TAMSAAL
ISSN Print: 3007-5939
ISSN Online: 3007-5947
Volume 4, Number 4, 2026, Pages 176 – 191
Journal Home Page
https://tamsaal.pk/index.php/tamsaal/index

Cyber Resilience Maturity Model for Government Organisations: A Secondary Data Analysis and Outcome-Based Framework

Ibtihajul Islam[1]

[1]*University of Salford, Department of Information Systems Management, Email: ibtihajul@gmail.com*

ARTICLE INFO

Article History:

Received:	*March*	*10, 2026*
Revised:	*April*	*08, 2026*
Accepted:	*April*	*13, 2026*
Available Online:	*April*	*21, 2026*

Keywords:

Cyber resilience; cybersecurity maturity; government organizations; public sector; maturity model; digital government; cybersecurity governance

Corresponding Author:
Ibtihajul Islam
Email:
ibtihajul@gmail.com

DOI: *https://doi.org/10.59075/tamsaal.v4i4.154*

ABSTRACT

Government entities are becoming more reliant on the interconnected digital infrastructure to perform the fundamental government roles, but traditional cybersecurity maturity measurements tend to capture most effectively the implementation of controls rather than the potential to withstand and recover valuable operations in the wake of havoc. The paper builds a Government Cyber Resilience Maturity Model (G-CRMM) based on systematic secondary research. The evidence base incorporates global cybersecurity frameworks, government strategies and assurance efforts, findings of audits by the government in the public sector, various surveys of sector maturity and occurrences, as well as peer-reviewed research published or modified since 2021 and August 2026. Directed content analysis mapped the evidence to the resilience cycle of anticipation, resistance, recovery and adaptation with consideration of government-specific issues such as statutory continuity of services, outdated technology, inter-organisational dependencies, supplier concentration, accountability, cyber workforce capacity and societal trust. Instances of secondary evidence portray ongoing incompatibility of the criticality of public administration with its maturity in cybersecurity. European evidence still has public administration in the risk zone of cybersecurity, and audit outcomes by the UK government show material weaknesses of critical systems, legacy workforce and capacity, and legacy assets. According to the principles of cross-source synthesis, the G-CRMM is characterised by five levels of maturity and eight dimensions: Reactive, Repeatable, Managed, Resilient and Adaptive. It suggests a non-compensatory scoring scheme based on geometric aggregation, and a critical-dimension ceiling that ensures that powerful technical regulations cannot hide critical flaws in mission visibility, governance or recovery capacity. The model adds a public-service-oriented model that relates cybersecurity maturity to operational continuity, collective defence and institutional learning. It offers a falsifiable way by which government organisations can calibrate capabilities, risk-aware target maturity and cyber-resilience funding priorities.

Introduction

Government digitisation has changed how taxation, social protection, healthcare, identity services, justice, and licensing, as well as the coordination of emergencies and other governmental services, are provided. These services are becoming notable due to intricate integrations comprising cloud technology, legacy applications, shared governmental frameworks, third-party suppliers and interconnected information representative environments. The same transformation that facilitates access to more convenient and efficient social institutions thus forms systemic vulnerability to cyber disturbances. However, unlike most private organisations, government agencies are not able to gauge cybersecurity solely by their financial loss or confidentiality of their data due to its long-term disruption, which can impact statutory requirements, the security of the population, democratic practice and the confidence of their citizens. Research conducted by local governments also demonstrates that constraints of budgets, gaps in the staffing system and responsibility fragmentation may prevent the regular implementation of the suggested cybersecurity measures (Norris et al., 2024). These developments in regulation support this service-continuity vision, so the NIS2 Directive clearly connects cybersecurity risk management to incident management, business continuity, supply-chain security and training (European Parliament and Council, 2022).

This exposure can be demonstrated through recent secondary evidence. In 2024, ENISA reported 586 publicly reported cybersecurity incidents to European public administration. Organisations of central government were the ones which recorded the highest number of incidents, at 69.0%, and denial-of-service attacks (DDoS) were the most common, with a number of 60.0%; data breaches were 17.4% (ENISA, 2025b). Even though numerous instances of a denial of service had a short duration of impact, ransomware, data breaches, and attacks on shared systems or service providers posed more potential to interrupt operations on a lasting basis. The bigger ENISA maturity test has kept putting public administration in the cybersecurity risk quadrant, an indication of the absence of a fit in the sectoral criticality and maturity (ENISA, 2025a; ENISA, 2026).

The issue at hand, central to it all, is not cybersecurity itself but cyber resilience. The old classical approach to cybersecurity has been to stop, find, and counter ungoverned activity. Cyber resilience acknowledges that the disruption may not be prevented but rather looks at whether the organisation is able to foresee disruption and how well it may survive its impact, restore its critical operations and adapt to those (Ross et al., 2021; Alhidaifi et al., 2024). This is of particular significance to government since the resilience outcome is the continuation or prompt restoration of the provision of a governmental function.

