article discusses a review of published literature on IoT governance frameworks. The remainder of the article will first, in section 2, describe the methodology followed in conducting the literature review. While section 3 is an exploratory section on the IoT governance definitions, perspectives and frameworks, section 4 is a discussion of the advancement of the IoT governance field and suggestions for future research. Finally, the article ends with implications for future research, in the conclusion section.

2. BACKGROUND

Things in the Internet of Things refers to sensor-fitted devices that are able to collect, process and transmit data about their surroundings(Abdul-Ghani & Konstantas, 2019; Ren et al., 2019). Sensor-fitted devices are often referred to as ‘smart’ with smart phones, smart appliances, smart clothes and even smart vehicles collecting, processing and transmitting data. The smart nature of these devices stems from their decision-making, which often requires no human intervention (Bharathi, 2019). IoT services are typically enabled by three components: data, architecture and infrastructure (Leiner et al., 1997), which are discussed in the following paragraphs.

2.1. Data

Bharathi (2019) reports that IoT services are enabled through large volumes of data often collected, processed and transmitted without human intervention. The type of data, the devices collecting the data, the protocols to transmit the data and when the data is collected also varies in the IoT. For example, sensors can transmit data about temperature levels, light intensity, noise levels and traffic conditions among other (Morar et al., 2021, p. 7).

2.2. Architecture

The IoT architecture is reportedly built on layers that are autonomous from each other. This allows services to be implemented at a specific layer, with little influence on other layers. Furthermore, it is between these layers that a lack of standardization in the IoT model exists (Stout & Urias, 2016).
The four commonly described layers of the IoT are:

- The Perception layer: at which data is collected from the physical world through sensors, actuators and smart devices among others;
- The Network Layer: responsible for transmitting information from the Perception Layer; Here, IoT gateways may be found to connect devices without Internet capabilities to the Internet. Typically, security, device addressing, forwarding and routing decisions will also be made at this layer (Morar et al., 2021, p. 7; Yousuf & Mir, 2019).
- The Middle Layer: presents data that can be aggregated from the Network Layer and visualised on a Data Visualisation platform. Examples of platforms at this layer include Blockchain and GIS (Morar et al., 2021).
- The Application Layer: where the mobile application and the Cloud can be found. At this layer, aggregated data about the environment that the sensors and actuators are in, is processed and presented for use. Therefore, it is also known as the layer that consists of interaction methods with users (Li et al., 2016; Morar et al., 2021, p. 7).

2.3. Infrastructure

Infrastructure in the IoT refers to the communication networks, devices and systems for data collection, analysis, storage and security which typically span all four of the architecture layers (Morar et al., 2021, p. 7; van Niekerk & Rudman, 2019). A major challenge highlighted in literature is the requirement for standardisation of IoT architecture; particularly challenging due to the heterogeneity of devices (Li et al., 2016; Morar et al., 2021; Roman et al., 2015; van Niekerk & Rudman, 2019).

As reported earlier, IoT collects and processes large volumes of data for decision making without human intervention, creating information security concerns (Bharathi, 2019). Rightfully so, as it is predicted that in coming years, more than 25% of identified security attacks on organisations will be against IoT devices or systems (Arias et al., 2015; Talwana & Hua, 2016). it is even harder to ignore that through a survey of IT firms, CompTIA discovered that 43 percent of the participants admitted that they were ill-equipped to deal with most areas of the IoT, several even calling IoT a "security disaster waiting to happen" (CompTIA, 2016). Even more concerning is that predictions indicate that in future, IoT security will account for less than ten percent of the information technology (IT) budgets of most organisations (Culot et al., 2019; Stout & Urias, 2016). Aligning the IT investment and budget of an organisation with its business objectives is the goal of IT governance (ITG) (Coertze & Von Solms, 2014).

2.3.1. Information Technology Governance

IT governance is defined as the set of processes, controls and relationships through which an organisation directs and controls its IT investments, to support business strategy through alignment; while managing the resultant risk (Coertze & Von Solms, 2014). As opposed to IT management, which details operational and technical matters, IT governance entails setting the strategic direction for IT (Brotby, 2009). Moreover, IT governance is reported to be a key point in mitigating the risks associated with IT implementation (Henriques et al., 2020; Huygh & De Haes, 2019). Several well-known ITG standards and best practices exist to assist organisations in overseeing their IT investments (Alberts et al., 2005; Asosheh et al., 2013; Delport et al., 2016; ISO/IEC38500, 2008; NIST, 2013). However, regarding IoT, it is reported that 90 percent of the current security offerings are just repackaged general-purpose IT security technologies (Yousuf & Mir, 2019). Moreover, it is reported that the heterogeneous nature of IoT as well as the breadth of "things" requires new types of architectures and protocols compared to traditional networks,

introducing a requirement for a new standards model that addresses several areas of the IoT (Al-Aqrabi & Hill, 2018; CompTIA, 2016; Williams & McCauley, 2017; Yousuf & Mir, 2019). The technical nature of an IoT standards model is but one area of the requirement. A multi-layered approach of technical and non-technical controls across the IoT architecture is required to adequately address the resultant IT risks from the introduction of IoT (Almeida et al., 2017; CompTIA, 2016; Irshad, 2017; Nagamalla & Varanasi, 2017; van Niekerk & Rudman, 2019; Yousuf & Mir, 2019).

