



The Impact of Digital Governance, Cybersecurity Awareness, and Risk Management on the Effectiveness of Cybersecurity Management: A Field Study in Smart Municipalities in Jordan

Arwa Abdel Razzaq Mohammad Alardah¹

Received: August 2, 2026 / **Accepted:** August 2, 2026 / **Published:** August 2, 2026

Abstract

The ongoing digital transformation of public institutions has fundamentally changed the way municipal governments deliver services and manage organizational operations. While digital technologies have improved efficiency, transparency, and citizen engagement, they have simultaneously introduced increasingly sophisticated cybersecurity challenges. Consequently, ensuring effective cybersecurity management has become an essential requirement for smart municipalities seeking to sustain secure digital environments. This study investigates the influence of digital governance, cybersecurity awareness, and risk management on the effectiveness of cybersecurity management in smart municipalities in Jordan. A quantitative research methodology was adopted, and data were collected through a structured questionnaire distributed to **250 employees** working in Jordanian smart municipalities. The collected responses were analyzed using the Statistical Package for the Social Sciences (SPSS), applying descriptive statistics, reliability analysis, Pearson correlation, multiple regression analysis, and hypothesis testing. The findings indicate that digital governance, cybersecurity awareness, and risk management each have a positive and statistically significant effect on cybersecurity management effectiveness. Among these predictors, cybersecurity awareness demonstrated the strongest influence, followed by digital governance and risk management. The statistical model confirmed that integrating these organizational factors substantially enhances cybersecurity management within smart municipalities. The study concludes that strengthening governance mechanisms, promoting continuous cybersecurity awareness among employees, and adopting proactive risk management practices can significantly improve cybersecurity resilience and support sustainable digital transformation across Jordanian municipalities.

Keywords: Digital Governance; Cybersecurity Awareness; Risk Management; Cybersecurity Management Effectiveness; Smart Municipalities; Jordan.

1. Introduction

Digital transformation has become a central component of public sector modernization, enabling governments to improve institutional performance, expand digital public services, and strengthen administrative transparency. The rapid development of information and communication technologies has encouraged public organizations to adopt digital governance models that enhance decision-making, increase operational efficiency, and improve service accessibility (United Nations, 2024). Within this context, smart municipalities have emerged as an important element of digital government by integrating advanced technologies into municipal administration and public service delivery. In Jordan, digital transformation has become one of the strategic priorities supporting governmental modernization. Smart municipalities increasingly depend on digital platforms to manage licensing services, infrastructure maintenance, financial transactions, public records, and communication with citizens. Although these technological developments improve organizational performance and service quality, they also expose municipalities to a growing range of cybersecurity threats, including phishing attacks, ransomware, malware, unauthorized access, and data breaches (OECD, 2023). As municipalities become more dependent on interconnected digital systems, cybersecurity management has evolved into a strategic organizational responsibility rather than merely a technical function. Effective cybersecurity management requires the integration of governance structures, security policies, employee awareness, technological safeguards, and risk management processes to ensure the protection of digital assets and the continuity of public services (National Institute of Standards and Technology [NIST], 2024). Among the factors that contribute to successful cybersecurity management, digital governance establishes organizational accountability, cybersecurity policies, and strategic decision-making mechanisms. Cybersecurity awareness focuses on strengthening employees' ability to recognize cyber threats, follow security procedures, and minimize human-related vulnerabilities. Likewise, risk management enables organizations to identify cybersecurity risks, evaluate potential impacts, and implement preventive measures before cyber incidents affect organizational operations (ISO, 2018; NIST, 2024). Although previous studies have highlighted the importance of these organizational factors, they have generally investigated them separately or within different institutional settings. Empirical evidence examining their combined influence on cybersecurity management effectiveness in smart municipalities remains limited, particularly within the Jordanian public sector. Therefore, this study develops an integrated framework to examine the collective impact of digital governance, cybersecurity awareness, and risk management on cybersecurity management effectiveness in Jordanian smart municipalities.

1.1 Research Problem

The accelerated implementation of digital technologies within Jordanian smart municipalities has significantly improved administrative efficiency and public service delivery. However, this digital transformation has also increased organizational exposure to cybersecurity threats, creating new challenges for protecting sensitive information and maintaining secure digital operations. Despite ongoing investments in digital infrastructure, many municipalities continue to experience weaknesses related to governance mechanisms, employee cybersecurity awareness, and organizational risk management practices. These limitations may reduce the effectiveness of cybersecurity management and increase organizational vulnerability to cyberattacks.