The concept of maturity models may offer a promising solution for transferring resilience into quantifiable steps of organisational capacity. The models and frameworks that exist, however, have been created to serve other purposes. NIST Cybersecurity Framework offers an opportunity to have a broad risk-management structure, the Zero Trust Maturity Model offered by CISA is specifically related to architecture, the C2M2 tool by the US Department of Energy is concerned with the capabilities of cybersecurity, and the NCSC Cyber Assessment Framework by the UK concentrates on the results that are linked to core functions (CISA, 2023; NIST, 2024; NCSC, 2025; US Department of Energy, 2022). Their respective advantages would not necessarily lead

to a government-specific maturity model that synthesises technical security, institutional governance, endurance of public services, cross-government dependencies and adaptive learning.

Three research questions are discussed, and a maturity architecture is directly based on cross-framework convergence and public-sector evidence. Its major input is the Government Cyber Resilience Maturity Model (G-CRMM), which ties together eight capability dimensions, a five-level maturity architecture and an evidence-based scoring mechanism that avoids overreliance on technical-control compliance. The model not only inquires about the existence of security controls, but it also inquires about whether or not public-service capability can be kept dependable when prevention is no longer possible.

Literature Review

From Cybersecurity to Cyber Resilience

Cyber resilience has emerged as a reaction to the constraints of simply preventive cybersecurity. Tzavara and Vassiliadis (2024) demonstrate that the concept has significantly changed, but remains to be explained inconsistently in terms of both technical and organisational settings. The modern definitions also mostly focus on the ability to predict, endure, heal and adjust to cyber-related negative situations. NIST uses that lifecycle view on a system level, focusing on the survivability and ability to keep serving the mission despite compromise (Ross et al., 2021).

Similarly, Alhidaifi et al. (2024) define cyber resilience as an organisational capability that consists of multiple domains instead of a set of security tools. The significance of this interpretation is that resilience may not work even in instances where the organisation has spent a substantial amount of money on preventive controls. An organisation can have good identity security and vulnerability management and lack tested recovery plans or reliable alternatives to provide important services.

Dupont et al. (2023) also provide that implementation is associated with organisational tensions, such as definitions, operating settings, institutional arrangements and control. Socio-technical alignment is thus needed in resilience. Governance, people, organisational learning and coordination are important too, as well as architecture and security technology. Neri et al. (2026) build on this interpretation by conceptualising organisational cyber resilience by synthesising the literature on organisational resilience and cyber resilience, and Pradana and Ekowati (2024) review in the context of anticipation, coping and adaptation as correlated organisational capabilities. This socio-technical sense is especially applicable to government organisations. The public services can include the interrelating ministries, agencies, local government, critical-infrastructure operators and strategic suppliers. A resilience assessment that only examines an individual network can be deficient in dependencies such that the collapse of one organisation could affect several other organisations.

Cybersecurity Maturity Assessment

Maturity models structure the development in organisations into stages. They are not only about the score but the skills needed to transition the non-uniform practices towards the repeatable, measurable, and constantly improving ones. Effective maturity assessment also entails governance and assurance arrangements that explain who has a role to play in cyber risk instead

of cybersecurity being the mandate of one technical division. This issue aligns with the survey of the Three Lines Model of cybersecurity governance conducted by Valkenburg and Bongiovanni (2024).

The recent literature confirms the growing interest in cybersecurity maturity assessment. In the systematic review of 96 studies (Brezavšček and Baggia, 2025), the finding is that new models continue to be developed, and established frameworks and methodologies to enable maturity assessments are implemented. Sector-specific customisation was one of the huge trends. A maturity model of cybersecurity developed by Bueyuokoza and Guler (2025) following systematic and bibliometric analysis attests to the need to have integrated assessment architectures in place.

A number of powerful working models depict various strategies. C2M2 offers a capability advancement that aims at helping benchmark and making investment choices (US Department of Energy, 2022). The Zero Trust Maturity Model of CISA organises an order of progress around identity, devices, networks, applications and workloads, and data with the help of governance, automation and analytics (CISA, 2023a). Its structure is useful to government agencies, but it is not a complete model of organisational resilience since the core unit of analysis is continuity, institutional learning and recovery of the governmental institutions of the place and its services. The Cross-Sector Cybersecurity Performance Goals developed by CISA offer a complementary baseline of prioritised practices based on which information-security management and continuous improvement may be provided at the organisation level (CISA, 2023b; ISO, 2022).