2.3.2. Internet of Things Governance

While governance has similar objectives across contexts, the pervasiveness, vulnerabilities and autonomy of IoT devices and systems are the major drivers for an IoT governance specific framework (Sadeghizadeh et al., 2022). Unlike traditional IT systems, which required human intervention, IoT systems often make decisions, even collecting and transferring data autonomously, using capabilities such as sensors in the physical world and artificial intelligence (Ashton, 2010). Devices and sensors are commonly battery-powered, making them unable to run complex security software and exposed to the environment where the data is collected(Skierka, 2018). Thus, while the underlying IT governance mechanisms will also appear in an IoT governance framework, particularly factors such as those discussed in section 3.5.2 must be considered beyond the confines of typical IT governance (Nagamalla & Varanasi, 2017; Salazar et al., 2019; van Niekerk & Rudman, 2019). Several researchers have highlighted that the governance of IoT and the resultant risk requires new standards and governance frameworks and that currently, none exist. To evidently present their concerns, consider some of the statements extracted from the literature below:

> *"Governance frameworks provide a comprehensive and structured approach to governing systems and managing risks. A governance framework can also be used in a heterogeneous technology landscape. A governance framework applied and customised to IoT, however, does not exist"* (van Niekerk & Rudman, 2019).

> *"Christian Christiansen, the program vice president for International Data Corporation's (IDC's) Security Products, believes that 90 per cent of the current IoT security offerings are just repackaged general-purpose security technologies. Such offerings simply miss the point and are ineffective in meeting IoT security challenges"* (Yousuf & Mir, 2019).

> *"Given all these new aspects of the IoT, it will present major issues of governance – policies and practices adequate to control and manage the IoT across a wide variety of contexts. It is one thing to develop appropriate policy and practices to govern the Internet and Web, although this continues to evade most national and international forums, but the IoT will involve a much greater scale of connections. Since the IoT can be used in many contexts to collect data that separately or in combination with other data can generate sensitive personal information, it promises to increase the number and range of issues tied to privacy and data protection, as but one example"* (Dutton, 2014).

To confirm the above statements, a systematic literature review (Fink, 2014; Okoli, 2015; Okoli & Schabram, 2010) was conducted to investigate the state of peer-reviewed, published literature pertaining to information technology governance (ITG) and the internet of things (IoT).

3. METHODOLOGY

Published literature reviews save scholars time, by presenting a single body of work, as opposed to other scholars synthesising a large body of literature. Therefore, the review process should instill confidence in the readers that the body of available literature was covered adequately. Thus, a published literature review should document the review process transparently, including the specifics of the search process (Okoli, 2015; vom Brocke et al., 2009). Conducting a literature review in an explicit, reproducible, systematic approach is known as a systematic literature review (SLR) (Fink, 2014; Okoli, 2015).

Fink (2014), suggests that SLRs serve the purpose of identifying, evaluating and analysing published literature in the field. Concurring with this suggestion, Okoli and Schabram (2010), also report that a methodological approach – explaining the procedures of conducting the review – should be followed to make it reproducible by those who follow the same approach. Furthermore, through a systematic literature review, scholars identify gaps in literature that can be exploitable as research endeavours (Okoli, 2015). As such, Okoli and Schabram (2010), define an eight-step guide for conducting systematic literature reviews (SLRs) in information systems research, as seen in Figure 1.

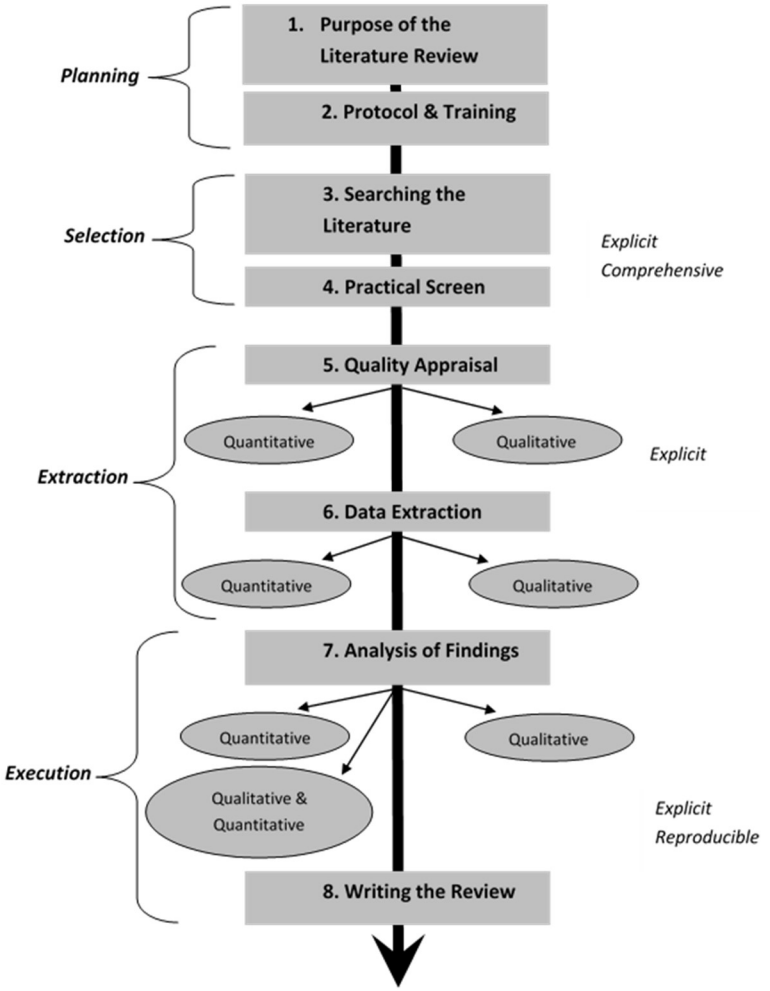

Figure 1. Eight-step systematic literature review process, adapted from Okoli and Schabram (2010).