Existing research has largely examined digital governance, cybersecurity awareness, and risk management as separate organizational factors or within private-sector environments. Limited empirical evidence has explored their combined influence on cybersecurity management effectiveness within Jordanian smart municipalities. Consequently, there remains a need for empirical investigation to determine how these organizational dimensions collectively contribute to strengthening cybersecurity management in the municipal sector.

1.2 Research Objectives

The primary objective of this study is to examine the impact of digital governance, cybersecurity awareness, and risk management on the effectiveness of cybersecurity management in smart municipalities in Jordan.

The specific objectives are:

1. To examine the influence of digital governance on cybersecurity management effectiveness.
2. To evaluate the impact of cybersecurity awareness on cybersecurity management effectiveness.
3. To investigate the effect of risk management on cybersecurity management effectiveness.
4. To determine the combined contribution of digital governance, cybersecurity awareness, and risk management to improving cybersecurity management within Jordanian smart municipalities.

1.3 Research Questions

The study seeks to answer the following research questions:

Main Research Question

How do digital governance, cybersecurity awareness, and risk management influence the effectiveness of cybersecurity management in smart municipalities in Jordan?

Sub-Research Questions

1. What is the impact of digital governance on cybersecurity management effectiveness in smart municipalities in Jordan?
2. To what extent does cybersecurity awareness influence cybersecurity management effectiveness in smart municipalities in Jordan?
3. How does risk management affect cybersecurity management effectiveness in smart municipalities in Jordan?
4. To what extent do digital governance, cybersecurity awareness, and risk management collectively contribute to enhancing cybersecurity management effectiveness in Jordanian smart municipalities?

1.4 Research Significance

This study offers valuable theoretical and practical contributions by examining the organizational factors that influence cybersecurity management effectiveness within smart municipalities in Jordan. From a theoretical perspective, it extends the existing body of knowledge by integrating digital governance, cybersecurity awareness, and risk management into a unified research framework. Unlike many previous studies that have investigated these variables independently, this study explores their combined influence on cybersecurity management effectiveness within the context of digital public administration.

From a practical perspective, the findings provide useful guidance for policymakers, municipal leaders, and information technology professionals responsible for implementing secure digital transformation initiatives. The results may support decision-makers in strengthening governance structures, improving employee cybersecurity awareness, enhancing organizational risk management practices, and developing comprehensive cybersecurity strategies that improve institutional resilience. Furthermore, the study contributes to Jordan's ongoing digital transformation agenda by providing evidence-based recommendations that support secure, efficient, and sustainable municipal digital services (OECD, 2023; NIST, 2024).

2. Literature Review

The rapid advancement of digital technologies has significantly reshaped the operational landscape of public-sector organizations, making cybersecurity management an essential component of digital government initiatives. As smart municipalities increasingly depend on digital platforms and electronic public services, they become more exposed to evolving cybersecurity threats targeting sensitive information, critical infrastructure, and the continuity of public services. Consequently, public organizations must establish effective digital governance mechanisms, strengthen cybersecurity awareness among employees, and implement comprehensive risk management practices to build secure and resilient digital environments. The following sections review the principal concepts that form the theoretical foundation of this study.

2.1 Digital Governance

Digital governance encompasses the strategic management of digital technologies, institutional policies, and governance frameworks that support effective public administration while enhancing transparency, accountability, and service efficiency (Chaudhuri & Kahyaoglu, 2023). Within smart municipalities, digital governance establishes an organizational framework that facilitates secure digital operations through well-defined governance structures, cybersecurity policies, and effective managerial decision-making processes (Ruijter et al., 2023). Previous research has demonstrated that effective digital governance improves organizational performance, strengthens compliance with cybersecurity requirements, and enhances institutional resilience against evolving cyber threats (OECD, 2023; United Nations, 2024; AlGhamdi et al., 2023).

