Article

Not peer-reviewed version

Local Government Cybersecurity Analysis: From Policy Review to Policy Framework Formulation

Sk Tahsin Hossain , Tan Yigitcanlar * , Kien Nguyen , Yue Xu

Posted Date: 10 May 2024

doi: 10.20944/preprints202405.0641.v1

Keywords: cybersecurity; cyber-attacks; cybersecurity policy; local government; local council; municipality; smart city

Article

Local Government Cybersecurity Analysis: From Policy Review to Policy Framework Formulation

Sk Tahsin Hossain [1], Tan Yigitcanlar [1,*], Kien Nguyen [2] and Yue Xu [3]

[1] City 4.0 Lab, School of Architecture and Built Environment, Queensland University of Technology, 2 George Street, Brisbane, QLD 4000, Australia; tahsin.hossain@qut.edu.au; tan.yigitcanlar@qut.edu.au

[2] School of Electrical Engineering and Robotics, Queensland University of Technology, 2 George Street, Brisbane, QLD 4000, Australia; k.nguyenthanh@qut.edu.au

[3] School of Computer Science, Queensland University of Technology, 2 George Street, Brisbane, QLD 4000, Australia; yue.xu@qut.edu.au

* Correspondence: tan.yigitcanlar@qut.edu.au; Tel.: +61-7-3138.2418

Abstract: Cybersecurity is a crucial concern for local governments, as they serve as the primary interface between public and government services, managing sensitive data and critical infrastructure. While technical safeguards are integral to cybersecurity, the role of well-structured policy is equally important, as it provides structured guidance to translate technical requirements into actionable protocols. This study reviews local governments' cybersecurity policies to provide a comprehensive assessment of how these policies align with NIST CSF, which is a widely adopted and commonly used cybersecurity assessment framework. The review offers local governments a mirror to reflect on their cybersecurity stance, identifying potential vulnerabilities and areas needing urgent attention. The study further extends to developing a cybersecurity policy framework, which local governments can use as a strategic tool. It provides valuable information on crucial cybersecurity elements that local governments must incorporate into their policies to protect confidential data and critical infrastructure.

Keywords: cybersecurity; cyber-attacks; cybersecurity policy; local government; local council; municipality; smart city

1. Introduction and Background

The smart city movement, which significantly enhances urban digital capabilities, also increases our cities' vulnerability to cybersecurity threats (D'Amico et al., 2020; Repette et al., 2021; Micozzi & Yigitcanlar, 2022; Son et al., 2023). In the age of smart cities and digital transformation, local governments (LGs) face increasing cybersecurity threats due to storing and managing a vast amount of sensitive information, including residents' data and critical infrastructure details (Ahmadi-Assalemi et al., 2020; Toh, 2020; Frandell & Feeney, 2022). The frequency and severity of cyber-attacks on LGs have increased in recent years (Chaudhuri & Bozkus Kahyaoglu, 2023). A nation-wide survey in the USA by Norris et al. (2019) revealed that 27.7% of their LGs are victims of hourly or more frequent cyber-attacks, while 19.4% are targeted at least once daily.

Another study by Norris & Mateczun (2022) encompassing three counties and 11 cities in the USA showed that LGs of these regions experienced cyber-attacks on a 'constant' or 'near-constant' basis. Specifically, 57.1% of the surveyed LGs reported constant targeting, while 28.6% reported hourly targeting. Moreover, many LGs across the world are embracing smart city initiatives and increasing the use of Internet-of-Things (IoT) devices, which further escalates their threat landscape to cyber-attacks (Ma, 2021). Insufficient cybersecurity measures in LGs can lead to significant consequences, including the exposure of sensitive information, potential reputational damage, high costs for fixing security breaches, and impaired capacity to effectively address routine and emergency service needs (Tariq et al., 2021; Sharma & Mukhopadhyay, 2022).

The cybersecurity of LGs primarily emphasises technical safeguards such as firewalls, encryption, and anti-malware tools (Sarker et al., 2021). While technical defences are critical to shielding digital infrastructure from cyber-attacks, having policies is equally important (Savaş & Karataş, 2022; Siudak, 2022). Cybersecurity policies offer a set of guidelines for employees and contractors and enhance the effectiveness of technical measures (Caruson et al., 2012; Hatcher et al., 2020; AlDaajeh et al., 2022). However, many LGs across the world do not have cybersecurity policies, which is a significant concern due to the increasing rate and ever-evolving nature of cyber-attacks (Hatcher et al., 2020; Frandell & Feeney, 2022; Preis & Susskind, 2022).

An earlier contribution in this field by Caruson et al. (2012) found that only 48% of the LGs had formal cybersecurity policies or standards in Florida's 67 counties. During a focus group discussion in 2018, IT professionals from the LGs in Maryland identified the lack of policy and its implementation as one of the principal challenges, along with insufficient funding and staffing for effective cybersecurity measures (Norris et al., 2018). In another study, Norris et al. (2019) found that 60% of the LGs in the USA lack cybersecurity policies. The Office of the Auditor General in Western Australia conducted a study on the cybersecurity issues of 15 LGs in that region and found only three with updated cybersecurity policies, nine with outdated or inadequate policies, and the rest without policies (Morrissey et al., 2021).

There is a noticeable lack of academic research on cybersecurity policies. Several studies have identified the lack of cybersecurity policies in LGs as a significant problem in protecting their digital assets and critical infrastructure (Caruson et al., 2012; MacManus et al., 2013; Norris et al., 2018; Chaudhary et al., 2023). However, Hatcher et al. (2020) authored the only article that explicitly investigated both cybersecurity policies and practices.

Hatcher et al. (2020) approached 2,436 LGs in the USA through an online survey but received only 7% responses. The survey aimed to examine the presence of cybersecurity policies in LGs, the use of internet-based technologies, the level of support received for cybersecurity planning, the specific types of cybersecurity policies implemented, and the resources needed for planning. Surprisingly, they found more than two-thirds of LGs with formal cybersecurity policies, but they identified multiple flaws in their practices. These include failure to document and take lessons from previous cyber-attacks, the lack of sufficient training and the absence of reviewing and updating training procedures, the absence of engaging experts in reviewing cybersecurity policies and practices, inadequate protection mechanisms for data, and the absence of appropriate protocols for accessing sensitive information.

Based on the gaps in practices, Hatcher et al. (2020) primarily emphasised putting more efforts into securing data, reviewing policies and practice strategies by external auditors and professionals, and allocating an adequate budget to effectively implement cybersecurity policies. They also cited respondents regarding the components of municipal cybersecurity policies, highlighting the necessity for additional research and the creation of a structured policy framework to assist LGs in crafting effective cybersecurity practices. However, a review and evaluation of the LGs' cybersecurity policies are critical prior to formulating a guiding policy framework, as it will help understand gaps in existing policy statements and contents. This is still a grey area in the academic field.

With this backdrop in mind, we designed this study, aiming to develop a cybersecurity policy framework using insights from LGs' evaluation of existing cybersecurity policy documents in different countries. For the empirical analysis, we used 38 cybersecurity policy documents of LGs in five different countries and evaluated them against the six Functions and underlying 22 Categories of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) 2.0.

The NIST CSF is a cybersecurity assessment framework designed to assess the cybersecurity posture of organisations against predefined criteria, providing a systematic methodology to identify strengths, weaknesses, and areas for improvement in controls, practices, and processes. A cybersecurity policy framework, on the other hand, can offer structured guidelines for LGs on what to include in cybersecurity policies. Cybersecurity policies do not typically include technical measures, but they outline the principles of cybersecurity governance and offer a structured approach to security measures for preventing and responding to cyber-attacks. Considering the importance of cybersecurity policies for any organisation, including LGs, and the absence of a cybersecurity policy framework, we designed this study. To achieve the aim of this study, we address the following research questions:

1. How effectively do the cybersecurity policy documents of LGs align with the Functions and Categories of the NIST CSF 2.0?
2. What are the key components that should be included in a cybersecurity policy document by LGs to ensure its effectiveness and comprehensiveness?

We conducted a qualitative and quantitative content analysis of the policy documents and stock-take insights to develop the policy framework, intending to inform cybersecurity policymakers, LG officials, and researchers in the field about the content and gaps in the existing policy documents, as well as the essential components required to be considered in cybersecurity policy for an effective security measure. Section 2 of this paper, following this introduction section, outlines the NIST CSF 2.0. Section 3 presents the methodology; Section 4 includes the results of the analysis, followed by the discussion and conclusion of this study in Section 5 and 6, respectively.

2. The NIST CSF 2.0

In February 2024, the NIST of the Department of Commerce in the USA released CSF 2.0, an updated version of CSF 1.1 from April 2018 (NIST, 2024a). The framework is a widely recognised assessment tool for all types of organisations' cybersecurity to strengthen their digital defences (Wolff & Lehr, 2018; Taherdoost, 2022). The CSF consists of three components: Organisational Profiles, Tiers, and CSF Core (NIST, 2024b). The Organisational Profiles describe an organisation's current or desired cybersecurity posture in relation to the outcomes of the CSF Core (NIST, 2023). The CSF Tiers are used to categorise the level of an organisation's cybersecurity risk governance and management practices in Organisational Profiles (NIST, 2024a).

The CSF Core is a structured taxonomy of cybersecurity objectives that help organisations manage risks effectively (NIST, 2024b). It consists of a hierarchy of Functions, Categories, and Subcategories, each specifying a target outcome. Central to the NIST CSF are the six Functions—Govern, Identify, Protect, Detect, Respond, and Recover. These Functions are universally applicable, allowing any organisation regardless of their type and size, to tailor strategies to meet their unique risk profiles, technological environments, and goals (Toussaint et al., 2024). The Functions are further classified into 22 Categories, representing collective cybersecurity outcomes (NIST, 2024b). These Categories consist of 108 Subcategories, providing detailed descriptions of technical and managerial activities supporting each Category. In this study, we evaluated the policy documents of LGs against 22 Categories of six Core Functions. Table 1 presents all these Categories that were used as the evaluation criteria in this study.

Table 1. Functions and Categories of NIST CSF.

Function	Category	Description
Govern	Organisational Context	Organisation's mission, goal, stakeholder expectations, legal requirements.
	Risk Management Strategy	Priorities, constraints, risk appetite and tolerance statements, and assumptions of the organisation are established, disseminated, and utilised to support operational risk decisions.
	Roles, Responsibilities, and Authorities	Establishment and communication of cybersecurity roles, responsibilities, and authorities to promote accountability.