NIST CSF 2.0 offers six functions: Govern, Identify, Protect, Detect, Respond and Recover. The Govern function ensures that cyber risk aligns with the enterprise decision-making (NIST, 2024). The framework is, however, intentionally result-oriented and not prescriptive, though, and does not offer a government-specific five-level resilience trajectory. The business continuity standards offer a significant additional lens since resilience necessitates an orchestrated recovery post-disturbance, and not mere implementation of control (ISO, 2019). The NIS2 Directive also integrates security risk management with incident management, business continuity, supply-chain security and effectiveness measurement, showing how security requirements and operational resilience requirements are converging (European Parliament and Council, 2022).

Why Government Requires a Specific Resilience Model

Institutional properties in government organisations make it difficult to directly adopt generic maturity models. To begin with, they have large differences in size, ability and resources. Based on interviews in Swedish local administrations, Andreasson et al. (2024) identified significant variations between smaller and larger organisations in their staffing, management support, cybersecurity organisation, and access to information needed to enable cyber situational awareness. Similar public-administration studies define the lack of resources, a low rate of policy implementation and a lack of specialised facilities as the most common limiting factors in local government cybersecurity (Norris et al., 2024).

Second, governments tend to rely on ageing systems which cannot be quickly replaced. Cyber resilience was found to be lower than previously estimated by the UK government by the UK National Audit Office, which also highlighted important gaps in controls, exposure to legacy systems and deficiencies in specialised cyber skills (NAO, 2025). Legacy systems are especially

applicable to resilience since not all risks can be eradicated by substituting them in the short term. Maturity maintenance, compensating controls, service-continuity arrangements and explicit recovery dependencies thus become concerns in themselves.

Third, resilience is becoming more of a group thing. The UK Government Cyber Security Strategy provided the philosophy of defend as one, and the following Government Cyber Action Plan enhanced centralised responsibility, shared services, visibility of risk, reacting and restoration, and professional effectiveness (Cabinet Office, 2022; DSIT, 2026). Government toughness is thus not reducible to the maturity of separate departments. The collapse of shared identity, network, cloud, supplier or data services can spread across boundaries in an organisation.

In the literature, therefore, three types of fragmentation are found. Domain fragmentation takes place when models focus on a certain choice of controls or architectures. Unit-of-analysis fragmentation is when system, organisation, and sector maturity are considered independently. Evidence fragmentation is when the existence of policies or controls is regarded as the same as resilience demonstrated. Recent organisational cyber-resilience work argues in favour of a more comprehensive perspective where technical, human, governance and adaptive capabilities are comprehensively considered (Neri et al., 2026; Sutton and Thompson, 2025). The proposed model is capable of remediating these weaknesses through the integration of organisational capabilities and evidence related to the ongoing provision of key public functions.

Methods

Research Design and Secondary Evidence

The research assumed an organised secondary-data synthesis, which entailed qualitative framework analysis besides the descriptive analysis of published evidence of cybersecurity at the government and sector levels. The secondary strategy was suitable as abundant authoritative data are already available in government audit reports, cyber frameworks, maturity measurements and datasets of public incidents. This was not intended to determine a single population parameter, but rather to seek common capability constructs and test their practicality and applicability against established weaknesses in government cyber resilience.

The priority was given to sources that were published or substantially revised after 31 August 2026 and December 2021, respectively, and ISO 22301:2019 remained a standard on business continuity that is directly related to recovery capacity. The evidence base included four categories: cybersecurity and resilience standards or frameworks, Government implementation and assurance documents, literature of published maturity, incident and audit evidence and peer-reviewed reviews or empirical studies. Official archives were NIST, CISA, the US Department of Energy, NCSC, the UK Government, the UK National Audit Office, ENISA, ISO and EUR-Lex. Inclusion was granted to the NIS2 Directive since the risk-management requirements that are comprehensive address incident response, continuity, security in the supply chain, training and control effectiveness (European Parliament and Council, 2022). There were also vendor maturity models and promotional-only industry reports, which were ignored to curtail commercial bias.

Qualitative observations were left as they were presented by the primary source. Statistical pooling was not attempted since the incidences were of different units, maturity surveys were based on different populations and scales and the government audit was based on different scales and populations. Rather, descriptive numerical evidence was employed to determine whether the capability gaps due to framework analysis were also manifested in public-sector performance and assurance evidence.

Analytical Procedure

The four resilience functions of anticipation, resistance, recovery and adaptation were selected as directed content analysis started work. This was even augmented through coding in which certain themes repeated across distinct entities among the sources were those of the government. When an element was supported by at least three forms of evidence and able to be embodied in terms of observable organisational practice or outcome, it was included in the proposed model.