Each of the eight steps of the process will be discussed in the context of this study, in subsequent sections. The discussion will be arranged according to the four stages of a systematic literature review (Planning, Selection, Extraction and Execution), as proposed by Okoli and Schabram (2010).

3.1. Stage 1: Planning

Stage 1 of the process is the Planning Stage. The Planning Stage intends to define the procedure or protocol to be followed in order to demonstrate consistency (Okoli & Schabram, 2010). This section discusses the purpose and the protocol of this SLR.

3.1.1. Step1: Purpose of the Literature Review

Okoli (2015), proposes that the first step of a literature review is to identify the intended purpose. According to Okoli and Schabram (2010), defining the purpose of a literature review should answer the question, 'Why do a literature review?' and is the first step in the process. This study employed a systematic literature review in an exploratory manner, to discover and identify gaps in literature that are exploitable as possible research endeavours. In simple terms, it can be said that this study was conducted as an exploratory study to determine the status quo of IoT governance frameworks from scholarly works.

3.1.2. Step 2: Protocol and Training

The second step of the process entails defining the protocol and training, where the reviewer formulates research questions to be answered as well as documenting details that will determine whether the review will be broad or narrow. The questions to be answered in this study were: What does published literature report on the existence of IoT governance frameworks? Why are IoT governance frameworks necessary? What are the factors that an IoT governance framework should address? Further on the protocol, Okoli and Schabram (2010), propose that developing a protocol is particularly important where the collected literature is reviewed by more than one reviewer. The protocol should also define the locations to be searched and the screening process for articles to pass in order to be reviewed further.

Ten databases were searched according to convenience of access under the Nelson Mandela University subscriptions. The databases were: EBSCOhost, Emerald, IEE Explore Digital Library, JSTOR, SAGE, SCOPUS, ScienceDirect, Springer Link, Taylor & Francis, and Web of Science. Results were first filtered on the date range, to include only works published from 2011 to 2019, owing to the evolving field of IoT. The results were further filtered to include only articles to which the reviewer had full-text access. The protocol included that all of the articles reviewed were written in English. Finally, in an attempt to obtain results applicable to the IT and computing field, results were filtered according to the field of study. Primarily, these were Computer Science, Information Systems, Information Technology, Internet of Things, Data Privacy and Security of Data. The keyword strings used in the search were Search Term 1: Internet of Things Governance and Information Technology Governance and Search Term 2: Internet of Things AND Information Technology Governance. This step concluded the Planning Stage.

3.2. Stage 2: Selection

Stage 2, the Selection Stage, encompasses conducting the search and excluding articles

according to practical screening criteria (Okoli & Schabram, 2010).

3.2.1. Step 3: Searching the Literature

The third step of the eight-step process begins the Selection Stage. Selection involves searching for the literature that will be included in the study (vom Brocke et al., 2009). To this extent, online databases should be searched using the defined search terms, with the use of Boolean operators (for example, AND, OR). Backward searches should also be conducted from the reference list of included works. Once the reviewer is satisfied that searches no longer yield new results, the searching is concluded (Fink, 2014). After conducting the search, another pertinent consideration is the management of references. Regardless of the systems and tools used, the reviewer should ensure that a 'systematic means is used for recording and storing references and abstracts, annotating them, and even storing and organizing electronic version of articles' (vom Brocke et al., 2009). Using the defined protocol, an initial search of the ten databases was conducted on 22 January 2020. Both search terms yielded the same number of results (75914 articles) across the ten databases. Another query of the databases was conducted using the same protocol on 22 April 2021. Although two more articles were identified, these were eventually excluded in the Practical Screening step. A final query was run in September of 2022, which yielded two articles directly relevant to this study. Retrieved articles were stored in directories named according to the database from which the article was downloaded. The directories were duplicated, with a higher order of directories used to track excluded articles on the stage or criteria for exclusion. These higher order directories were named, Initially Retrieved, Non-applicable Title, Duplicates, Non-applicable Abstract Analysis, and Non-Applicable Full Article Analysis. Furthermore, the full-text analysis was recorded using a Microsoft-Word document.

3.2.2. Step 4: Practical Screening

The fourth step of the process requires that articles for review are identified by means of practical screening criteria (Okoli, 2015). A search will typically result in a large number of articles being found. Therefore, the practical screening step is carried out to decide which articles should be included for further review (not based on quality). Rather, articles are included based on whether the study's content is applicable to the research question and according to the criteria defined in the protocol (Fink, 2014). Here, the reviewer reads no more than the title and abstract of the discovered articles to decide whether they are worth reading further or not (Okoli & Schabram, 2010). Fink (Fink, 2014, pp. 55–56), lists several criteria commonly used to evaluate whether articles warrant further review and limit the scope of the study:

- Content (topics or variables): studies that contribute to answering the research question should be considered.
- Publication language: reviewers are unable to synthesize articles written in a language they do not understand.
- Date of publication: certain date ranges are often used to limit the number of articles returned by a search.
- Setting: studies only in certain settings may either be included or excluded. Settings include healthcare and financial services to name a few examples.