Identify	Policy	Cybersecurity policy is established, communicated, and enforced.
	Oversight	The outcomes and performance of risk management activities are utilised to inform, enhance, and modify the risk management strategy.
	Cybersecurity Supply Chain Risk Management	Supply chain risk management processes are identified, established, managed, monitored, and improved.
	Asset Management	Managing of assets, including personnel, facilities, services, data, hardware, software, and systems.
	Risk Assessment	Understanding risk to the organisation, its assets, and involved individuals.
	Improvement	Necessary improvement to organisational cybersecurity risk management processes, procedures, and activities.
Protect	Identity Management, Authentication, and Access Control	Restricting access to assets to only authorised users, services, and hardware.
	Awareness and Training	Training staff about cybersecurity related activities and raising awareness.
	Data Security	Management of data consistent with organisation's risk strategy.
	Platform Security	Management of hardware, software, systems, applications, and services of physical and virtual platforms consistent with organisation's risk strategy.
	Technology Infrastructure Resilience	Management of security architecture in accordance with the organisation's risk strategy.
Detect	Continuous Monitoring	Monitoring assets to detect anomalies, adverse events, potential breach.
	Adverse Event Analysis	Events are analysed to characterise and learn about them for future detection.
Respond	Incident Management	Managing incidents through response mechanism.
	Incident Analysis	Support forensics and recovery efforts and to ensure an effective response.
	Incident Response Reporting and Communication	Coordinating response activities with internal and external stakeholders.
	Incident Mitigation	Preventing the escalation of an incident and alleviating its consequences.
Recover	Incident Recovery Plan Execution	Ensuring operational availability of systems and services.
	Incident Recovery Communication	Coordination of restoration activities involving both internal and external stakeholders.

3. Methodology

3.1. Policy Documents

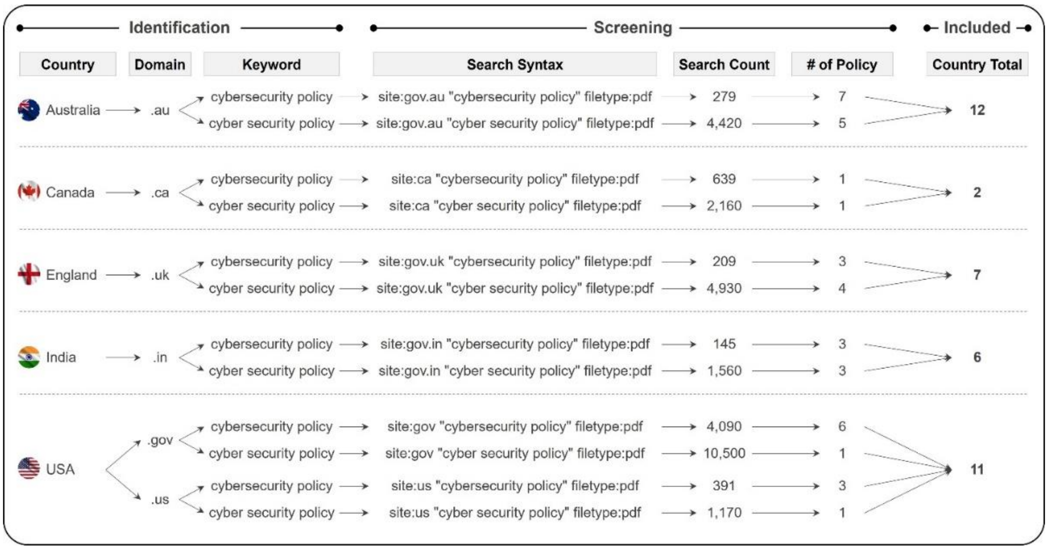
To address the first research question, our initial plan was to assess the policy documents of the top 100 digital cities under the assumption that they would possess structured cybersecurity policies. However, we found less than ten cybersecurity policy documents available online for those cities. This unavailability of policy documents in the online portal and their website should not be misunderstood as a lack of cybersecurity policies without empirical evidence; rather, it suggests that such policies may exist but are not readily available in the public domain.

In response to this challenge, we shifted to a more targeted approach by conducting an advanced keyword search in Google Search Engine to explore the cybersecurity policy documents of LGs in G20 member countries, focusing on English-language documents only. This strategy yielded relevant policy documents from LGs in Australia, Canada, England, India, and the USA, demonstrating the effectiveness of our approach. To broaden our scope, we expanded our search to include countries such as the Netherlands, Ireland, Scotland, Bangladesh, the UAE, and Saudi Arabia, anticipating the presence of cybersecurity policies in English. However, we did not find one available in the public domain. As a result, we excluded them from our study.

To locate policy documents, we employed an advanced search query in the following format: “site: (government domain) “keyword” filetype: (type of file)”. We substituted the term “government domain” with the appropriate domain for each country, such as “.in” for India and “.au” for Australia, to limit our search exclusively to websites belonging to government entities. Otherwise, we encountered a substantial volume of search results that were predominantly unrelated to our research. In “keyword”, we used “cybersecurity policy” and “cyber security policy”.

Lastly, we specified the filetype as “pdf” to search for policy documents in Portable Document Format (PDF), which is a commonly used format used to upload policies online. For example, to find policy documents in Australian LGs, we employed two search syntaxes: (a) site:gov.au “cybersecurity policy” filetype:pdf, and (b) site:gov.au “cyber security policy” filetype:pdf. The first search yielded 279 results, while the second search yielded 4,420 results. We applied similar strategies to other countries, except for the USA. Since the USA has two public domains, namely “.gov” and “.us”, we repeated the process twice.

Figure 1 displays the search count and the number of policy documents identified by each search query. We conducted the search during the first week of December 2023. We discovered a total of 38 cybersecurity policy documents, distributed as follows: 12 in Australia, two in Canada, seven in England, six in India, and 11 in the USA. Table 2 presents notable attributes of the LGs that possess the cybersecurity policy documents identified in this study.



Country	Domain	Keyword	Search Syntax	Search Count	# of Policy	Country Total
Australia	.au	cybersecurity policy	site:gov.au "cybersecurity policy" filetype:pdf	279	7	12
		cyber security policy	site:gov.au "cyber security policy" filetype:pdf	4,420	5	
Canada	.ca	cybersecurity policy	site:ca "cybersecurity policy" filetype:pdf	639	1	2
		cyber security policy	site:ca "cyber security policy" filetype:pdf	2,160	1	
England	.uk	cybersecurity policy	site:gov.uk "cybersecurity policy" filetype:pdf	209	3	7
		cyber security policy	site:gov.uk "cyber security policy" filetype:pdf	4,930	4	
India	.in	cybersecurity policy	site:gov.in "cybersecurity policy" filetype:pdf	145	3	6
		cyber security policy	site:gov.in "cyber security policy" filetype:pdf	1,560	3	
USA	.gov	cybersecurity policy	site:gov "cybersecurity policy" filetype:pdf	4,090	6	11
		cyber security policy	site:gov "cyber security policy" filetype:pdf	10,500	1	
	.us	cybersecurity policy	site:us "cybersecurity policy" filetype:pdf	391	3	
		cyber security policy	site:us "cyber security policy" filetype:pdf	1,170	1	

Figure 1. Summary of search results for LG cybersecurity policy documents.

Table 2. Salient characteristics of LGs that have cybersecurity policy documents found in this study.

LG	Location	LG Status					Population	Policy Adoption/ Last Update Year
		Country Capital	State	State Capital	Metropolitan	Rural Area		2021
Central Highlands Council	Australia					✓	2,144	Not Mentioned
Murray River Council						✓	11,456	2022
Sutherland Shire Council					✓		218,464	2023
Bayswater					✓		69,283	2021
Western Australia			✓				2,660,026	2022
New South Wales			✓				8,072,163	2022
Tasmania			✓				557,571	2023
Murrumbidgee Council						✓	4,000	2021
Rous County Council						✓	100,000	2019
King Island Council						✓	1,617	2022
Copper Coast Council						✓	15,050	2022
Balranald Shire Council						✓	2,208	2023
Vancouver	Canada				✓		662,248	2022
Greenview						✓	8,584	2016
London	England	✓			✓		9,748,033	2023
Enfield					✓		330,000	2021
Northwest Leicestershire District Council					✓		104,705	2020
Crediton Town					✓		21,990	2020
Royal Borough Windsor & Maidenhead (RBWM)					✓		154,738	2021
Saughall and Shotwick						✓	3,094	2022

Park Parish Council						
Aylesford Parish Council				✓	11,671	2022
Telangana	India	✓			38,157,311	2021
Odisha		✓			47,099,270	2022
Jammu and Kashmir		✓			14,999,397	2020
Tamil Nadu		✓			83,697,770	2020
Assam		✓			35,713,000	2018
Tripura		✓			4,184,959	
Woodburn City Council	USA		✓		26,243	2019
City and County of San Francisco			✓		670,625	2021
New York			✓		7,613,466	2020
Village of Pleasantville				✓	7,305	2021
Beaverton			✓		100,559	2022
Albuquerque			✓		556,496	2023
Portland			✓		13,701	2020
Scappoose			✓		8,191	2020
City of Madras			✓		8,200	2020
Town of Norwich				✓	6,476	2021
City of Lebanon			✓		48,629	2022

3.2. Research Strategy

This study used the content analysis method to evaluate cybersecurity policy documents. We defined the Functions of NIST CSF as codes and Categories as sub-codes (Table 3) and used NVivo 14.23.2 (46) software to classify and conduct analysis. The evaluation process encompasses the identification of recurring themes, patterns, and gaps. We employed this systematic approach to gain insights from the existing policy documents, which later helped us develop the cybersecurity policy framework.

Table 3. Codes and sub-codes used in this study for content analysis.

Function	Category
Govern	Organisational Context, Risk Management Strategy, Roles, Responsibilities, and Authorities, Policy, Oversight, and Cybersecurity Supply Chain Risk Management
Identify	Asset Management, Risk Assessment, Improvement

doi:10.20944/preprints202405.0641.v1

Protect	Identity Management, Authentication, and Access Control, Awareness and Training, Data Security, Platform Security, Technology Infrastructure Resilience
Detect	Continuous Monitoring, Adverse Event Analysis
Respond	Incident Management, Incident Analysis, Incident Response Reporting and Communication, Incident Mitigation
Recover	Incident Recovery Plan Execution, Incident Recovery Communication

4. Results and Analysis

4.1. Quantitative Content Analysis

We assessed LGs' cybersecurity policy documents using quantitative content analysis tools in NVivo Software. Initially, we generated word clouds to visually emphasise the most frequently cited words within the policy documents, with the largest size representing those that were mentioned most frequently. Figure 2 displays the frequency of words in cybersecurity policy documents, while Figure 3 shows the frequency of words in the coded data specifically. We examined the number of cited policy documents for each code and sub-code, as well as the frequency of sub-codes within the policy documents. Of the six codes, 37 policy documents addressed Govern, while 16 policy documents addressed Recover. Table 4 shows that the sub-codes under Protect Function were cited most frequently (n=222), followed by the sub-codes under Govern (n=220), while the sub-codes under Recover were cited the least (n=22).

Figure 4 displays a hierarchical chart generated in NVivo software showing all the codes and sub-codes from the aggregated cybersecurity policy document data. Each rectangular section corresponds to a specific code frequency. The chart shows that the most prevalent codes in the analysis of policy documents were Protect and Govern, while the least prevalent codes were Recover and Detect. The hierarchy chart shows the prominence of sub-codes, with Identify, Management, Authentication, and Access Control under the Protect code and Roles, Responsibilities, and Authorities under the Govern code being the most prominent. On the other hand, Incident Recovery Communication under the Recover code and Incident Analysis under the Respond code are the least prominent sub-codes.