They were categorised in eight dimensions: governance and accountability; mission, asset and dependency visibility; protective architecture; detection and situational awareness; response, continuity and recovery; ecosystem and supply-chain resilience; workforce and culture; and assurance, learning and adaptation. The concepts of the framework were cross-tabulated in terms of conceptual similarity, government applicability and quantifiability. Some kind of triangulation was then provided by using the public-sector audit and incident findings to further establish whether the dimensions were merely the postulated factors or real weaknesses had been observed.

Five levels of institutionalisation were differentiated to build up the maturity structure. Advancement is towards undocumented and person practices, through standardised management, tested resilience and, lastly, continuously adaptive capability. The design understands that maturity is a measure of how consistent a capability is as opposed to the existence of a single control. The model thus uses testing, quality of evidence and institutional learning as a higher maturation level.

Findings and Analysis

Secondary Evidence of the Government Resilience Gap

Based on the secondary data, high levels of criticality and imbalance in maturity are present in the context of public administration in society. The trend is key as the weakness has not manifested itself within a single technical area. Rather, there is evidence of ineffective aspects of collaboration, legacy technology, staffing, supplier management, independent assurance and recovery-related capabilities.

In the 2024 evaluation, ENISA applied a moderate level of maturity to its evaluation of the public administration. Even though cyber-risk controls were approved by leaders in an estimated 80% of the surveyed organisations, only 60% had supply-chain risk policies, the lowest percentage compared to measured sectors. More importantly, three-quarters of significant government-administration organisations have indicated that they have not participated in collaboration or information-sharing efforts (ENISA, 2025a). The 2026 NIS360 audit of ENISA kept the bodies of administration within the risk zone (ENISA, 2026).

Table 1: Selected secondary indicators informing the G-CRMM

Indicator	Secondary evidence	Resilience implication
Public-administration cyber incidents reported in the EU during 2024	586	Government services experience sustained threat exposure
Incidents involving central governments	69%	National departments and agencies are prominent targets
DDoS share of public-administration incidents	60%	Availability and service continuity require explicit resilience measures
Data breaches	17.4%	Resilience must protect service availability and sensitive public data
Entities not participating in collaboration or information-sharing initiatives	76%	Collective defence and cross-agency learning remain weak
UK critical government IT systems independently assessed by August 2024	58	Independent assurance is feasible at scale
UK legacy IT systems identified	At least 228	Asset lifecycle and legacy exposure are core resilience issues
Legacy systems without fully funded remediation plans	120 of 228	Maturity is constrained by investment and technology debt
Government cyber roles vacant or filled by temporary personnel in 2023-24	Approximately one in three	Workforce maturity affects sustainability of controls

Sources: ENISA (2025a, 2025b); NAO (2025).

This is evidence as to why policy adoption is an inadequate measure of maturity. An organisation can have approved controls by the management but without effective supplier governance, operational coordination or common situational awareness. Another point to note, which was also identified by ENISA, was the difference in the self-assessment of the risk-management capability of entities and the assessments of the risk-management capability by authorities, which added weight to the independent assurance. The interpretation aligns with that of NIS2, which focuses on evaluating the usefulness of risk-management measures, and the governance studies that isolate the operational ownership, oversight, and independent assurance roles (European Parliament and Council, 2022; Valkenburg and Bongiovanni, 2024).

An alternative institutional context in the UK results in the same evidence. NAO found serious gaps in cyber-resilience during its evaluation of 58 independently tested systems in the important government departments and singled out at least 228 legacy systems. About 53% of those legacy assets had no fully funded remediation plans. The workforce was also a significant factor, with about 1/3 of cyber roles being unfilled or being provided by short-term employees in 2023-24 (NAO, 2025).

These results reveal that the interaction between technical and institutional factors defines the government cyber resilience. The presence of weaknesses in asset visibility, investment, staffing or accountability could inhibit the protection technologies from generating consistent service-level resilience. Detecting maturity additionally relies upon the chance to transform threat information into actionable organisational knowledge, an undertaking highlighted in the cyber-threat-intelligence literature (Saeed et al., 2023). Similarly, resilience cannot be complete unless organisations engage in the systematic learning about incidents and convert lessons into transformed practices (Patterson et al., 2024).

Cross-Framework Synthesis

The analysis of key frameworks reveals a good deal of complementarity but also why an integrated government maturity model is still valuable. The key strengths of NIST CSF 2.0 are that it is most effective as an enterprise risk architecture; NIST SP 800-160 Volume 2 demonstrates a highly rigorous, engineering conception of cyber resiliency; NCSC CAF locates the key functions at the core of evaluation; C2M2 provides capability progression; the Zero Trust Maturity Model of CISA provides an evidence-based architecture of rigorously relevant sector-level criticality; and ENISA adds sector-level criticality and maturity evidence. All these contributions are not redundant, and they have other primary functions and work on different levels.