Thus, the screening criteria used in this study were as follows:

- Year of publication: included only results from 2011 to 2019; the number of articles was reduced to 40534. Another search was conducted to include the 2020 and 2021 period.
- Full-text access: only 27571 full-text articles were accessible for review.

- Language: 27514 of the articles written in English (down by 57 articles).
- Field of study: filtering the results on the field of study, only 1021 articles remained.
- Duplicates: ten duplicates were identified, leaving 1111 articles unique articles.
- Title and abstract: the remaining 1111 articles were each screened for applicability to the study based on title and abstract of the article. Articles that included IoT in the title but did not mention IoT or IT governance in the abstract, were not included for further review and only 85 articles remained, concluding the searching stage.

3.3. STAGE 3: EXTRACTION

Stage 3 requires the researchers to review the quality of articles filtered through from the practical screening step. This is also the stage in which articles are reviewed to extract information systematically.

3.3.1. Step 5: Quality Appraisal

The fifth step calls for an appraisal of the quality of articles selected in the practical screening step. Contrary to Okoli's (2015), recommendation that articles should be excluded for insufficient quality, Okoli and Schabram (2010), concede that 'not all literature reviews will eliminate studies based on their quality'. Moreover, relevant studies might be excluded from the review, on condition that the reviewer erroneously assumed the authors of the study had not maintained a level of quality, whereas this might have been an omission by the authors of the study (Kitchenham, 2004). However, it is acknowledged that studies of a nature that is sensitive to the quality of the review studies should be screened for quality, to identify the highest quality studies available (Fink, 2014, p. 49; Okoli, 2015; Okoli & Schabram, 2010). Owing to the exploratory nature of this SLR, no articles were excluded on quality. However, a full-text review of the remaining 85 articles was conducted to establish their applicability to the research question.

Upon a full-text review of these 85 articles, it was found that only 50 of them were directly relevant to the questions posed for the SLR. Okoli and Schabram (2010), recommend using an electronic tool to manage and catalogue articles throughout the SLR process. Again, in the full-text review, a Microsoft-Word document was kept with three categories, namely Relevant, Somewhat Relevant, and Irrelevant. A colour of either green, orange or red was assigned to each article's annotated bibliography in the Microsoft-Word document according to its respective relevance. The majority of articles deemed as Irrelevant were found to be those in fields such as Law, Accounting and Business, where there was no direct or indirect link to IT or ITG. These articles were also moved into a separate folder as opposed to deleting them from the downloaded articles. Somewhat relevant articles were also moved into a separate folder but contained aspects such as references that could be further explored. In this category, the majority of articles alluded to e-government and the development of smart cities, among others. This concluded the quality appraisal step of the SLR.

3.3.2. Step 6: Data Extraction

In the sixth step, once reviewers have concluded which articles are to be reviewed further, data should be extracted systematically from each article as raw material for the synthesis step (Okoli & Schabram, 2010). The type of data to be extracted is determined by the research question defined in the protocol and training stage (Okoli, 2015). In addition to the information to answer

the research question, a data extraction form should provide standard information (Kitchenham, 2004; Okoli, 2015). Kitchenham (2004), suggests that a data extraction form should provide space for the following standard information:

- Name of reviewer
- Date of data extraction
- Title, authors, publication details
- Space for additional notes

3.4. Stage 4: Execution Stage

After data has been extracted from the review articles, the reviewer should combine the data to make comprehensive sense of a large number of studies. The fourth stage of the SLR entails analysing the findings and writing the review (Okoli & Schabram, 2010).

3.4.1. Step 7: Analysis of Findings

Step seven, the analysis step, also referred to as the data synthesis step, involves collating and summarising the results of the reviewed studies (Kitchenham, 2004). This step produces an aggregated and organised discussion comparing the included studies (Okoli & Schabram, 2010), which according to Fink (2014, p. 188), is the final outcome of a research review. More so, 'the synthesis is used in describing the status of current knowledge about a topic, describing the quality of available research and the need or significance of new research'(Fink, 2014, p. 188). Okoli and Schabram (2010) refer to the synthesis either being qualitative or quantitative, depending on the data being analysed. Fittingly, a qualitative synthesis approach was adopted in the synthesis of articles in this study.

3.5. Step 8: Writing the Review

Okoli and Schabram (Okoli & Schabram, 2010), define writing the review as the final step of an SLR, in which the researcher(s) reports the findings of the study. Primarily important in this step of the SLR process, is the explicitness of the process making the study reproducible. Additionally, any novel findings should be highlighted in this step. Braun and Clarke (2006), define this phase as 'Producing the report'. According to these authors, this is the phase for presenting the final analysis with the selection of 'vivid, compelling extract examples' relating back to the research questions. Thus, the layout of the discussion was structured in a manner that addresses the research questions presented in Step 1.