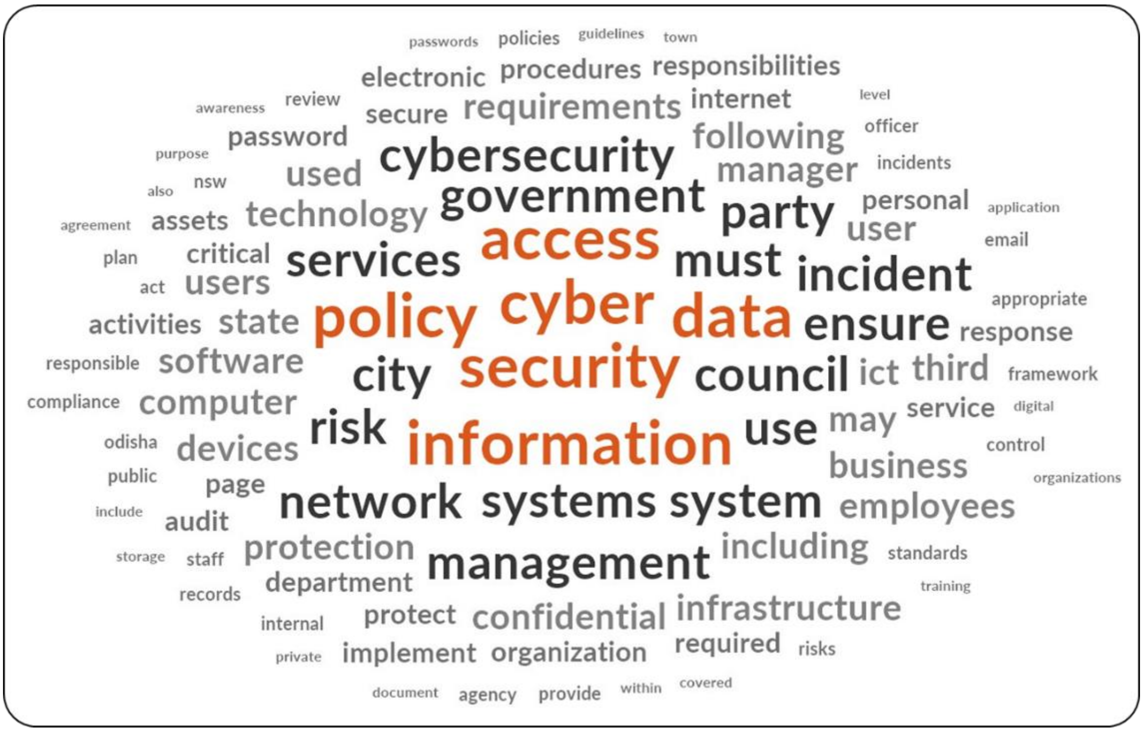


Figure 2. Word cloud of the policy documents.

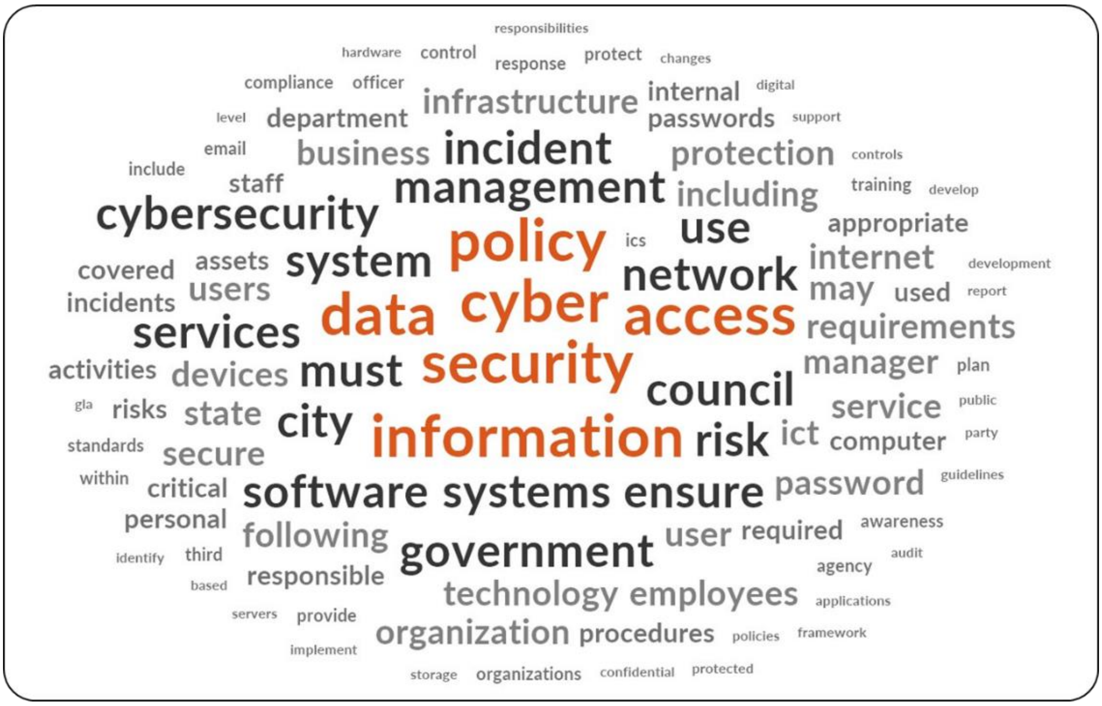


Figure 3. Word cloud of the coding.

Table 4. Frequency of the codes and sub-codes.

Code and Document Frequency	Sub-Code	Documents with Sub-Code	Frequency of Sub-Code	Total Frequency for Sub-Codes
Govern = 37	Organisational Context	27	71	220
	Risk Management Strategy	22	37	
	Roles, Responsibilities, and Authorities	27	76	
	Policy	21	31	
	Oversight	0	0	
	Cybersecurity Supply Chain Risk Management	4	5	
Identify = 29	Asset Management	25	42	71
	Risk Assessment	14	18	
	Improvement	9	11	
Protect = 32	Identity Management, Authentication, and Access Control	29	77	222
	Awareness and Training	24	40	
	Data Security	18	51	
	Platform Security	15	43	
	Technology Infrastructure Resilience	5	11	
Detect = 19	Continuous Monitoring	19	23	34
	Adverse Event Analysis	7	11	
Respond = 30	Incident Management	27	44	64
	Incident Analysis	2	2	

	Incident Response Reporting and Communication	9	13	
	Incident Mitigation	5	5	
Recover = 16	Incident Recovery Plan Execution	16	20	22
	Incident Recovery Communication	2	2	

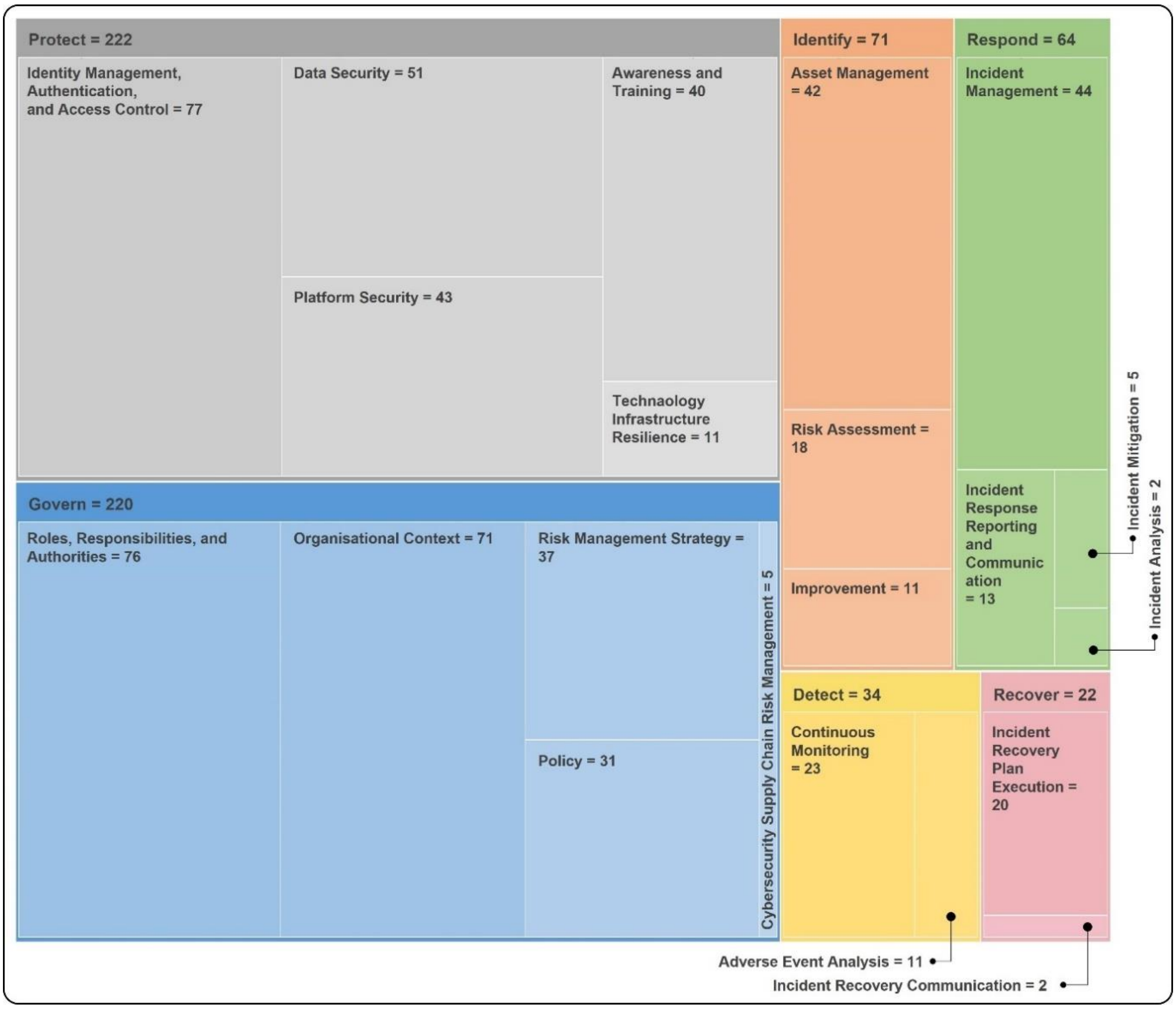


Figure 4. Hierarchy of codes and sub-codes.