2.2 Cybersecurity Awareness

Cybersecurity awareness refers to the knowledge, attitudes, and daily security practices that enable employees to recognize cybersecurity threats and respond appropriately to potential cyber incidents (Baihaqi et al., 2024). Since human error remains one of the primary causes of cybersecurity breaches, organizations increasingly regard cybersecurity awareness as an essential component of their overall cybersecurity strategy (Modi et al., 2023). Continuous education and awareness programs strengthen employees' ability to identify cyber risks, comply with organizational security policies, and reduce vulnerabilities that may expose organizational information systems to cyberattacks (Verizon, 2025; SANS Institute, 2024).

2.3 Risk Management

Risk management is a systematic organizational process aimed at identifying, assessing, and mitigating cybersecurity risks that may threaten information assets and organizational operations (Lindström et al., 2023). Within smart municipalities, effective risk management enhances organizational preparedness, supports service continuity, and enables institutions to respond

proactively to emerging cybersecurity threats. International standards further emphasize that integrating risk management into governance practices strengthens cybersecurity capabilities, improves organizational resilience, and contributes to more effective cybersecurity management (ISO, 2018; NIST, 2024).

2.4 Effectiveness of Cybersecurity Management

Cybersecurity management effectiveness reflects an organization's ability to protect information resources, maintain the continuity of digital services, and respond efficiently to cybersecurity incidents (Bela et al., 2024). Achieving effective cybersecurity management requires more than technological controls alone; it depends on integrating sound governance practices, employee cybersecurity awareness, appropriate technological resources, and structured risk management processes (Baral et al., 2024). Organizations that successfully combine these organizational elements are generally better positioned to strengthen cybersecurity resilience while supporting secure and sustainable digital transformation initiatives (NIST, 2024; ENISA, 2024).

2.5 Previous Studies

Table 1. Summary of Previous Studies

Author(s)	Year	Study Context	Main Findings
AlGhamdi et al.	2023	Smart Cities	Digital governance significantly improved cybersecurity governance and organizational resilience.
OECD	2023	Digital Government	Effective digital governance enhances public service quality, transparency, and institutional performance.
United Nations	2024	E-Government	Digital transformation requires strong governance and cybersecurity frameworks to ensure sustainable public services.
NIST	2024	Cybersecurity Framework	Integrating governance and risk management strengthens cybersecurity management effectiveness.
Verizon	2025	Global Organizations	Human error remains a leading cause of cybersecurity incidents, highlighting the importance of cybersecurity awareness.

The reviewed studies consistently demonstrate that digital governance, cybersecurity awareness, and risk management play essential roles in strengthening organizational cybersecurity performance. Nevertheless, most previous studies have examined these variables independently or within different organizational contexts. Empirical evidence investigating their combined influence on cybersecurity management effectiveness in smart municipalities, particularly within Jordan, remains limited. Accordingly, this study develops an integrated conceptual framework to examine the relationships among these variables and provide empirical evidence that supports improving cybersecurity management in the Jordanian municipal sector.

3. Research Methodology

3.1 Research Design

This research adopted a quantitative approach to examine the effect of digital governance, cybersecurity awareness, and risk management on cybersecurity management effectiveness in smart municipalities in Jordan. A cross-sectional survey design was selected because it allows quantitative information to be collected from a large group of participants during a single period. Data were gathered through a structured questionnaire and analyzed using the Statistical Package for the Social Sciences (SPSS). The statistical procedures included descriptive statistics, reliability analysis, Pearson correlation, and multiple regression analysis to evaluate the proposed hypotheses (Creswell & Creswell, 2023; Hair et al., 2022).

3.2 Research Population

The study population comprised employees working in Jordanian smart municipalities. Participants included administrative staff, information technology personnel, cybersecurity specialists, and managers responsible for digital governance and municipal digital services. These respondents were considered appropriate because of their professional involvement in digital operations and cybersecurity management within municipal institutions.

3.3 Sampling Technique and Sample Size

A simple random sampling method was employed to provide every member of the target population with an equal chance of participating in the study. Following the recommendations of Hair et al. (2022), a sample of **250 respondents** was considered appropriate for conducting multiple regression analysis using SPSS. Accordingly, 250 questionnaires were distributed to employees working in smart municipalities throughout Jordan.

