FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 10 No. 23, December (Special Issue), 2026, pp 22 – 28
DOI: https://doi.org/10.33003/fjs-2026-1023-6564

Development and Evaluation of a Quantitative Framework for Assessing Critical Infrastructure Asset Criticality

***Yashen Yakson Akas and Uche M. Mbanaso**

Center for Cybersecurity Studies, Nasarawa State University, Keffi, Nigeria

*Corresponding authors' email: akasyashen1@gmail.com

Received: 19 Sept. 2026
Accepted: 22 Nov. 2026
Published: 27 Nov. 2026

ABSTRACT
Critical infrastructure assets support essential economic, social, public-health and national-security functions, yet categorical designation alone does not indicate the degree of criticality of individual assets or provide a consistent basis for prioritization. This study presents the Criticality Quantification Assessment Framework (CQAF) and the Mathematical Quantification of Critical Infrastructure Assets Model (MQCIAM), an original integrated approach for assessing, computing, classifying and comparing infrastructure asset criticality. The framework organizes eight conceptual dimensions: geographic and population scope, impact severity, economic impact, dependency and interdependency, public confidence and societal impact, national-security impact, recovery time, and availability of alternatives. Empirical assessment is informed by a 109-item questionnaire, with responses measured on a five-point Likert scale and translated into factor values through the model's assessment procedures. MQCIAM combines normalized factor scores and model-defined weights to produce a criticality index. The index is interpreted through four bands: Negligible (0.00–0.25), Low (0.26–0.55), Moderate (0.56–0.75) and High (0.76–1.00). A Python-based proof-of-concept application operationalizes the workflow, enabling asset-level computation, comparison and recalculation when updated values are entered into the CSV dataset. A supplied fourteen-sector output records three High, two Moderate, seven Low and two Negligible sectors. Industrial and Manufacturing has the highest normalized score (1.0000), while Health Services has the lowest (0.0000) within that dataset. The contribution is an integrated and dynamically updateable criticality assessment and decision-support process; the reported software demonstration should not be mistaken for independent national-scale validation.

Keywords: Critical Infrastructure, Asset Criticality, CQAF, MQCIAM, Criticality Index, Dynamic Classification, Decision Support

INTRODUCTION

Critical infrastructure comprises assets, systems and networks whose disruption can seriously affect national security, economic activity, public health or public safety. Electricity, water, telecommunications, transport, healthcare and financial services are examples of interconnected systems whose operations depend on one another. A disruption in one infrastructure may therefore propagate to other services, producing consequences beyond the initially affected asset (Rinaldi et al., 2001; Grafius et al., 2020).

A persistent challenge in critical infrastructure protection is the distinction between identifying an asset as critical and determining its degree of criticality relative to other assets. Binary designation can obscure differences in consequence severity, geographic reach, service dependencies, recovery time and the availability of alternatives. Research has consequently emphasized the need to account for impact scope, severity and interdependency rather than relying exclusively on categorical lists (Theoharidou et al., 2010; Mbanaso et al., 2019; Kulugh et al., 2022).

Criticality is related to, but distinct from, risk, vulnerability and threat likelihood. In this study, criticality denotes the importance of an asset to essential societal and infrastructure functions, as represented by the consequences and systemic significance of its disruption. Vulnerability refers to weaknesses that may be exploited; threat likelihood concerns the probability of a disruptive event; and risk combines likelihood and consequence. These concepts may inform assessment, but they are not interchangeable. The CQAF/MQCIAM therefore uses the factor definitions and scoring procedures established by the model rather than treating criticality as a generic risk score.

Quantitative assessment can make different dimensions more comparable by translating them into a common index. Research on infrastructure interdependencies demonstrates why an asset's importance cannot always be inferred from its standalone function (Rinaldi et al., 2001; Theoharidou et al., 2010). Other work on systemic criticality and interdependent networks reinforces the need for transparent factor definitions and context-specific assessment (Kruse et al., 2021; Weir et al., 2024). However, the usefulness of a composite index depends on the measurement process, normalization, weights, data quality and interpretation of the resulting score. Quantification of resilience in systems-of-systems also illustrates the need to make aggregation assumptions explicit (Ed-daoui et al., 2018).

This study aims to develop and evaluate a quantitative framework for assessing and prioritizing critical infrastructure assets using measurable criticality factors, mathematical modelling, and computational decision-support tools.

Related Work

Criticality assessment has developed from qualitative designation toward methods that examine the consequences of asset failure and relationships among infrastructure

components. Rinaldi et al. (2001) describe physical, cyber, geographic and logical interdependencies, while Theoharidou et al. (2010) present a multi-layer assessment methodology that considers interdependent infrastructure. These perspectives establish that the significance of an asset may extend beyond its immediate operational role.