4.2. Qualitative Content Analysis

Following the quantitative analysis, this study conducted a qualitative content analysis to identify recurring themes and patterns in the policy documents for each of the Categories of NIST CSF Functions. We developed a concept map (Figure 5) to effectively communicate these themes and emphasis of each Categories in the policies, which ultimately indicate the areas of strength or weakness in current cybersecurity practices at the LG level. The following sections present details of the qualitative content analysis.

doi:10.20944/preprints202405.0641.v1

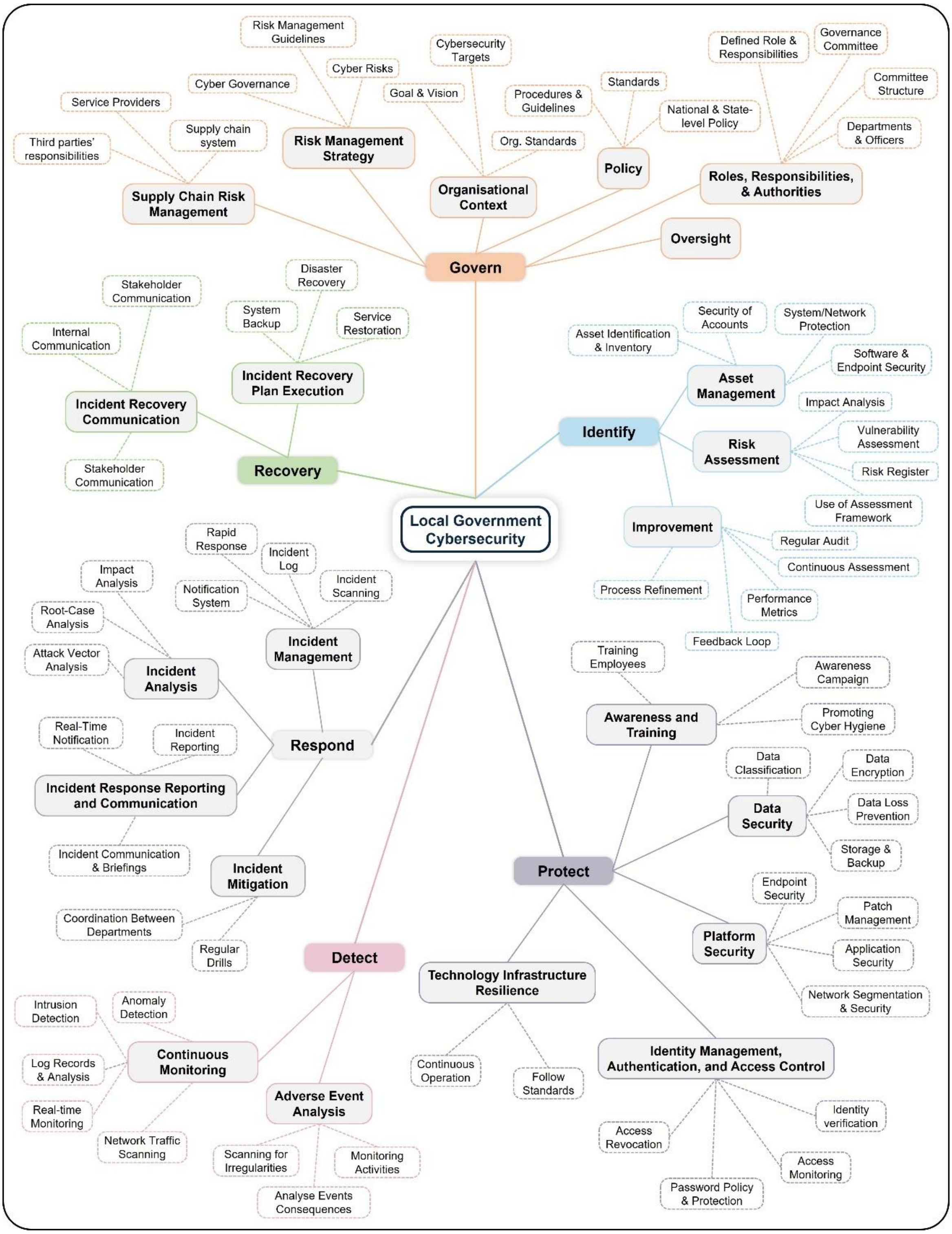


Figure 5. Local Governments' cybersecurity policy concept map.

4.2.1. 'Govern' with Focus on Organisational Risk and Responsibility

The Govern Function includes six Categories as presented in Table 4. Among the 38 policy documents that we reviewed, 37 addressed Govern. However, none of them encompassed all six Categories under this Function. Most of the policies (n=27) included statements on organisational context and the roles of personnel, emphasising LGs' goals, vision, cybersecurity targets, standards, and responsibilities of officials, departments, and dedicated committees. For example, the RBWM's policy highlighted the importance of executing desired actions as suggested in the policies:

"The aim ... to ensure that the correct processes and procedures, roles and responsibilities are in place and followed for any council cyber threat or incident while we continue our normal business operations" (RBWM, 2020, p. 4).

Articulating risk management strategies involves establishing and communicating the organisation's priorities, constraints, and assumptions to support operational risk decisions (Öğüt et al., 2011). Only 22 policy documents covered this Category, addressing statements mostly related cyber risks, risk management guidelines, and cyber governance. A similar number of policy documents (n=21) addressed statements on communication and enforcement of policies, emphasising the need for procedures and guidelines, standards, and national and state-level policy alignment. The study also revealed that supply chain risk management, and oversight have been rarely cited (n=4, and n=0, respectively) in the policies. In four documents that included statements for supply chain risk management, mostly focused on the roles and responsibilities of third parties and service providers who support LGs in operating software and maintaining hardware.

4.2.2. 'Identify' with Focus on Asset and Risk Management

Our study found a total of 29 cybersecurity policy documents that addressed at least one of the three underlying Categories. Among them, 25 policy documents adequately covered asset management, addressing endpoint or hardware security, software security, security of personal and organisational service accounts, and network protection. For instance, Beaverton's policy focused on keeping inventory of hardware and software as follow:

"...must take an inventory of all approved hardware and software on City networks and systems; one inventory for hardware and one for software" (Beaverton, 2021, p. 4).

Impact analysis of cyber-attacks, vulnerability assessment, risk registration, and use of assessment frameworks have been highlighted to address Risk Assessment Category in the policies. This Category has been covered by only 14 policies. Improvement is another Category under Identify Function and has been address only in a few policies (n=9). Regular audits, continuous assessments, feedback loops, performance metrics, and process refinements have been emphasised in the policies to address this Category.

4.2.3. 'Protect' with Focus on Access Control, and Raising Awareness

We found 32 policies addressing one or more among five Categories of this Function. Identity verification, password policy, and access monitoring have been heavily emphasised in the policy documents (n=29) to address identity management and access control. Some policy documents have also included statements on the access revocation of employees as soon as they leave LGs, such as Portland's policy:

"System administrator passwords will be terminated immediately if the employee who has access to such passwords is terminated, fired, investigated, or otherwise leaves employment" (Portland, 2023, p. 3).

The policy documents (n=24) have frequently addressed the Awareness and Training Category, with emphasis on training employees, running awareness campaigns, and promoting cyber-hygiene. The Technology Infrastructure Resilience Category has been mentioned in a few policies (n=5), emphasising continuous operation and following standards. Data Security and Platform Security are two crucial Categories of Protect Function, particularly critical for LGs. Data and platform security are very important aspect of organisational cybersecurity. However, we found only 18 policy documents that addressed Data Security and 15 that cited Platform Security. Endpoint security, patch management, network segmentation, and application security are covered under Platform Security Category, whereas data classification, encryption, Data Loss Prevention, and storing and backing up data have been highlighted under the Data Security Category in the policy documents.

4.2.4. 'Detect' with Focus on Continuous Monitoring

A total of 19 cybersecurity policy documents encompassed statements on this Function. All of them included statements about ongoing surveillance to identify anomalies and breaches. However, only seven of them addressed adverse event analysis, which is the other Category of this Function, focusing statements on scanning for irregularities, analysis of cyber-attack consequences, and monitoring activities. To address continuous monitoring, the policies mentioned anomaly detection, real-time monitoring, keeping log records, intrusion detection, and network traffic monitoring. For instance, the policy document of the City of Madras addressed:

"All organization servers and workstations will utilize Microsoft Windows Defender with Windows Advanced Threat Protection (ATP) to protect systems from malware and viruses. Real-time scanning will be enabled on all systems and weekly malware scans will be performed" (Madras, 2020, p. 13).

4.2.5. 'Respond' with Focus on Incident Management

We found 30 cybersecurity policy documents covering this Function in varying degrees of adherence to the four Categories under this Function. Of those, 27 addressed incident management, with an emphasis on incident scanning, logs, rapid response, and notification systems. The policy document of Norwich stated:

"... develop and implement appropriate activities to take action regarding a detected cybersecurity event, Response processes and procedures are executed and maintained, to ensure adequate response and recovery actions" (Norwich, 2020, p. 2).

Other Categories under Respond have been cited in a significantly low number of policies, with the Incident Analysis (n=2) focusing on impact analysis, root-cause analysis, and attack vector analysis; the Incident Response, Reporting, and Communication (n=9) emphasising real-time notification, incident reporting, incident communication, and briefings; and the Incident Mitigation (n=2) focusing on regular drills and coordination between departments.

4.2.6. 'Recover' with Focus on Incident Recovery Plan Execution

We only identified 16 policy documents addressing this Function. All of them included statements on incident recovery plan execution, which included statements for service restoration, disaster recovery, and system backup. Woodburn and Lebanon included statements on Incident Recovery Communication, which is the other Category under Recover. The statements emphasised stakeholders' communication, international communication, and internal coordination. For instance, Woodburn's cybersecurity policy stated:

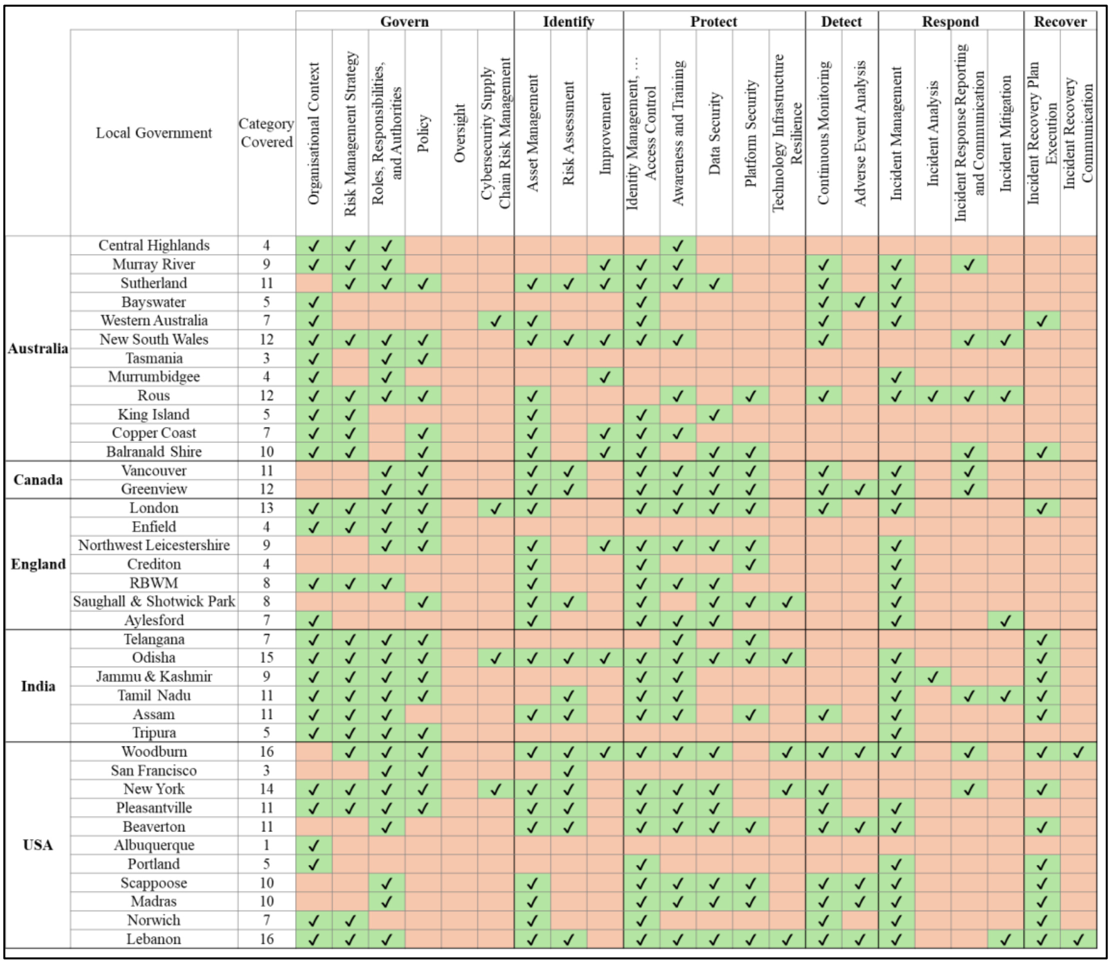
"External communications should only be handled by designated individuals at the direction of the City Administrator. Recovery activities are communicated to internal stakeholders, executives, and management teams" (Woodburn, 2021, p. 12).