Table 2: Contribution and limitations of major frameworks

Framework	Primary contribution	Limitation when used alone for government resilience maturity
NIST CSF 2.0	Enterprise-wide governance and cybersecurity lifecycle	Not a government-specific maturity ladder
NIST SP 800-160 Vol. 2 Rev. 1	Anticipate, withstand, recover and adapt through resilient engineering	Strong system-engineering orientation
NCSC CAF 4.0	Essential functions, outcome-focused resilience and indicators of good practice	Outcome-assessment architecture rather than a five-stage maturity pathway
CISA Zero Trust Maturity Model 2.0	Progressive security architecture across identity, devices, networks, applications and data	Limited treatment of full organisational continuity and recovery
C2M2 2.1	Structured capability maturity and improvement planning	Not specifically designed around statutory government service delivery
ENISA NIS360	Sector maturity, criticality, ecosystem and institutional capacity	Sector-level assessment rather than individual organisation maturity
UK GovAssure and Government Cyber Action Plan	Independent assurance, accountability, shared services, response, recovery and skills	Implementation architecture rather than a complete maturity scoring instrument

The synthesis indicates that protection and risk management are not as poorly represented within the current approaches. The weaknesses that are government-specific are more prevalent around the areas of mission dependency mapping, legacy exposure, supplier concentration, collective defence, workforce sustainability, independently tested recovery and systematic learning in the organisation. The workforce aspect cannot be boiled down to awareness training due to the fact that cybersecurity culture is reliant on leadership, shared norms, organisational support and visible employee behaviours (Sutton and Thompson, 2025). Likewise, adaptive maturity needs intentional learning, which follows incidents instead of merely backgrounding technical tickets (Patterson et al., 2024).

The NCSC CAF and recent UK government reforms are closest to a whole-of-government resilience view in being driven by starting with the fundamental functions but not the security technologies. Nonetheless, there are still merits in the maturity mechanism that can enable an organisation to describe the extent to which each of the resilience capabilities has developed, as well as whether progress is balanced across dimensions or not. The G-CRMM will deliver that process without supplanting the current control/assurance systems already in use by government.

The Government Cyber Resilience Maturity Model

The resulting G-CRMM contains eight dimensions. The dimensions intentionally combine capability and outcome evidence. For example, the existence of a backup policy contributes little to response and recovery maturity unless recovery is demonstrably tested. Similarly, a supplier-security clause alone does not establish ecosystem maturity unless dependencies are understood and supplier incidents can be coordinated. The model therefore emphasises evidence quality, repeatability and operational demonstration as organisations progress through maturity levels.

Table 3: G-CRMM dimensions and indicative evidence

Dimension	Assessment focus	Illustrative evidence
D1. Governance, risk and accountability	Whether cyber risk is owned as a public-service and enterprise risk	Named accountable executives; risk appetite; board reporting; funded improvement plans; escalation mechanisms
D2. Mission, assets, legacy and dependencies	Whether the organisation understands what must continue and what those services depend upon	Critical-service maps; asset inventories; data classification; legacy registers; recovery priorities; dependency maps
D3. Protective architecture, identity and data	Whether proportionate controls reduce compromise and limit propagation	MFA; privileged access management; segmentation; secure configuration; encryption; vulnerability management; secure-by-design practices
D4. Detection and situational awareness	Whether adverse activity is identified quickly and interpreted in mission context	Central logging; EDR; SIEM; threat intelligence; detection engineering; defined detection

		coverage and escalation thresholds
D5. Incident response, continuity and recovery	Whether essential public services can continue or be restored within accepted tolerances	Incident plans; crisis roles; tested backups; alternate processes; recovery objectives; exercises; crisis communications
D6. Ecosystem, supply chain and collective defence	Whether third-party and cross-government risks are understood and managed	Supplier assurance; dependency concentration analysis; contractual incident requirements; shared intelligence; coordinated exercises
D7. Workforce, leadership and culture	Whether sufficient capability exists to sustain resilience	Workforce planning; role-based competencies; recruitment and retention indicators; leadership training; organisation-wide awareness
D8. Assurance, learning and adaptation	Whether resilience is independently verified and systematically improved	Independent assessments; control testing; post-incident reviews; exercise findings; metrics; remediation closure; investment feedback

Five Maturity Levels

Table 4: G-CRMM maturity levels

Level	Label	Organizational characteristics
1	Reactive	Cyber resilience is fragmented, informal and person-dependent. Critical services and dependencies are incompletely understood. Response is primarily improvised after incidents.
2	Repeatable	Basic controls, inventories and plans exist. Responsibilities are documented, and recurring security activities occur, but coverage and testing are inconsistent.
3	Managed	Governance, service mapping, security controls, monitoring and recovery are standardised and measured. Supplier requirements and workforce responsibilities are systematically managed.
4	Resilient	Critical services are engineered and tested to withstand disruption. Recovery objectives are demonstrated through exercises and technical testing. Independent assurance and cross-government coordination are routine.
5	Adaptive	Resilience continuously adjusts to changing threats, technology and mission dependencies. Intelligence, telemetry, exercises and incident learning directly modify controls, architecture, investment and policy.