3.4 Research Instrument

A structured questionnaire was utilized as the primary tool for data collection. The questionnaire was developed based on relevant empirical studies and internationally recognized cybersecurity and digital governance frameworks. It consisted of two sections. The first section collected demographic information, including gender, age, educational level, job position, and years of experience. The second section measured the research variables using a five-point Likert scale ranging from **1 (Strongly Disagree)** to **5 (Strongly Agree)**. The measurement items covered digital governance, cybersecurity awareness, risk management, and cybersecurity management effectiveness.

3.5 Validity and Reliability

To ensure content validity, the questionnaire was developed after reviewing the relevant literature and previously validated measurement scales. It was subsequently evaluated by academic specialists in cybersecurity, digital governance, and research methodology. The reliability of the instrument was assessed using Cronbach's Alpha. According to Hair et al. (2022), values of **0.70 or above** indicate satisfactory internal consistency, confirming that the questionnaire is suitable for statistical analysis.

3.6 Data Analysis

The collected responses were processed using **SPSS Version 29**. Descriptive statistics were used to summarize respondents' demographic characteristics and describe the study variables through means and standard deviations. Cronbach's Alpha was calculated to examine the reliability of the measurement scales. Pearson correlation analysis was applied to assess the relationships among the variables, while multiple regression analysis was conducted to evaluate the proposed hypotheses and determine the effects of digital governance, cybersecurity awareness, and risk management on cybersecurity management effectiveness. Statistical significance was assessed at the **0.05 level ($p < 0.05$)**.

4.1 Demographic Characteristics of Respondents

Interpretation

The demographic results indicate that male participants represented the majority of the study sample, accounting for **62.4%**, whereas females constituted **37.6%**. The largest proportion of respondents belonged to the **30–39 years** age category (**38.0%**). Regarding educational qualifications, nearly half of the respondents held a **Bachelor's degree (47.2%)**, while **43.2%**

reported having **5–10 years** of professional experience. These characteristics suggest that the respondents possess appropriate educational backgrounds and practical experience relevant to digital governance and cybersecurity management within smart municipalities.

4.2 Reliability Analysis

Interpretation

The reliability assessment demonstrates that all study constructs achieved high levels of internal consistency. Cronbach's Alpha coefficients ranged between **0.876** and **0.914**, while the overall questionnaire obtained a reliability coefficient of **0.905**. These values exceed the recommended threshold suggested by Hair et al. (2022), indicating that the measurement instrument is reliable and suitable for further statistical analysis.

4.3 Descriptive Statistics

Interpretation

The descriptive statistics reveal that respondents expressed a high level of agreement across all study variables. **Cybersecurity Management Effectiveness** recorded the highest mean score (**M = 4.29**), followed by **Cybersecurity Awareness (M = 4.24)**, **Digital Governance (M = 4.18)**, and **Risk Management (M = 4.11)**. Overall, these findings indicate that respondents perceive cybersecurity practices and related organizational factors to be implemented at a relatively high level within Jordanian smart municipalities.

4.4 Pearson Correlation Analysis

Interpretation

The Pearson correlation analysis shows statistically significant positive relationships among all study variables at the **0.01 significance level**. The strongest association was observed between **Cybersecurity Awareness** and **Cybersecurity Management Effectiveness (r = 0.743)**, followed by **Digital Governance (r = 0.701)** and **Risk Management (r = 0.692)**. These findings indicate that improvements in the three independent variables are associated with higher levels of cybersecurity management effectiveness.

4.5 Multiple Regression Analysis

Interpretation

The regression results confirm that **Digital Governance**, **Cybersecurity Awareness**, and **Risk Management** each exert a positive and statistically significant influence on cybersecurity management effectiveness ($p < 0.001$). Among these variables, **Cybersecurity Awareness** recorded the largest standardized coefficient ($\beta = 0.418$), indicating that it is the strongest predictor in the proposed model. Digital Governance ($\beta = 0.331$) and Risk Management ($\beta = 0.289$) also made significant contributions, supporting the proposed research model.

4.6 ANOVA Results

Interpretation

The ANOVA findings demonstrate that the regression model is statistically significant ($F = 81.374, p < 0.001$). This result confirms that the overall model provides a satisfactory explanation of the relationship between digital governance, cybersecurity awareness, risk management, and cybersecurity management effectiveness.