5. Findings and Discussion

5.1. Insights from Cybersecurity Policies of LGs

Our study revealed concerning gaps since none of the policies addressed each Categories of NIST CSF. In fact, 24 of the 38 policies covered less than half of total Categories. Figure 6 shows the coverage of Functions and Categories by policy documents.

doi:10.20944/preprints202405.0641.v1



	Local Government	Category Covered	Govern						Identify			Protect					Detect		Respond				Recover	
			Organisational Context	Risk Management Strategy	Roles, Responsibilities, and Authorities	Policy	Oversight	Cybersecurity Supply Chain Risk Management	Asset Management	Risk Assessment	Improvement	Identity Management, … Access Control	Awareness and Training	Data Security	Platform Security	Technology Infrastructure Resilience	Continuous Monitoring	Adverse Event Analysis	Incident Management	Incident Analysis	Incident Response Reporting and Communication	Incident Mitigation	Incident Recovery Plan Execution	Incident Recovery Communication
Australia	Central Highlands	4	✓	✓	✓								✓											
	Murray River	9	✓	✓	✓						✓	✓	✓				✓		✓		✓			
	Sutherland	11		✓	✓	✓			✓	✓	✓	✓	✓	✓			✓		✓					
	Bayswater	5	✓									✓					✓	✓	✓					
	Western Australia	7	✓					✓	✓			✓					✓		✓				✓	
	New South Wales	12	✓	✓	✓	✓			✓	✓	✓	✓	✓				✓				✓	✓		
	Tasmania	3	✓		✓	✓																		
	Murrumbidgee	4	✓		✓						✓								✓					
	Rous	12	✓	✓	✓	✓			✓				✓		✓		✓		✓	✓	✓	✓		
	King Island	5	✓	✓					✓			✓		✓										
	Copper Coast	7	✓	✓		✓			✓		✓	✓	✓											
	Balranald Shire	10	✓	✓		✓			✓		✓	✓		✓	✓						✓		✓	
Canada	Vancouver	11			✓	✓			✓	✓		✓	✓	✓	✓		✓		✓		✓			
	Greenview	12			✓	✓			✓	✓		✓	✓	✓	✓		✓	✓	✓		✓			
England	London	13	✓	✓	✓	✓		✓	✓			✓	✓	✓	✓		✓		✓				✓	
	Enfield	4	✓	✓	✓	✓																		
	Northwest Leicestershire	9			✓	✓			✓		✓	✓	✓	✓	✓				✓					
	Crediton	4							✓			✓			✓				✓					
	RBWM	8	✓	✓	✓				✓			✓	✓	✓					✓					
	Saughall & Shotwick Park	8				✓			✓	✓		✓		✓	✓	✓			✓					
	Aylesford	7	✓						✓			✓	✓	✓					✓			✓		
India	Telangana	7	✓	✓	✓	✓							✓		✓								✓	
	Odisha	15	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓			✓				✓	
	Jammu & Kashmir	9	✓	✓	✓	✓						✓	✓						✓	✓			✓	
	Tamil Nadu	11	✓	✓	✓	✓				✓		✓	✓						✓		✓	✓	✓	
	Assam	11	✓	✓	✓				✓	✓		✓	✓		✓		✓		✓				✓	
	Tripura	5	✓	✓	✓	✓													✓					
USA	Woodburn	16		✓	✓	✓			✓	✓	✓	✓	✓	✓		✓	✓	✓	✓		✓		✓	✓
	San Francisco	3			✓	✓				✓														
	New York	14	✓	✓	✓	✓		✓	✓	✓		✓	✓	✓		✓	✓				✓		✓	
	Pleasantville	11	✓	✓	✓	✓			✓	✓		✓	✓	✓			✓		✓					
	Beaverton	11			✓				✓	✓		✓	✓	✓	✓		✓	✓	✓				✓	
	Albuquerque	1	✓																					
	Portland	5	✓									✓							✓				✓	
	Scappoose	10			✓				✓			✓	✓	✓	✓		✓	✓	✓				✓	
	Madras	10			✓				✓			✓	✓	✓	✓		✓	✓	✓				✓	
	Norwich	7	✓	✓					✓			✓					✓		✓				✓	
	Lebanon	16	✓	✓	✓				✓	✓		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓

Figure 6. NIST CSF Function and Category coverage by policy documents.

In Australia, only three LGs (Sutherland, NSW, and Rous) addressed more than 10 Categories (n=11, n=12, and n=12, respectively). State Governments such as Tasmania and Western Australia (WA), presumably with more resources than local councils, addressed only 3 and 7 Categories, respectively. None of Australia's cybersecurity policies addressed supply chain risk management, except for WA. This gap is particularly concerning given the rapid increase in digital device usage and LGs' adoption of smart city initiatives (Verhulsdonck et al., 2023; Yigitcanlar et al., 2023a, 2023b). In the process of digital advancement, LGs tend to rely more on an intricate web of suppliers (Popescul & Radu, 2016; David et al., 2023). Inadequate measures to proper management of these suppliers make them vulnerable to increased cybersecurity threats (Boyson, 2014; Vitunskaite et al., 2019).

An important, perhaps most critical, asset of LGs, which often makes them an attractive and frequent target for cyber-attacks, is the storage of a wide range of sensitive data, including individual-centric data, public safety and governance data, infrastructure and utility data, and community and environment data (MacManus et al., 2013; Ali et al., 2020; Sadik et al., 2020). LGs typically prioritise securing this data and platforms, which include software and hardware for storage and communication (Caruson et al., 2012; Ullah et al., 2021). Most of the policies in Australia did not mention clear statements in these two Categories. Even NSW's policy, which is among the top two that covered the greatest number of Categories, failed to comprehensively mention statements on data and platform security.

Risk assessment involves understanding risks to LG's assets and employees (Kalinin et al., 2021), an important Category that has been overlooked in most of the policies in Australia, except for Sutherland and New South Wales, revealing a potential gap in risk assessment practices in LGs. This lack can hinder effective cybersecurity threat mitigation and response (Fielder et al., 2018; Goel et al., 2020). One of the strengths identified in most of the cybersecurity policies in Australia, which is often missing in the policies of other countries, is the presence of Improvement in most of the policies. This Category involves identifying enhancements to organisational cybersecurity risk management processes, procedures, and activities to keep up with evolving threats (Srinivas et al., 2019; Hatcher et al., 2020).

Vancouver and Greenview in Canada addressed 11 and 12 Categories, respectively, in their policies. These two policies effectively mentioned employer responsibilities, asset management, risk assessment, access control, data and platform security, and continuous monitoring for cyber-attacks. However, both policies failed to address incident mitigation, recovery plan execution, and communication, which are crucial to restoring assets and operations affected by cybersecurity incidents (Hamdani et al., 2021; Ma, 2021). None of the LG's policies in Canada mentioned technology infrastructure resilience, indicating a significant gap in maintaining continuous operations or defending against the increasing sophistication of cyberthreats (AlDaajeh et al., 2022).

In England, except for the policy documents of London, other LGs addressed less than 10 Categories each. The cybersecurity policies of Enfield and Crediton are among the least comprehensive ones, covering only four Categories each, ignoring important statements on training and awareness, data and platform security, and monitoring activities to detect and respond. Even though London's cybersecurity policy is one of the most comprehensive policies that we reviewed, it still failed to include crucial details on incident analysis, reporting, and mitigation, along with most other LGs in England. The incident analysis entails activities such as investigation to facilitate efficient response and recovery efforts (Sun et al., 2019; Patterson et al., 2023), whereas the incident mitigation involves activities to prevent the expansion of a cyber-attack (Habibzadeh et al., 2019; Ali et al., 2020). The policy documents of London, Northwest Leicestershire, the RBWM, and Aylesford in England emphasised training and awareness, understanding the need to equip personnel with the necessary knowledge and skills. This is particularly significant as human factors are often considered a vital weak point in cyber defences (Javed et al., 2022; Nuñez et al., 2023).

Among Indian LGs, Odisha has successfully addressed 15 Categories. However, like other policies in India, Odisha's cybersecurity policy inadequately addressed the Detect Function. This Function refers to the process of identifying and analysing potential cybersecurity threats, which serves as a foundation for the efficient implementation of incident response and recovery activities (Ahmadi-Assalemi et al., 2020; NIST, 2024a). None of the policy documents of Indian LGs mentioned incident recovery communication, which involves informing internal and external stakeholders, such as communities, about the incident to update them about the restoration process and maintain organisational integrity and public trust. Another important Function that has not been addressed in most of the cybersecurity policies in India is the Protect Function. Critical topics such as asset management, including data, software, hardware, services, people, facilities, and systems, risk assessment, and improvement, have been largely absent in most of the cybersecurity policies of LGs in India.

In the USA, six of the 11 policy documents addressed less than 10 Categories of NIST CSF. Some cities such as Albuquerque, San Francisco, and Portland addressed only one, three, and five Categories, respectively, which is particularly concerning. Articulating risk management strategies in the policies is crucial, as it involves establishing and communicating the organisation's priorities, constraints, risk tolerance, and assumptions to support operational risk decisions (Öğüt et al., 2011). But the policy documents of Albuquerque, San Francisco, Portland, Scappoose, Madras, Beaverton, and Woodburn failed to mention this. Statements on supply chain risk management are also absent in all the policies in the USA, except for New York. The USA's policy documents showed strength in addressing Protect Function, which refers to security measures created to prevent or minimise cybersecurity threats by securing assets (Ibrahim et al., 2018; Möller, 2023). As indicated in Figure 6, most of the LGs in the USA addressed access control, awareness and training procedures, data security, and platform security adequately.

5.2. Key Contributing Factors to Existing Gaps in the Cybersecurity Policies

The study revealed a significant gap in encompassing NIST CSF Functions and Categories in the policies as discussed above. We identified and argued for several potential factors behind these gaps in the policies. A key contributing factor could be that LGs may follow country specific cybersecurity guidelines or frameworks such as the Essential Eight in Australia (Syafrizal et al., 2020; Grobler et al., 2021). To verify this, we calculated the number of NIST CSF Categories addressed by each policy document, as shown in Figure 7.

We found that there is no significant difference in NIST CSF Function and Category coverage between cybersecurity policy documents in the USA and in other countries. In fact, policy documents in Australia, Canada, England, India, and the USA addressed about four to five Functions on average. On the other hand, the policy documents of Australia, England, India, and the USA covered about seven to nine Categories on average. Canada's policy documents addressed more Categories (n=11) on average than other countries. However, these numbers of Category coverage are significantly lower than the total number of Categories (n=22) in the NIST CSF. Despite differences in terminologies or categorical emphasis between national frameworks, the fundamental objective and thematic elements of cybersecurity are consistent across most frameworks. So, while some LGs may align with their national framework or strategy, we still found a similar coverage of NIST CSF Functions and Categories among LGs from different countries.