One of the critical design principles is that Level 5 should not be the target of all capabilities. The target maturity needs to be chosen based on service criticality, exposure to threats, sensitivity of information and toleration of risk by government organisations. An agency with limited resources or a small-scale government entity can reasonably expect to use mature shared government services as opposed to in-house development. Maturity thus ought to be a term that characterises the sufficiency and institutionalisation of capability in terms of mission requirements rather than the amount of security technology in possession by an organisation.

Scoring and Non-Compensation

The maturity descriptors are used to rate each evidence indicator between 1 and 5. Each dimension has the median of indicator scores in order to decrease distortion by the isolated high-performing controls. In the event of a lack of evidence or its inability to be proved independently, the evaluation should fail to the lower level evidenced as against policy intent.

$$\mathbf{M = \exp[(\Sigma\, w_i \ln D_i) / (\Sigma\, w_i)]}$$

Here, Dx is the maturity score of dimension x, and w x is the approved weight of the dimension. The default should be equal weighting unless other weights are substantiated by mission risk. It is suggested to use geometric as opposed to arithmetic aggregation since cyber resilience has the property of weakest links. A very robust identity architecture can not mathematically cancel the ability to recover important services.

The second is a critical-dimension ceiling. The organisation-level maturity may be no more than one level higher than the lowest maturity (D1 Governance, D2 Mission and Dependencies, D5 Response and Recovery) score. The dimensions reflect executive control, knowledge of what needs to be safeguarded, and the potential to maintain the mission following a disruption. This rule is chosen to ensure that the model is non-compensatory in places where failure may nullify an otherwise good technical profile.

Level 4 and Level 5 claims ought also to seek such evidence in addition to internal policy documents. Appropriate evidence comprises independent assurance, adversarial testing, technical testing, recovery testing, cross-organisation testing, service-level testing and reported closure of incident or exercise conclusions. This need is justified by the fact that research indicates that organisational learning in response to cyber incidents tends to be haphazard unless the concept of reflection, openness and follow-through is institutionalised (Patterson et al., 2024). It also corresponds to the nature of IEEC 27001, which remains on a continuous improvement of its system, and the need by ISO 22301 for a continuity capability monitored and maintained (ISO, 2019, 2022).

Practical Application

The G-CRMM should not substitute but rather supplement established frameworks. Government organisations that implement NIST CSF, CAF, C2M2, and Zero Trust guidance that are already in practice can implement ISO/IEC 27001 or CISA performance goals into the eight dimensions (CISA, 2023a, 2023b; ISO, 2022; NIST, 2024; NCSC, 2025; US Department of Energy, 2022). This interoperability is of significance since government organisations have better chances of

enhancing resilience by making use of available assurance evidence than by developing parallel compliance activities.

The test ought to start with a specific scope of the public service or the organisation. Before scoring maturity, critical services, systems, data, suppliers and dependencies are identified. This ensures that an assessment is not initiated with a technology inventory without paying attention to the outcome of technology which is in the hands of the people. This should be followed by gathering evidence in the form of policies, technical telemetry, assurance findings, incident reporting, exercise reports, supplier assessments, and workforce metrics.

The answers can be employed to build a current profile and target profile. These differences are presented in the form of an investment and remediation roadmap. Notably, the biggest numerical difference must not be prioritised as a matter of course. Remediation must depend on the magnitude of the related public-service impact, presence of exposure and cross-dependency within government.

The central government bodies can combine recurring weaknesses at the portfolio level without the maturity score being viewed as a simplistic ranking of agencies. An illustration of this would be a common low D6 score to request centralised supplier-assurance services, and that low D7 scores might indicate that there is a structural workforce issue that this individual agency cannot overcome by simply competing with other agencies over the same tiny pool of specialists. Likewise, the typical vulnerabilities of D5 have the potential to facilitate shared crisis-management or backup validation and recovery exercise capacities.

This practice aligns with the trend of central risk visibility, shared cyber services, independent assurance and coordinated response that can be found in recent government strategies. It also transforms assessment of maturity on a periodic compliance exercise into an evidence-based resilience governance mechanism. This focus on collective risk aligns with the performance-goal strategy of CISA and the NIS2 mandate of developing coordinated information sharing and risk management across key and critical entities (CISA, 2023b; European Parliament and Council, 2022).