3.5.1. Why are IoT governance frameworks necessary?

While it is widely agreed that an IoT governance framework is necessary (Henriques et al., 2020; Sedrati et al., 2022) there is belief that IoT is simply an extension of the Internet and should be regulated in a similar fashion (Weber, 2013). It has also emerged that there is currently an absence of IoT governance frameworks: "a governance framework applied and customised to IoT, however, does not exist" (van Niekerk & Rudman, 2019).

The answer to whether an IoT governance framework is necessary can be found in the rationale of a governance framework. A governance framework presents a systematic strategy to minimise risks and ensure a consistent and stable outcome (Morar et al., 2021; Webb & Hume, 2018).

Furthermore, several authors propose that the greatest challenge of the IoT is establishing how to govern a network of so many heterogeneous devices (Weber, 2013; Nagamalla & Varanasi, 2017; Deloitte, 2021, p.5). The IoT ecosystem is by nature, agile and therefore requires an agile and adaptive governance methodology (Morar et al., 2021).

3.5.2. What are the factors that an IoT governance framework should address?

A total of 13 factors that an IoT governance framework should address, were derived from literature (Almeida et al., 2015; Bharathi, 2019; Dutton, 2014; Hudson, 2018; Kautsarina & Anggorojati, 2018; Morar et al., 2021; Weber, 2015; Weber & Studer, 2016). These factors span the components of IoT as defined in Section 2 (architecture, infrastructure and data) and are not confined to the four layer architectural model.

- Trust – only designated people, services or systems should have access to devices or data. A mechanism to ensure that devices, systems and people can trust one another and the decisions made is necessary.
- Privacy – IoT sensors have become pervasively integrated into devices, increasing concerns of surveillance and privacy contravention.
- Data governance – IoT services are enabled through large volumes of data. The lifecycle of the data should be governed including data collection, distribution, analysis and ownership.
- Information security – the critical characteristics of the information should be protected across all levels of the architecture.
- Enterprise architecture (EA) governance – IoT systems are often connected to existing enterprise technology architecture. The flow of information, purpose, functioning and ownership of the architecture and associated risks should be governed.
- Heterogeneous systems – IoT systems include many devices and subsystems of various types in terms of functioning, capacity, decision making, data collection, and analysis, as well as related risks. This should form part of the governance strategy and must include a strategy for device management.
- Accountability – as systems in the IoT are composed of sensors from various vendors, connect into heterogeneous systems and collect and transmit data; measures for ensuring accountability should be part of an IoT governance framework. These include consideration of *n-th* party risk, vulnerability component patching, etc.
- Transparency – in alignment with data privacy and protection laws, users should be aware of data collected, the purpose of collection, its use, transmission and retention. In addition, consent should be sought before any data is collected and any breaches should be reported.
- Interoperability – an IoT governance framework should also be cognisant of the heterogeneous systems, as well as the EA, to ensure interoperability.
- Risk – similar to EA governance, information security and the management of heterogeneous systems, the risks introduced by every ‘smart’ device connected to the corporate network should be considered in a risk versus benefit analysis.
- Standardisation - systematic and standardised safeguards should be introduced to manage risks, not only at an organisational level, but as part of IoT device manufacturing.
- Agile and adaptive – as IoT is an evolving technology, an IoT governance framework should be agile, with continual review and adaptive with a degree of modularity.
- Regulation – relevant laws, rules, policies, regulations and best practice and standards consideration should be evident in an IoT governance framework.

In addition to the 13 factors above, traditional corporate governance of ICT factors such as (ISO/IEC38500, 2008) and COBIT-19 should feature in an IoT governance framework.

3.5.3. What does published literature report on the existence of IoT governance frameworks?

As reported in Section 2, published literature until 2019 reported that no IoT governance frameworks were in existence. At that period, several entities had congregated to attempt to define standards that address IoT governance, however no IoT governance frameworks had been defined (CompTIA, 2016; Dutton, 2014; van Niekerk & Rudman, 2019). Although several works were identified and reviewed, the three below were selected as the most relevant to the problem at hand.

Technologies, Applications and Governance in the Internet of Things

In this article, Zheng, Zhang, Han, Zhou, H, Zhang, Gu and Wang (2022)present a two-view IoT model. Furthermore, they discuss the IoT governance challenges according to a three-layer IoT reference architecture. Moreover, challenges IoT architecture, network, discovery, search engines, security and privacy and applications are presented. Standards synonymous with IoT operations are also listed. Under governance, the features of an IoT ecosystem are presented. Finally, recommendations to address the listed challenges are proposed.

The article presented ideas which incorporated the factors listed in Section 3.5.2 besides transparency, data governance and risk management (further than mitigation through security controls). Moreover, the ideas of the authors were not presented as a framework that will align the IoT investment with the strategic objectives of organisations.

IoT-Gov: An IoT governance framework using the blockchain

Sedrati, Ouaddah and Bellaj (2022), identify IoT governance requirements and subsequently design a framework to fulfill these requirements. IoT-Gov is the designed framework and addresses challenges listed as data governance, device management, privacy and security as well as legal challenges. The categories of identified governance requirements are thus listed as:

- IoT governance grounds: roles, responsibilities, rules, policies, processes, legitimacy and representation, transparency and accountability
- IoT reference architecture: based on layers – application, platform, communication and physical devices
- IoT device management: assessing device decision-making ability, as well as lifecycle management
- Data governance: governing the full data lifecycle including collection, analysis, distribution and security and privacy
- Security and privacy: across all layers of the architecture, protection is required against vulnerabilities and potential attacks.