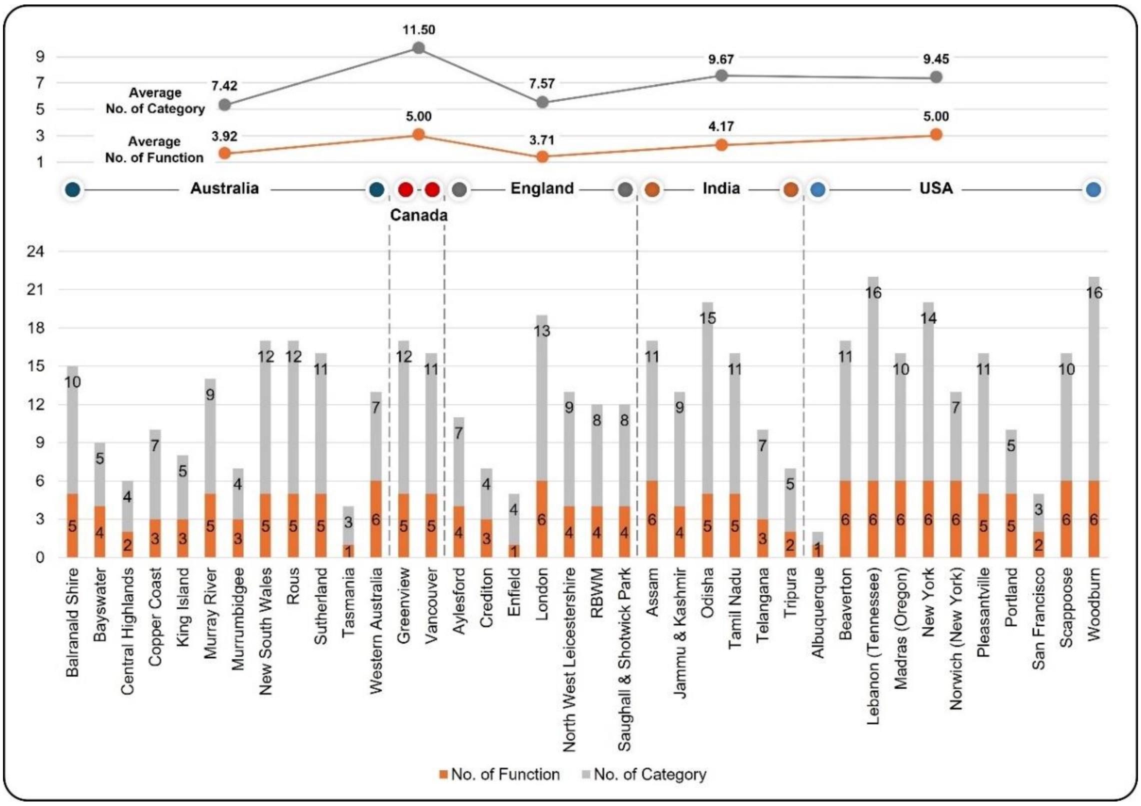


Figure 7. Number of Functions and Categories addressed by each policy documents and country-wise average of Functions and Categories.

The use of NIST CSF 2.0 as the evaluation benchmark, which was recently released in February 2024, could also contribute to the disparities in cybersecurity policy documents, as all the policy documents used in the study were published prior to 2024. So, we further examined the Functions and Categories of previous NIST CSF versions. The current version introduces a sixth Function—Govern, recognising its importance and influence across all other Functions. This new Function is an extension of the Governance Category under Identify Function in the previous versions. The Govern Function comprises two Categories from previous versions and four new Categories. Despite these changes, 18 Categories out of 22 in the latest NIST CSF remained consistent with the previous versions. Surprisingly, our study found that three of the four recently added Categories (Organisational Context, Roles, Responsibilities, and Authorities, and Policy) have been addressed relatively higher (n=27, n=27, and n=21, respectively) than many other Categories. Overall, the update in versions mostly involved reclassification and combining certain Categorise together to enhance their applicability and simplicity. Therefore, this consistency between versions allowed us to conduct a valid and relevant evaluation of the cybersecurity policy documents against the Functions and Categories of NIST CSF 2.0 and present an overview of the gaps in existing policy documents.

Several studies identified limited financial resources and expertise and a lack of proper knowledge of the LGs' officials about the significance of cybersecurity as major challenges to effective cybersecurity measures (Ibrahim et al., 2018; Norris et al., 2021; Norris & Mateczun, 2022). LGs, particularly smaller LGs, face these challenges more often (Hatcher et al., 2020). Furthermore, many LGs underestimate their digital infrastructure with a lower risk profile, overlooking the fact that all LGs, regardless of their size, are attractive targets because they store critical citizen and governance data (Bauer & van Eeten, 2009; Li et al., 2019). Our findings also indicate the same, as we found that the policy documents of the top 10 smaller LGs in terms of population addressed a lower number (n=8) of Categories on average than the top 10 larger LGs (n=10) even though they covered a similar number of Functions on average (n=4) as presented in Figure 8.

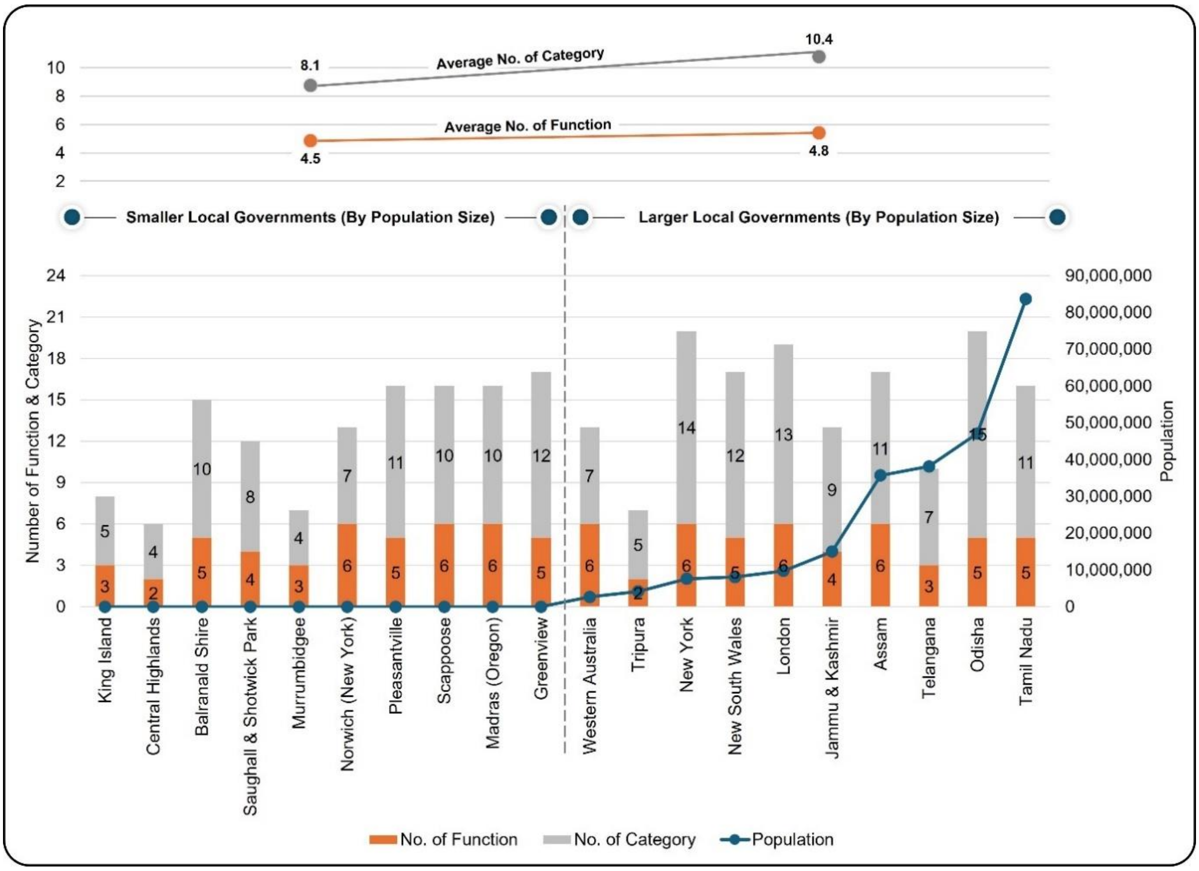


Figure 8. Average coverage of Functions and Categories in cybersecurity policy documents by top 10 smaller and larger LGs.

However, the average number of Categories covered either by smaller or larger LGs is not even close to the total number of 22 Categories. These statistics indicate that regardless of the size of LGs, cybersecurity policy documents still lack critical details, and we acknowledge the absence of a well-defined and acceptable cybersecurity policy framework as a vital cause. Several researchers have also emphasised the importance of cybersecurity policy and a structured policy framework (Harknett & Stever, 2011; Hatcher et al., 2020; Wu et al., 2020; Ariffin & Ahmad, 2021; Grobler et al., 2021; Mishra et al., 2022) as the inconsistencies in the policy documents not only hinder best practices but also significantly expose LGs to cyber-attacks. Therefore, this study advocates for and develops a

doi:10.20944/preprints202405.0641.v1

cybersecurity policy framework to guide LGs through the complex process of establishing effective cybersecurity strategies without missing any critical details.

5.3. Cybersecurity Policy Framework for LGs

Our proposed cybersecurity policy Framework encompasses seven key components and 38 sub-items, as illustrated in Figure 9. Document Introduction is the first key component that includes introductory information, such as organisation name, approvers' details, approval date and upcoming review date. The second key component —Organisational Context comprises sub-items that present organisational background, including organisational overview, purposes, scope, definition or explanation of the vital terms, policy alignment with state, national, or regional policy or agreement, and periodic or emergency policy amendment procedures. Cybersecurity administrative structure, roles and responsibilities of departments, employees, and contractors, regulatory compliances, disciplinary actions in case of policy violation, and public communication in case of a breach are all included under Cybersecurity Governance, which is the third key component of our policy framework.