Conclusion

This paper came up with a Government Cyber Resilience Maturity Model by Methodical analysis of the current frameworks, public-sector audit results, maturity benchmarks, evidence of the threats, as well as peer-reviewed studies. Through the analysis, it has been established that government cyber resilience cannot be determined by merely the presence of security policies or technical controls. It should be measured based on the institutional ability to foresee disruption, reduce operational degradation, establish essential services and adjust based on evidence.

According to recent secondary evidence, there have been endemic weaknesses that included legacy systems, workforce capacity in the cyber field, supply-chain management, information sharing and resilience that had been demonstrated on its own. The latter weaknesses are of great significance due to the fact that cyber disruption of government not only causes damage to the performance of the organisation but also to crucial services, public safety, statutory functions and citizen trust.

The G-CRMM is a response that is comprised of eight dimensions, which include governance, mission dependencies, protection, detection, recovery, ecosystems, workforce and adaptive assurance. Its five levels of maturity draw the line between reactive security and the real adaptive resilience. Geometric aggregation and critical-dimension ceiling further dilute the probability of high scores of the chosen areas of technical performance masking gross failures in other areas.

The focal idea of the model is that fully-grown government cybersecurity ought to eventually be exercised in dependable provision and recovery of state functions in the event of unfavourable cyber circumstances. The G-CRMM may be applied together with other existing frameworks like NIST CSF and NCSC CAF to facilitate more consistent assurance, benchmarking and risk-based investment in heterogeneous government organisations. Its predictive validity must now be empirically validated in a variety of national and subnational contexts to better indicate the weighting of its dimensions.

Limitations

The research is reliant on secondary evidence and is therefore limited to the underlying datasets. The publicly available evidence is skewed towards Europe, the United Kingdom and the United States, and the classified government systems and incidents are necessarily underrepresented. There can also be self-assessment bias in maturity surveys; this is shown through differences between organisational and supervisory assessment of surveys conducted by ENISA. Incident datasets can also be underrepresentative of low-visibility incidents and do not form any causal linkages between maturity dimensions and resilience consequences.

The proposed model is yet to be tested prospectively using a sample of national, regional and local government organizations, a representative sample. The synthesis of the content was also done as a single study analytic exercise, instead of a multi-coder validation study. Research in the future must thus utilize Delphi validation, inter-rater reliability and multi-country organization test to measure construct validity, weighting, predictive value and relationship of maturity scores and observed recovery performance.

Declarations

Ethics approval: Not applicable. The study used publicly available secondary information and did not involve human participants or identifiable personal data.

Consent to participate: Not applicable.

Funding: No external funding was received for this study.

Conflict of interest: The author(s) declare no conflict of interest.

Data availability: All data used in the analysis were obtained from publicly accessible documents and sources identified in the reference list.

References

1. Alhidaifi, S.M., Asghar, M.R. and Ansari, I.S. (2024) 'A survey on cyber resilience: Key strategies, research challenges, and future directions', ACM Computing Surveys, 56(8), Article 196. https://doi.org/10.1145/3649218

2. Andreasson, A., Artman, H., Brynielsson, J. and Franke, U. (2024) 'Cybersecurity work at Swedish administrative authorities: taking action or waiting for approval', Cognition, Technology & Work, 26, pp. 709-731. https://doi.org/10.1007/s10111-024-00779-1
3. Bitzer, M., Häckel, B., Leuthe, D., Ott, J., Stahl, B. and Strobel, J. (2023) 'Managing the inevitable: A maturity model to establish incident response management capabilities', Computers & Security, 125, 103050. https://doi.org/10.1016/j.cose.2022.103050
4. Brezavšček, A. and Baggia, A. (2025) 'Recent trends in information and cyber security maturity assessment: A systematic literature review', Systems, 13(1), 52. https://doi.org/10.3390/systems13010052
5. Büyüközkan, G. and Güler, M. (2025) 'Cybersecurity maturity model: Systematic literature review and a proposed model', Technological Forecasting and Social Change, 213, 123996. https://doi.org/10.1016/j.techfore.2025.123996
6. Cabinet Office (2022) Government Cyber Security Strategy: 2022 to 2030. London: UK Government. Accessed 31 August 2026. https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030
7. Cybersecurity and Infrastructure Security Agency (CISA) (2023a) Zero Trust Maturity Model, Version 2.0. Washington, DC: CISA. Accessed 31 August 2026. https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model
8. Cybersecurity and Infrastructure Security Agency (CISA) (2023b) Cross-Sector Cybersecurity Performance Goals. Washington, DC: CISA. Accessed 31 August 2026. https://www.cisa.gov/cybersecurity-performance-goals
9. Department for Science, Innovation and Technology (DSIT) (2026) Government Cyber Action Plan. London: UK Government. Accessed 31 August 2026. https://www.gov.uk/government/publications/government-cyber-action-plan
10. Dupont, B., Shearing, C., Bernier, M. and Leukfeldt, R. (2023) 'The tensions of cyber-resilience: From sensemaking to practice', Computers & Security, 132, 103372. https://doi.org/10.1016/j.cose.2023.103372
11. European Parliament and Council (2022) Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), Official Journal of the European Union, L 333, pp. 80-152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj
12. European Union Agency for Cybersecurity (ENISA) (2025a) ENISA NIS360 2024: Cybersecurity Maturity and Criticality Assessment of NIS2 Sectors. Athens: ENISA. https://doi.org/10.2824/1378797
13. European Union Agency for Cybersecurity (ENISA) (2025b) Sectorial Threat Landscape: Public Administration. Athens: ENISA. Accessed 31 August 2026. https://www.enisa.europa.eu/publications/enisa-sectorial-threat-landscape-public-administration
14. European Union Agency for Cybersecurity (ENISA) (2026) NIS360: The Bigger Picture on Maturity and Criticality of NIS Critical Sectors. Athens: ENISA. Accessed 31 August 2026. https://www.enisa.europa.eu/news/nis360-the-bigger-picture-on-maturity-and-criticality-of-nis-critical-sectors
15. Government Security Group (2026) GovAssure Guidance. London: UK Government Security. Accessed 31 August 2026. https://www.security.gov.uk/policy-and-guidance/govassure/govassure-guidance/