Four levels or layers define the IoT-Gov framework and are listed with the objective of each:

- Strategic objective layer – determining the requirements and functionalities to create the intended solution, including whether devices shall make decisions autonomously. Needs related to data collection, analysis and privacy and security are inputs to this layer.
- Design and modelling layer – where the governance models to be applied as well as roles and responsibilities are defined. No governance models are specified, however the authors define governance models are the design of policies, practices and roles, which are applied to achieve an outcome.

- Implementation layer – technologies are deployed to enforce the decisions and policies from the Design and modelling layer.

In this framework, the system manager sets the governance policies. Thereafter, things and users are to request access and be authorised by authorisation hubs. This would be a challenge in a consumer-IoT system. Furthermore, as the authors have not included any traditional governance structures, the framework does not lend itself to corporate IoT governance. Having made the above observations, it was concluded that the IoT-Gov framework is an IoT access governance framework, rather than an IoT governance framework.

High-level IoT Governance Model Proposal for Digitised Ecosystems

In this study, Salazar, Hervas, Estevez and Marrone (2019) propose an IoT governance model which outlines the structures of IoT governance. The view of these authors is that IoT governance can be complex because of the integration of IoT with IT services, while aligning it with business requirements. Therefore, the proposed model was designed to address:

- IoT governance processes and policies according to business and economic objectives
- Establish technical strategy to over system complexity
- Select a reference IoT architecture
- Develop skills needed to design and implement the solution and
- Use checkpoints to verify and improve the correct flow of the project.

In the Technical Strategy category, the model defines four phases for the design and implementation of IoT systems.

- Preparation phase: business objectives and service delivery approach are defined. Risk assessment and a work team for the current situation are developed.
- Design phase: the solution is defined and the prototype and proof-of-concept are taken into account.
- Development phase: refining of the architecture, integration of different technology platforms and a general evaluation of the system is done.
- Deployment phase: there is an integration of data and a deployment of a management solution to obtain measurement metrics.
- Operation phase: this phase is primarily about maintenance, automation and monitoring of the solution to measure goals, improve the solution and define scalability.

The model refers to standards such as the Internet of Things – Architecture (IoT-A), IEEE P2413 and Industrial Internet Reference Architecture (IIRA) for a standardised IoT reference architecture. This model forms a good base for IoT governance, however, data governance – an integral part of IoT governance – is not explicitly incorporated. Furthermore, there appears to be little emphasis on privacy in this IoT governance model. Evaluating each of the proposed solutions, as discussed above, using the factors as discussed in Section 3.5.2 the findings are presented in Table 1.

Table 3: Evaluation of Papers using Factors

Factors	Paper 1	Paper 2	Paper 3
Heterogeneous systems	×	×	×
Trust	×	×	×
Privacy	×	×	×
EA governance	×		×

Data governance		×	
Information security	×	×	×
Accountability	×	×	×
Transparency		×	×
Interoperability	×	×	×
Risk management			
Standardisation	×	×	×
Agile and adaptive	×		×
Regulation	×	×	×

In Table 1, the articles were referred to using an alias that represents the order in which each article appeared in Section 3.5.3. Data governance and risk management appeared to be the least addressed factors. While these authors made well merited contributions to IoT governance, a comprehensive IoT governance framework is still required.

4. Summary of Findings

This study set out to establish the status quo of IoT governance. Three questions were answered through this study. Firstly, it was established that due to the nature of the IoT, typical IT governance frameworks will not suffice for IoT governance. Secondly, it was discovered that there is a need for an IoT governance framework to manage risks and align IoT investment with business requirements. Third and finally, several IoT governance considerations from literature were presented. However, it was acknowledged that the list is not comprehensive as the IoT is agile and is continuously evolving – another consideration for an IoT governance framework.

5. Conclusion

This article discussed the findings of a systematic literature review conducted to establish the status quo of IoT governance frameworks from literature. The findings of the SLR were that there appears to be a lack of governance frameworks and regulations for the IoT. It was not only brought to light that there is a lack of IoT governance frameworks, but also that there is a lack of IoT security frameworks, IoT privacy frameworks and regulations, and IoT risk assessment frameworks and models. It is reported that IoT solutions need to take into account the dynamic nature of IoT, the heterogeneity of connected devices, cyber-physical systems, lack of processing power, IoT as an attack platform, and the vast amount of data processed without human intervention. These have all been identified as avenues of exploration for future work in the IoT governance.

6. References

Abdul-Ghani, H. A., & Konstantas, D. (2019). A comprehensive study of security and privacy guidelines, threats, and countermeasures: An IoT perspective. *Journal of Sensor and Actuator Networks*, *8*(2). https://doi.org/10.3390/jsan8020022

Al-Aqrabi, H., & Hill, R. (2018). A secure connectivity model for internet of things analytics service delivery. *Proceedings - 2018 IEEE SmartWorld, Ubiquitous Intelligence and Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People and Smart City Innovations, SmartWorld/UIC/ATC/ScalCom/CBDCo*, 9–16. https://doi.org/10.1109/SmartWorld.2018.00038

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2005). *OCTAVE-S Implementation Guide* (Vol.