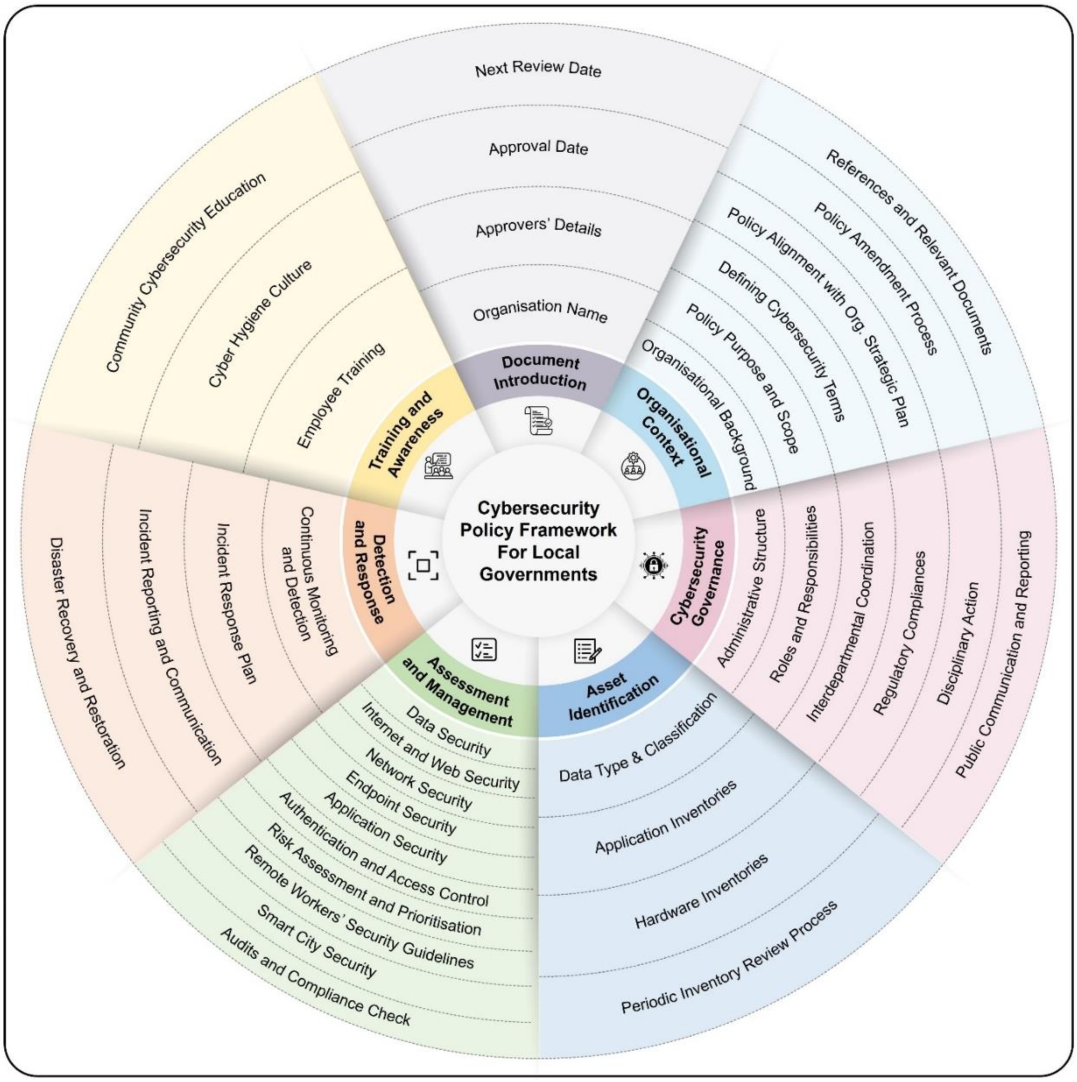

Cybersecurity Policy Framework For Local Governments
Document Introduction
Organisation Name
Approvers' Details
Approval Date
Next Review Date
Organisational Context
Organisational Background
Policy Purpose and Scope
Defining Cybersecurity Terms
Policy Alignment with Org. Strategic Plan
Policy Amendment Process
References and Relevant Documents
Cybersecurity Governance
Administrative Structure
Roles and Responsibilities
Interdepartmental Coordination
Regulatory Compliances
Disciplinary Action
Public Communication and Reporting
Asset Identification
Data Type & Classification
Application Inventories
Hardware Inventories
Periodic Inventory Review Process
Assessment and Management
Data Security
Internet and Web Security
Network Security
Endpoint Security
Application Security
Authentication and Access Control
Risk Assessment and Prioritisation
Remote Workers' Security Guidelines
Smart City Security
Audits and Compliance Check
Detection and Response
Continuous Monitoring and Detection
Incident Response Plan
Incident Reporting and Communication
Disaster Recovery and Restoration
Training and Awareness
Employee Training
Cyber Hygiene Culture
Community Cybersecurity Education

Figure 9. Proposed cybersecurity policy framework.

Asset Identification is the fourth key component of our framework dedicated to identifying and categorising LGs' assets, including the types of data, inventories of software, applications, and digital devices. The fourth key component also includes a Sub-item—periodic inventory review process—highlighting the importance of having a structured inventory review process, considering the constantly evolving nature of technology and cyberthreats. The fifth key component —Assessment and Management emphasises identifying potential risks and implementing appropriate measures to mitigate them. The component includes sub-items such as risk assessment and prioritisation, authentication and access control mechanisms, and clear guidelines on the core cybersecurity concepts, including data security, internet security, web security, network security, application security, and endpoint security. Given the rise of remote workers, we have also included a sub-item under this component that highlights the security protocols and practices necessary to secure their access to LGs' networks. LGs have significantly increased their use of IoT devices in recent years, as have adoption of smart city initiatives. This prompted us to add a sub-item—Smart City Security—to our framework, which is only applicable for LGs that act as the administrators of smart cities. Audits and Compliance Check is the last sub-item under the fifth Key Component, emphasising the importance of assessing vulnerabilities regularly and keeping practices updated.

Detection and Response is the sixth key component of our policy framework, which includes Sub-items for continuous and real-time monitoring to detect cyber-attacks. A structured incident response plan, with procedures to report and alert within departments, detailing a clear step-by-step process for swift and coordinated actions during a cyber incident, is crucial for immediate action against cyber-attacks. Sequential instructions on disaster recovery and restoration after a cyber-attack should also be included in the LGs' cybersecurity policy to minimise operational disruptions, and hence, we included this as a Sub-item in our policy framework. Training and Awareness is the last and final key component of our policy framework, recognising the importance of training and awareness for employees, contractors, and anyone who interacts with LGs. Particularly for employees, establishing a culture of cyber-hygiene in their day-to-day activities can significantly benefit LGs by reducing potential weak links for breaches. Overall, the policy framework covers a wide range of considerations—from governance and asset management to response planning and community awareness—and provides a blueprint for LGs to develop cybersecurity policies and

6. Conclusion

This study revealed concerning gaps in the existing cybersecurity policies of LGs, irrespective of their size and location. We investigated and discussed various potential contributing factors to these gaps, and we acknowledged the absence of a unifying and guiding framework as a principal cause. Therefore, we developed a cybersecurity policy framework for LGs, offering a structured approach to cover all essential aspects and guiding them to formulate effective policy documents.

Our proposed policy framework shares certain overlapping and similarities of topics with NIST CSF. However, while NIST CSF act as an assessment tool of the cybersecurity posture of any organisation, our policy framework serves as a guiding tool for LGs to formulate effective cybersecurity policies without missing critical details. Most of the sub-items under the seven key components of our cybersecurity policy framework are broadly applicable in various organisational contexts, but its true uniqueness and value lie in its tailored approach to address specific aspects of LG operations. Among them is the emphasis on data security. Unlike many organisations, LGs store and manage a diverse range of sensitive data, including residents' personal information, urban infrastructural data, governance data, spatial data, and so on. Public trust and safety. Given the sensitivity and breadth of this data, it necessitates a nuanced approach to data security, one that goes beyond standard practices to address the specificities of public sector information management.

Author Contributions: STH: Data collection, processing, investigation, analysis, and writing - review & editing; TY, KN and YX: Supervision, conceptualization, writing - review & editing. All authors have read and agreed to the published version of the manuscript.".

Funding: This research was funded by the Australian Research Council Discovery Grant Scheme, grant number DP220101255.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data will be made available upon request from the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Ahmadi-Assalemi, G., Al-Khateeb, H., Epiphaniou, G., & Maple, C. (2020). Cyber resilience and incident response in smart cities: A systematic literature review. Smart Cities, 3(3), 894-927. https://doi.org/https://doi.org/10.3390/smartcities3030046
2. AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Raymond Choo, K.-K. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security, 119, 102754. https://doi.org/https://doi.org/10.1016/j.cose.2022.102754
3. Ali, O., Shrestha, A., Chatfield, A., & Murray, P. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. Government Information Quarterly, 37(1), 101419. https://doi.org/https://doi.org/10.1016/j.giq.2019.101419
4. Ariffin, K. A. Z., & Ahmad, F. H. (2021). Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0. Computers & Security, 105, 102237. https://doi.org/https://doi.org/10.1016/j.cose.2021.102237
5. Bauer, J. M., & van Eeten, M. J. G. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. Telecommunications Policy, 33(10), 706-719. https://doi.org/https://doi.org/10.1016/j.telpol.2009.09.001
6. Beaverton. (2021). Cybersecurity policy. City of Beaverton, Oregon, USA Retrieved from https://content.civicplus.com/api/assets/fda4939f-c8e3-4228-85b8-87d31ae22c6d
7. Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation, 34(7), 342-353. https://doi.org/https://doi.org/10.1016/j.technovation.2014.02.001
8. Caruson, K., MacManus, S. A., & McPhee, B. D. (2012). Cybersecurity policy-making at the local government level: An analysis of threats, preparedness, and bureaucratic roadblocks to success. Journal of Homeland Security and Emergency Management, 9(2). https://doi.org/doi:10.1515/jhsem-2012-0003
9. Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. Computer Science Review, 50, 100592. https://doi.org/https://doi.org/10.1016/j.cosrev.2023.100592
10. Chaudhuri, A., & Bozkus Kahyaoglu, S. (2023). Cybersecurity assurance in smart cities: A risk management perspective. EDPACS, 67(4), 1-22. https://doi.org/10.1080/07366981.2023.2165293
11. D'Amico, G., L'Abbate, P., Liao, W., Yigitcanlar, T., & Ioppolo, G. (2020). Understanding sensor cities: Insights from technology giant company driven smart urbanism practices. Sensors, 20(16), 4391. https://doi.org/10.3390/s20164391
12. David, A., Yigitcanlar, T., Li, R. Y. M., Corchado, J. M., Cheong, P. H., Mossberger, K., & Mehmood, R. (2023). Understanding local government digital technology adoption strategies: A PRISMA review. Sustainability, 15(12), 9645. https://www.mdpi.com/2071-1050/15/12/9645
13. Fielder, A., König, S., Panaousis, E., Schauer, S., & Rass, S. (2018). Risk assessment uncertainties in cybersecurity investments. Games, 9(2), 34. https://www.mdpi.com/2073-4336/9/2/34
14. Frandell, A., & Feeney, M. (2022). Cybersecurity threats in local government: A sociotechnical perspective. The American Review of Public Administration, 52(8), 558-572. https://doi.org/10.1177/02750740221125432
15. Goel, R., Kumar, A., & Haddow, J. (2020). PRISM: A strategic decision framework for cybersecurity risk assessment. Information & Computer Security, 28(4), 591-625. https://doi.org/https://doi.org/10.1108/ICS-11-2018-0131
16. Grobler, M., Gaire, R., & Nepal, S. (2021). User, usage and usability: Redefining human centric cyber security. Frontiers in Big Data, 4. https://doi.org/10.3389/fdata.2021.583723
17. Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustainable Cities and Society, 50, 101660. https://doi.org/https://doi.org/10.1016/j.scs.2019.101660
18. Hamdani, S. W. A., Abbas, H., Janjua, A. R., Shahid, W. B., Amjad, M. F., Malik, J., Murtaza, M. H., Atiquzzaman, M., & Khan, A. W. (2021). Cybersecurity standards in the context of operating system: Practical aspects, analysis, and comparisons. ACM Comput. Surv., 54(3), Article 57. https://doi.org/10.1145/3442480
19. Harknett, R. J., & Stever, J. A. (2011). The new policy world of cybersecurity. Public Administration Review, 71(3), 455-460. https://doi.org/https://doi.org/10.1111/j.1540-6210.2011.02366.x
20. Hatcher, W., Meares, W. L., & Heslen, J. (2020). The cybersecurity of municipalities in the United States: An exploratory survey of policies and practices. Journal of Cyber Policy, 5(2), 302-325. https://doi.org/10.1080/23738871.2020.1792956