16. International Organization for Standardization (ISO) (2019) ISO 22301:2019 Security and resilience: Business continuity management systems: Requirements. Geneva: ISO. https://www.iso.org/standard/75106.html
17. International Organization for Standardization (ISO) (2022) ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection: Information security management systems: Requirements. Geneva: ISO. https://www.iso.org/standard/27001
18. National Audit Office (NAO) (2025) Government Cyber Resilience. London: National Audit Office. Accessed 31 August 2026. https://www.nao.org.uk/reports/government-cyber-resilience/
19. National Cyber Security Centre (NCSC) (2025) Cyber Assessment Framework, Version 4.0. London: NCSC. Accessed 31 August 2026. https://www.ncsc.gov.uk/collection/cyber-assessment-framework
20. National Institute of Standards and Technology (NIST) (2024) The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29
21. Neri, M., Niccolini, F. and Virili, F. (2026) 'Organizational cyber resilience: toward an integrative conceptual framework', Management Review Quarterly, 76(1), pp. 789-840. https://doi.org/10.1007/s11301-025-00496-7
22. Norris, D.F., Mateczun, L., Hatcher, W., Meares, W.L. and Heslen, J. (2024) 'Local government cyber insecurity: Causes and recommendations for improvement', Public Administration Review, 84(4), pp. 651-659. https://doi.org/10.1111/puar.13743
23. Patterson, C.M., Nurse, J.R.C. and Franqueira, V.N.L. (2024) '"I don't think we're there yet": The practices and challenges of organisational learning from cyber security incidents', Computers & Security, 139, 103699. https://doi.org/10.1016/j.cose.2023.103699
24. Pradana, D.W. and Ekowati, D. (2024) 'Future organizational resilience capability structure: a systematic review, trend and future research directions', Management Research Review, 47(10), pp. 1586-1605. https://doi.org/10.1108/MRR-08-2023-0538
25. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D. and McQuaid, R. (2021) Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST Special Publication 800-160 Volume 2 Revision 1. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2r1
26. Saeed, S., Suayyid, S.A., Al-Ghamdi, M.S., Al-Muhaisen, H. and Almuhaideb, A.M. (2023) 'A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience', Sensors, 23(16), 7273. https://doi.org/10.3390/s23167273
27. Sutton, A. and Tompson, L. (2025) 'Towards a cybersecurity culture-behaviour framework: A rapid evidence review', Computers & Security, 148, 104110. https://doi.org/10.1016/j.cose.2024.104110
28. Tzavara, V. and Vassiliadis, S. (2024) 'Tracing the evolution of cyber resilience: A historical and conceptual review', International Journal of Information Security, 23, pp. 1695-1719. https://doi.org/10.1007/s10207-023-00811-x
29. US Department of Energy (2022) Cybersecurity Capability Maturity Model (C2M2), Version 2.1. Washington, DC: US Department of Energy. Accessed 31 August 2026. https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

30. Valkenburg, B. and Bongiovanni, I. (2024) 'Unravelling the three lines model in cybersecurity: a systematic literature review', Computers & Security, 139, 103708. https://doi.org/10.1016/j.cose.2024.103708