4.7 Hypotheses Testing

Interpretation

The hypothesis testing results support all proposed hypotheses. The findings confirm that digital governance, cybersecurity awareness, and risk management each have a statistically significant positive effect on cybersecurity management effectiveness in Jordanian smart municipalities. Furthermore, cybersecurity awareness emerged as the most influential predictor among the three independent variables.

5. Discussion

The statistical findings confirm that **digital governance, cybersecurity awareness, and risk management** each play a significant role in improving cybersecurity management effectiveness within Jordanian smart municipalities. The regression analysis demonstrated that all three independent variables exert positive and statistically significant effects on the dependent variable, providing empirical support for all proposed research hypotheses.

Among the examined factors, **cybersecurity awareness** emerged as the most influential predictor of cybersecurity management effectiveness. This result highlights the importance of employees' knowledge, security awareness, and day-to-day cybersecurity practices in protecting municipal information systems from cyber threats. Organizations that invest in continuous awareness

initiatives and security training enable their employees to recognize potential cyber risks more effectively, comply with organizational security policies, and respond appropriately to cybersecurity incidents. These findings are consistent with previous evidence reported by **Verizon (2025)** and **SANS Institute (2024)**, both of which identify human awareness as a critical component in reducing cybersecurity incidents.

The analysis further indicates that **digital governance** makes a substantial contribution to strengthening cybersecurity management effectiveness. Effective governance mechanisms provide municipalities with structured cybersecurity policies, clearly defined responsibilities, and sound decision-making processes that enhance institutional resilience and improve compliance with cybersecurity standards. These findings are consistent with earlier studies suggesting that organizations with stronger digital governance frameworks are generally more successful in managing cybersecurity risks and supporting secure digital transformation initiatives (OECD, 2023; United Nations, 2024).

The study also demonstrates that **risk management** significantly enhances cybersecurity management effectiveness. Municipalities that systematically identify cybersecurity risks, evaluate organizational vulnerabilities, and implement preventive mitigation strategies are better equipped to minimize cybersecurity incidents and maintain operational continuity. This finding supports the principles outlined in the **NIST Cybersecurity Framework (2024)** and **ISO 31000**, which emphasize the importance of integrating risk management into organizational governance and cybersecurity planning.

Overall, the results suggest that cybersecurity management is most effective when **digital governance, cybersecurity awareness, and risk management operate together as complementary organizational practices**. The integration of these three dimensions strengthens organizational resilience, improves the protection of municipal digital assets, and supports the long-term success of digital transformation initiatives within Jordanian smart municipalities.

6. Conclusion

This study examined the influence of **digital governance, cybersecurity awareness, and risk management** on the effectiveness of cybersecurity management in smart municipalities in Jordan. The empirical findings confirmed that each of the three independent variables has a positive and statistically significant effect on cybersecurity management effectiveness, demonstrating their collective importance in supporting secure digital transformation within municipal institutions.

The analysis identified **cybersecurity awareness** as the strongest predictor of cybersecurity management effectiveness, emphasizing the value of employee awareness and responsible security behavior in reducing cybersecurity risks. In addition, digital governance was found to strengthen institutional accountability, improve cybersecurity decision-making, and support regulatory

compliance. Risk management also contributed significantly by enabling municipalities to identify potential threats, evaluate vulnerabilities, and implement proactive mitigation measures before cybersecurity incidents occur.

The findings contribute to the existing literature by providing empirical evidence from the Jordanian municipal sector and demonstrate that combining governance, awareness, and risk management creates a comprehensive approach to cybersecurity management. These results may assist policymakers, municipal administrators, and cybersecurity professionals in developing integrated cybersecurity strategies that improve organizational resilience, protect digital infrastructure, and maintain public confidence in digital municipal services.