1, Issue V 1.0).
Almeida, V. A. F., Doneda, D., & Monteiro, M. (2015). Governance challenges for the internet of things. *IEEE Internet Computing*, *19*(4), 56–59. https://doi.org/10.1109/MIC.2015.86
Almeida, V. A. F., Goh, B., & Doneda, D. (2017). A principles-based approach to govern the IoT ecosystem. *IEEE Internet Computing*, *21*(4), 78–81. https://doi.org/10.1109/MIC.2017.2911433
Arias, O., Wurm, J., Hoang, K., & Jin, Y. (2015). Privacy and Security in Internet of Things and Wearable Devices. *IEEE Transactions on Multi-Scale Computing Systems*, *1*(2), 99–109. https://doi.org/10.1109/TMSCS.2015.2498605
Ashton, K. (2010). That ' Internet of Things ' Thing. *RFiD Journal*, 4986. http://www.itrco.jp/libraries/RFIDjournal-That Internet of Things Thing.pdf
Asosheh, A., Hajinazari, P., & Khodkari, H. (2013). A practical implementation of ISMS. *International Journal of Information Science and Management*, *11*(SPL.ISS.), 111–126. https://doi.org/10.1109/ECDC.2013.6556730
Bharathi, S. V. (2019). Forewarned is forearmed: Assessment of IoT information security risks using analytic hierarchy process. *Benchmarking*, *26*(8), 2443–2467. https://doi.org/10.1108/BIJ-08-2018-0264
Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. http://www.tandfonline.com/action/journalInformation?journalCode=uqrp20%5Cnhttp://www.tandfonline.com/action/journalInformation?journalCode=uqrp20
Brotby, K. (2009). *Information Security Governance: A Practical Development and Implementation Approach* (Vol. 53). John Wiley & Sons, Inc. https://doi.org/10.1002/9780470476017
Coertze, J., & Von Solms, R. (2014). The murky waters of IT governance. *2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference*. https://doi.org/10.1109/ISSA.2014.6950498
CompTIA. (2016). *Internet of Things Insights and Opportunities* (Issue July). https://www.comptia.org/resources/internet-of-things-insights-and-opportunities?c=50079 [Accessed 1 Sep. 2016]
Culot, G., Fattori, F., Podrecca, M., & Sartor, M. (2019). Addressing Industry 4.0 Cybersecurity Challenges. *IEEE Engineering Management Review*, *47*(3), 79–86. https://doi.org/10.1109/EMR.2019.2927559
Delport, P. M. J., Von Solms, R., & Gerber, M. (2016). Towards corporate governance of ICT in local government. *2016 IST-Africa Conference, IST-Africa 2016*, *152*(1), 1–11. https://doi.org/10.1109/ISTAFRICA.2016.7530582
Dutton, W. H. (2014). Putting things to work: Social and policy challenges for the Internet of things. *Info*, *16*(3), 1–21. https://doi.org/10.1108/info-09-2013-0047
Fink, A. (2014). Conducting Research Literature Reviews: From the Internet to Paper. In V. Knight, K. Kosielak, J. Miller, S. Palermini, L. Pitman, & K. Ehrmann (Eds.), *New Horizons in Adult Education and Human Resource Development* (4th ed., Vol. 20, Issue 4). SAGE. https://doi.org/10.1002/nha3.10270
Henriques, D., Pereira, R. F., Almeida, R., & Mira da Silva, M. (2020). IT governance enablers in relation to IoT implementation: a systematic literature review. *Digital Policy, Regulation and Governance*, *22*(1), 32–49. https://doi.org/10.1108/DPRG-02-2019-0013
Hudson, F. D. (2018). Enabling Trust and Security: TIPPSS for IoT. *IT Professional*, *20*(2), 15–18. https://doi.org/10.1109/MITP.2018.021921646

Huygh, T., & De Haes, S. (2019). Investigating IT Governance through the Viable System Model. *Information Systems Management*, *36*(2), 168–192. https://doi.org/10.1080/10580530.2019.1589672

Irshad, M. (2017). A systematic review of information security frameworks in the internet of things (IoT). *Proceedings - 18th IEEE International Conference on High Performance Computing and Communications, 14th IEEE International Conference on Smart City and 2nd IEEE International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2016*, 1270–1275. https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0180

ISO/IEC38500. (2008). *ISO/IEC 38500 : Corporate governance of information technology*.

Kautsarina, & Anggorojati, B. (2018). A Conceptual Model for Promoting Positive Security Behavior in Internet of Things Era. *6th Global Wireless Summit, GWS 2018*, 358–363. https://doi.org/10.1109/GWS.2018.8686701

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews. In *Keele University Technical Report TR/SE-0401*. https://doi.org/10.1145/3328905.3332505

Leiner, B., Cerf, V., Cark, D., Kahn, R., Kleinrock, L., Lynch, D., Postel, J., Roberts, L., & Stephen, W. (1997). The Past and Future History of the Internet. *Communications of the ACM*, *40*(2), 102–108. https://doi.org/10.1088/0004-637X/698/1/666

Li, S., Tryfonas, T., & Li, H. (2016). The Internet of Things: a security point of view. *Internet Research*, *26*(2), 337–359. https://doi.org/10.1108/IntR-07-2014-0173

Morar, B., Barkawie, Y., Balakrishnan, R., Khasawneh, M., Bangara, J., & Baker, H. A. (2021). *IoT Governance Governance framework*. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/xe/Documents/technology/me_IoT-Governance.pdf