21. Ibrahim, A., Valli, C., McAteer, I., & Chaudhry, J. (2018). A security review of local government using NIST CSF: A case study. The Journal of Supercomputing, 74(10), 5171-5186. https://doi.org/10.1007/s11227-018-2479-2
22. Javed, A. R., Shahzad, F., Rehman, S. u., Zikria, Y. B., Razzak, I., Jalil, Z., & Xu, G. (2022). Future smart cities: Requirements, emerging technologies, applications, challenges, and future aspects. Cities, 129, 103794. https://doi.org/https://doi.org/10.1016/j.cities.2022.103794
23. Kalinin, M., Krundyshev, V., & Zegzhda, P. (2021). Cybersecurity risk assessment in smart city infrastructures. Machines, 9(4), Article 78. https://doi.org/10.3390/machines9040078
24. Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 45, 13-24. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2018.10.017
25. Ma, C. (2021). Smart city and cyber-security; technologies used, leading challenges and future recommendations. Energy Reports, 7, 7999-8012. https://doi.org/https://doi.org/10.1016/j.egyr.2021.08.124
26. MacManus, S. A., Caruson, K., & McPhee, B. D. (2013). Cybersecurity at the local government level: Balancing demands for transparency and privacy rights. Journal of Urban Affairs, 35(4), 451-470. https://doi.org/10.1111/j.1467-9906.2012.00640.x
27. Madras. (2020). Cybersecurity policy. City of Madras, Oregon, USA Retrieved from https://www.ci.madras.or.us/sites/default/files/fileattachments/city_council/page/98/g-council_policies-approved_4-27-2021.pdf
28. Micozzi, N., & Yigitcanlar, T. (2022). Understanding smart city policy: Insights from the strategy documents of 52 local governments. Sustainability, 14(16), 10164. https://doi.org/10.3390/su141610164
29. Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. Computers & Security, 120, 102820. https://doi.org/https://doi.org/10.1016/j.cose.2022.102820
30. Möller, D. P. F. (2023). NIST cybersecurity framework and MITRE cybersecurity criteria. In D. P. F. Möller (Ed.), Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices (pp. 231-271). Springer Nature Switzerland. https://doi.org/https://doi.org/10.1007/978-3-031-26845-8_5
31. Morrissey, A., Aslam, K., Goodwin, B., Vikas, R., & Langford-Smith, J. (2021). Cyber security in local government. https://audit.wa.gov.au/reports-and-publications/reports/cyber-security-in-local-government/
32. NIST. (2023). The NIST cybersecurity framework 2.0 - initial public draft. USA: National Institute of Standards and Technology, US Department of Commerce
33. NIST. (2024a). NIST cybersecurity framework 2.0: Resource & overview guide. USA: National Institute of Standards and Technology, US Department of Commerce
34. NIST. (2024b). NIST cybersecurity framework (CSF) 2.0. USA: National Institute of Standards and Technology, US Department of Commerce
35. Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2018). Cybersecurity at the grassroots: American local governments and the challenges of internet security. Journal of Homeland Security and Emergency Management, 15(3), Article 20170048. https://doi.org/10.1515/jhsem-2017-0048
36. Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2019). Cyberattacks at the grass roots: American local governments and the need for high levels of cybersecurity. Public Administration Review, 79(6), 895-904. https://doi.org/10.1111/puar.13028
37. Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2021). Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity. Journal of Urban Affairs, 43(8), 1173-1195. https://doi.org/10.1080/07352166.2020.1727295
38. Norris, D. F., & Mateczun, L. K. (2022). Cyberattacks on local governments 2020: Findings from a key informant survey. Journal of Cyber Policy, 7(3), 294-317. https://doi.org/10.1080/23738871.2023.2178319
39. Norwich. (2020). Cybersecurity policy. Town of Norwich, New York, USA Retrieved from http://norwich.vt.us/wp-content/uploads/2020/03/SB-packet-03-25-20.pdf
40. Nuñez, M., Palmer, X. L., Potter, L., Aliac, C. J., & Velasco, L. C. (2023). ICT security tools and techniques among higher education institutions: A critical review. International Journal of Emerging Technologies in Learning, 18(15), 4-22. https://doi.org/10.3991/ijet.v18i15.40673
41. Öğüt, H., Raghunathan, S., & Menon, N. (2011). Cyber security risk management: Public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. Risk Analysis, 31(3), 497-512. https://doi.org/https://doi.org/10.1111/j.1539-6924.2010.01478.x

42. Patterson, C. M., Nurse, J. R. C., & Franqueira, V. N. L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. Computers & Security, 132, 103309. https://doi.org/https://doi.org/10.1016/j.cose.2023.103309
43. Popescul, D., & Radu, L. D. (2016). Data security in smart cities: Challenges and solutions. Informatica Economica, 20(1), 29-38. https://doi.org/https://doi.org/10.12948/issn14531305/20.1.2016.03
44. Portland. (2023). A resolution authorizing the city of Portland to enact a critical infrastructure cyber security policy. City of Portland, Tennessee, USA Retrieved from https://www.cityofportlandtn.gov/AgendaCenter/ViewFile/Item/865?fileID=2178
45. Preis, B., & Susskind, L. (2022). Municipal cybersecurity: More work needs to be done. Urban Affairs Review, 58(2), 614-629. https://doi.org/10.1177/1078087420973760
46. RBWM. (2020). Cyber security policy. Royal Borough Windsor & Maidenhead, South East England, UK Retrieved from https://www.rbwm.gov.uk/sites/default/files/2020-10/info_sec_cyber_security_policy.pdf
47. Repette, P., Sabatini-Marques, J., Yigitcanlar, T., Sell, D., & Costa, E. (2021). The evolution of city-as-a-platform: Smart urban development governance with collective knowledge-based platform urbanism. Land, 10(1), 33. https://doi.org/10.3390/land10010033
48. Sadik, S., Ahmed, M., Sikos, L. F., & Najmul Islam, A. K. M. (2020). Toward a sustainable cybersecurity ecosystem. Computers, 9(3), 1-17, Article 74. https://doi.org/10.3390/computers9030074
49. Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-driven cybersecurity: An overview, security intelligence modeling and research directions. SN Computer Science, 2(3), 173. https://doi.org/10.1007/s42979-021-00557-0
50. Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. International Cybersecurity Law Review, 3(1), 7-34. https://doi.org/10.1365/s43439-021-00045-4
51. Sharma, K., & Mukhopadhyay, A. (2022). Sarima-based cyber-risk assessment and mitigation model for a smart city's traffic management systems (SCRAM). Journal of Organizational Computing and Electronic Commerce, 32(1), 1-20. https://doi.org/10.1080/10919392.2022.2054259
52. Siudak, R. (2022). Cybersecurity discourses and their policy implications. Journal of Cyber Policy, 7(3), 318-335. https://doi.org/10.1080/23738871.2023.2167607
53. Son, T. H., Weedon, Z., Yigitcanlar, T., Sanchez, T., Corchado, J. M., & Mehmood, R. (2023). Algorithmic urban planning for smart and sustainable development: Systematic review of the literature. Sustainable Cities and Society, 104562. https://doi.org/10.1016/j.scs.2023.104562
54. Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. Future Generation Computer Systems, 92, 178-188. https://doi.org/https://doi.org/10.1016/j.future.2018.09.063
55. Sun, N., Zhang, J., Rimba, P., Gao, S., Zhang, L. Y., & Xiang, Y. (2019). Data-diven cybersecurity incident prediction: A survey. IEEE Communications Surveys & Tutorials, 21(2), 1744-1772. https://doi.org/https://doi.org/10.1109/COMST.2018.2885561
56. Syafrizal, M., Selamat, S., & Zakaria, N. (2020). Analysis of sybersecurity standard and framework components. International Journal of Communication Networks and Information Security, 12, 417-432. https://doi.org/10.17762/ijcnis.v12i3.4817
57. Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview. Electronics, 11(14), 2181. https://www.mdpi.com/2079-9292/11/14/2181
58. Tariq, N., Khan, F. A., & Asim, M. (2021). Security challenges and requirements for smart internet of things applications: A comprehensive analysis. Procedia Computer Science, 191, 425-430. https://doi.org/https://doi.org/10.1016/j.procs.2021.07.053
59. Toh, C. K. (2020). Security for smart cities. IET Smart Cities, 2(2), 95-104. https://doi.org/https://doi.org/10.1049/iet-smc.2020.0001
60. Toussaint, M., Krima, S., & Panetto, H. (2024). Industry 4.0 data security: A cybersecurity frameworks review. Journal of Industrial Information Integration, 100604. https://doi.org/https://doi.org/10.1016/j.jii.2024.100604
61. Ullah, F., Qayyum, S., Thaheem, M. J., Al-Turjman, F., & Sepasgozar, S. M. E. (2021). Risk management in sustainable smart cities governance: A TOE framework. Technological Forecasting and Social Change, 167, 120743. https://doi.org/https://doi.org/10.1016/j.techfore.2021.120743
62. Verhulsdonck, G., Weible, J. L., Helser, S., & Hajduk, N. (2023). Smart cities, playable cities, and cybersecurity: A systematic review. International Journal of Human–Computer Interaction, 39(2), 378-390. https://doi.org/10.1080/10447318.2021.2012381

63. Vitunskaite, M., He, Y., Brandstetter, T., & Janicke, H. (2019). Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. Computers & Security, 83, 313-331. https://doi.org/https://doi.org/10.1016/j.cose.2019.02.009
64. Wolff, J., & Lehr, W. (2018). When cyber threats loom, what can state and local governments do? Georgetown Journal of International Affairs, 19, 67-75. https://doi.org/https://doi.org/10.1353/gia.2018.0008
65. Woodburn. (2021). Cybersecurity policy and procedures. Woodburn, Oregon, USA Retrieved from https://www.woodburn-or.gov/sites/default/files/fileattachments/human_resources/page/13801/cybersecurity_policy.pdf
66. Wu, Y. C., Sun, R., & Wu, Y. J. (2020). Smart city development in Taiwan: From the perspective of the information security policy. Sustainability, 12(7), Article 2916. https://doi.org/10.3390/su12072916
67. Yigitcanlar, T., Agdas, D., & Degirmenci, K. (2023a). Artificial intelligence in local governments: Perceptions of city managers on prospects, constraints and choices. AI & Society, 38(3), 1135-1150. https://doi.org/10.1007/s00146-022-01450-x
68. Yigitcanlar, T., Li, R. Y. M., Beeramoole, P. B., & Paz, A. (2023b). Artificial intelligence in local government services: Public perceptions from Australia and Hong Kong. Government Information Quarterly, 40(3), 101833. https://doi.org/10.1016/j.giq.2023.101833

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.