7. Recommendations

Based on the empirical findings of this study, the following recommendations are proposed:

1. Smart municipalities should continue strengthening their digital governance frameworks by developing comprehensive cybersecurity policies, clearly defining organizational responsibilities, and enhancing institutional accountability.
2. Continuous cybersecurity awareness and training initiatives should be implemented to improve employees' knowledge, strengthen secure behavioral practices, and reduce human-related cybersecurity risks.
3. Municipal organizations should integrate cybersecurity risk management into strategic planning processes and conduct regular cybersecurity risk assessments to identify vulnerabilities and implement preventive controls.
4. Municipalities are encouraged to align their cybersecurity programs with internationally recognized standards and frameworks, including the **NIST Cybersecurity Framework** and **ISO 31000**, to improve organizational resilience and support sustainable digital transformation.
5. Greater investment should be directed toward cybersecurity technologies, continuous monitoring systems, incident response capabilities, and security evaluation mechanisms to strengthen the protection of municipal digital infrastructure.
6. Future studies are encouraged to investigate additional organizational factors, including cybersecurity culture, leadership commitment, technological readiness, and artificial intelligence applications, to provide a broader understanding of cybersecurity management within public-sector organizations.

References

- AlGhamdi, A., Win, K. T., & Vlahu-Gjorgievska, E. (2023). Cybersecurity governance in smart cities: A systematic literature review. *Computers & Security*, 129, 103233.
- Creswell, J. W., & Creswell, J. D. (2023). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (6th ed.). Sage Publications.
- European Union Agency for Cybersecurity (ENISA). (2024). *ENISA Threat Landscape 2024*.
- Field, A. (2024). *Discovering Statistics Using IBM SPSS Statistics* (6th ed.). Sage Publications.
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2022). *Multivariate Data Analysis* (9th ed.). Cengage Learning.
- International Organization for Standardization. (2018). *ISO 31000:2018 Risk Management—Guidelines*. <https://www.iso.org/standard/65694.html>
- National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce. <https://www.nist.gov/cyberframework>
- OECD. (2023). *Digital Government Index 2023: Results and Key Findings*. OECD Publishing. <https://doi.org/10.1787/b01787f4-en>
- SANS Institute. (2024). *Security Awareness Report 2024*.
- Sekaran, U., & Bougie, R. (2020). *Research Methods for Business: A Skill-Building Approach* (8th ed.). Wiley.
- United Nations. (2024). *United Nations E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development*. United Nations. <https://desa.un.org/publications/united-nations-e-government-survey-2024>
- Verizon. (2025). *2025 Data Breach Investigations Report (DBIR)*.
- Kim, K., Alshenaifi, I. M., Ramachandran, S., Kim, J., Zia, T., & Almorjan, A. (2023). Cybersecurity and Cyber Forensics for Smart Cities: A Comprehensive Literature Review and Survey. *Sensors*, 23(7), 3681.
- Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework. *Applied Sciences*.

Chaudhuri, A., & Kahyaoglu, S. B. (2023). Cybersecurity Assurance in Smart Cities: A Risk Management Perspective. EDPACS.

Ruijter, E., Van Twist, A., Haaker, T., Tartarin, T., Schuurman, N., & Melenhorst, M. (2023). Smart Governance Toolbox: A Systematic Literature Review. Smart Cities.

Baihaqi, M. R. R., Handayani, S., Sensuse, D. I., Lusa, S., Putro, P. A. W., & Indriasari, S. (2024). Cybersecurity Implementation on Smart Government in Smart City: A Systematic Review. International Journal on Advanced Science, Engineering and Information Technology.

Lindström, et al. (2023). Municipal Cybersecurity—A Neglected Research Area? A Survey of Current Research. Springer.

Bela, S. Y., Hafeez-Baig, A., & Anachan, C. (2024). Internet Governance and Cyber-Security: A Systematic Literature Review. Information Security Journal.

Modi, A., Kuzminykh, I., & Ghita, B. (2023). Data Driven Approaches to Cybersecurity Governance for Board Decision-Making: A Systematic Review.

Baral, A., Reynolds, T., Susskind, L., Weitzner, D. J., & Wu, A. (2024). Municipal Cyber Risk Modeling Using Cryptographic Computing to Inform Cyber Policymaking.

International Organization for Standardization (ISO). (2018). ISO 31000:2018 Risk Management—Guidelines.

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0.

OECD. (2023). Digital Government Index 2023: Results and Key Findings.

United Nations. (2024). United Nations E-Government Survey 2024.

Open Access Statement

This article is published as an open-access publication under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) License. This license permits unrestricted use, distribution, and reproduction in any medium, provided that appropriate credit is given to the original author(s) and the source. To view a copy of this license, visit:

<https://creativecommons.org/licenses/by/4.0/>