Nagamalla, V., & Varanasi, A. (2017). A review of security frameworks for Internet of Things. *2017 International Conference on Information Communication and Embedded Systems, ICICES 2017*, *Icices*. https://doi.org/10.1109/ICICES.2017.8070757

NIST. (2013). *SP800-53: Security and Privacy Controls for Federal Information Systems and Organizations*. https://doi.org/http://dx.doi.org/10.6028/NIST.SP.800-53r4

Okoli, C. (2015). A guide to conducting a standalone systematic literature review. *Communications of the Association for Information Systems*, *37*(1), 879–910. https://doi.org/10.17705/1cais.03743

Okoli, C., & Schabram, K. (2010). (Okoli, Schabram 2010 Sprouts) systematic literature reviews in IS research. *Working Papers on Information Systems*, *10*(26), 10–26. http://sprouts.aisnet.org/10-26

Ren, J., Mandalari, A. M., Dubois, D. J., Kolcun, R., Choffnes, D., & Haddadi, H. (2019). Information exposure from consumer IoT devices: A multidimensional, network-informed measurement approach. *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, 267–279. https://doi.org/10.1145/3355369.3355577

Roman, R., Najera, P., & Lopez, J. (2015). Securing the Internet of Things. *Computer*, *September*, 42–53. https://doi.org/10.1002/9781118680605.ch3

Sadeghizadeh, H., Markazi, A. H. D., & Shavvalpour, S. (2022). Investigating the Relationship between Governance and Key Processes of the Iran IoT Innovation System. *Sensors*, *22*(2), 1–19. https://doi.org/10.3390/s22020652

Salazar, G. D., Hervas, C., Estevez, E., & Marrone, L. (2019). High-level IoT governance model proposal for digitized ecosystems. *Proceedings - 2019 International Conference on Information Systems and Software Technologies, ICI2ST 2019*, 79–84. https://doi.org/10.1109/ICI2ST.2019.00018

Schinagl, S., & Shahim, A. (2020). What do we know about information security governance?: "From the basement to the boardroom": towards digital security governance. *Information and Computer Security*, *28*(2), 261–292. https://doi.org/10.1108/ICS-02-2019-0033

Sedrati, A., Ouaddah, A., Mezrioui, A., & Bellaj, B. (2022). IoT-Gov: an IoT governance framework using the blockchain. *Computing*, *104*(10), 2307–2345. https://doi.org/10.1007/s00607-022-01086-1

Skierka, I. M. (2018). The governance of safety and security risks in connected healthcare. *IET Conference Publications*, *2018*(CP740), 1–12. https://doi.org/10.1049/cp.2018.0002

Stout, W. M. S., & Urias, V. E. (2016). Challenges to securing the Internet of Things. *Proceedings - International Carnahan Conference on Security Technology*, *0*. https://doi.org/10.1109/CCST.2016.7815675

Talwana, J. C., & Hua, H. J. (2016). Smart World of Internet of Things (IoT) and Its Security Concerns. *Proceedings - 2016 IEEE International Conference on Internet of Things; IEEE Green Computing and Communications; IEEE Cyber, Physical, and Social Computing; IEEE Smart Data, IThings-GreenCom-CPSCom-Smart Data 2016*, 240–245. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.64

van Niekerk, A., & Rudman, R. (2019). Risks, controls and governance associated with internet of things technologies on accounting information. *Southern African Journal of Accountability and Auditing Research-Sajaar*, *21*, 15–30.

vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., & Cleven, A. (2009). RECONSTRUCTING THE GIANT: ON THE IMPORTANCE OF RIGOUR IN DOCUMENTING THE LITERATURE SEARCH PROCESS. *European Conference on Information Systems (ECIS)*, *17*, 2206–2217. https://doi.org/10.1007/BF01938871

Webb, J., & Hume, D. (2018). Campus IoT collaboration and governance using the NIST cybersecurity framework. *IET Conference Publications*, *2018*(CP740), 1–7. https://doi.org/10.1049/cp.2018.0025

Weber, R. H. (2013). Internet of things - Governance quo vadis? *Computer Law and Security Review*, *29*(4), 341–347. https://doi.org/10.1016/j.clsr.2013.05.010

Weber, R. H. (2015). Internet of things: Privacy issues revisited. *Computer Law and Security Review*, *31*(5), 618–627. https://doi.org/10.1016/j.clsr.2015.07.002

Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. *Computer Law and Security Review*, *32*(5), 715–728. https://doi.org/10.1016/j.clsr.2016.07.002

Williams, P. A. H., & McCauley, V. (2017). Always connected: The security challenges of the healthcare Internet of Things. *2016 IEEE 3rd World Forum on Internet of Things, WF-IoT 2016*, 30–35. https://doi.org/10.1109/WF-IoT.2016.7845455

Yousuf, O., & Mir, R. N. (2019). A survey on the Internet of Things security: State-of-art, architecture, issues and countermeasures. *Information and Computer Security*, *27*(2), 292–323. https://doi.org/10.1108/ICS-07-2018-0084

Zheng, L., Zhang, H., Han, W., Zhou, X., He, J., Zhang, Z., Gu, Y., & Wang, J. (2022). Technologies, Applications, and Governance in the Internet of Things. *Internet of Things - Global Technological and Societal Trends from Smart Environments and Spaces to Green Ict*, 143–177. https://doi.org/10.1201/9781003338604-7