Recent studies have examined systemic criticality and network vulnerability. Kruse et al. (2021) discuss systemic criticality as a basis for improving evidence used in critical infrastructure protection. Weir et al. (2024) quantify systemic vulnerability in interdependent infrastructure networks under volcanic hazards. In smart critical infrastructure, Almaleh and Tipper (2022) examine risk-based criticality assessment. Together, these studies support multidimensional assessment while illustrating the importance of distinguishing inherent asset importance from exposure to particular threats.

Quantitative assessment approaches can combine indicators, but the factor definitions, weighting procedure and interpretation must be specific to the model being applied. In CQAF/MQCIAM, the comparison function compares the criticality values computed for infrastructure assets and assigns them to defined criticality bands. It does not compare assessment criteria pairwise; rather, it compares model outputs to support asset-level and cross-sector prioritization.

The contribution of CQAF/MQCIAM is the integration of factor assessment, mathematical computation, four-band classification, asset comparison and a Python proof-of-concept workflow. The framework is intended to make differences in criticality visible and actionable for infrastructure stakeholders.

MATERIALS AND METHODS

Research Design

The study adopts a design-oriented computational modelling approach within a pragmatic, mixed-methods orientation. The research combines a literature-informed conceptualization of criticality factors, empirical questionnaire inputs, mathematical model development and software implementation. The developed artefacts are the CQAF, the MQCIAM and the Python-based application that demonstrates the computation and presentation of assessment results. The software is a proof of concept: it demonstrates the workflow and update capability, but does not by itself establish independent empirical validation or operational deployment at national scale.

CQAF: Conceptual Factors

The CQAF organizes eight conceptual dimensions used to assess the importance and systemic significance of an infrastructure asset. These dimensions are described in Table 1. The questionnaire and model assessment procedures translate responses and other relevant asset information into values for the dimensions. The dimensions are conceptually distinct, although their effects may be related; assessment definitions should therefore be applied consistently to reduce double counting.

Table 1: Conceptual Dimensions Organized by The CQAF

CQAF dimension	Operational meaning
Geographic and population scope	Geographic extent and population affected by loss or degradation of the asset.
Impact severity	Seriousness of consequences, including injury, fatalities, physical damage and essential-service interruption.
Economic impact	Direct and indirect financial consequences, including disruption to production, commerce and economic activity.
Dependency and interdependency	Extent to which the asset relies on other infrastructures and the extent to which other assets or sectors rely on it.
Public confidence and societal impact	Potential effects on public trust, social stability, confidence and societal functioning.
National-security impact	Consequences for defence, national security, emergency coordination and essential governmental functions.
Recovery time	Time required to restore the asset to an acceptable operational state after disruption.
Availability of alternatives	Extent to which substitutes, backup capacity or alternative service routes can maintain the function.

Questionnaire and Measurement

The empirical instrument comprises 109 questions designed to obtain assessment information relevant to infrastructure criticality across the study's infrastructure sectors. Responses are recorded on a five-point Likert scale (1–5). The response values are organized and processed through the model's factor-assessment procedures to determine the relevant impact, dependency, risk and other factor values. The questionnaire is the source of empirical assessment inputs; it is not itself the mathematical model. The 109 figure refers to the number of questionnaire items, were spread over the 14 critical infrastructure assets in relevant departments based on the information required.as shown below:

Table 2: Questionnaire items when spread over relevant departments

Questionnaire	Power and Energy	Water	Information	Science and Technology	Financial Services	Health Services	Public Administration
Q1	3	2	1	5	3	1	4
Q2	4	2	3	5	4	4	5
Q108	1	3	3	3	5	4	0
Q109	0	5	2	2	2	0	3

The questionnaire responses are scored on the five-point scale and processed through the model-defined procedures to derive the factor values used in MQCIAM. The specific item-to-factor coding and any intermediate transformation should be reported with the questionnaire and implementation documentation; no additional response-normalization equation is asserted here.

MQCIAM: Criticality Computation

MQCIAM computes an asset-level Criticality Index by combining the normalized values of the applicable factors with their corresponding model-defined weights. For asset i and factor j, let x_{ij} denote the normalized factor value and w_j the weight assigned to that factor. The weighted aggregation is expressed as follows:

$$CI_i = \sum_{j=1}^{n} W_j * S_{ij} \quad (1)$$

The weights are non-negative model coefficients used to express the contribution of the respective factors. The weighted aggregation produces the asset's computed criticality value. The complete numerical weight vector and its derivation should be reported with the model configuration used for a particular application. In particular, the sector-summary CSV supplied for this article displays explicit weights for Impact (0.25), Dependencies (0.15) and Cyber Risk (0.20), but does not show the complete set of factor weights. These displayed values are reported as dataset fields and are not presented as a complete weight vector for all eight conceptual dimensions.

The model's comparison function operates on the criticality values produced by MQCIAM. It compares assets or sectors on the common criticality scale and classifies them according to the four ranges defined in Section 3.5. The purpose is to establish relative asset criticality and provide a consistent basis for stakeholder prioritization.

Normalization and Four-Band Classification

The model expresses criticality on a normalized scale from 0 to 1 so that the resulting values can be compared and interpreted consistently. For the supplied fourteen-sector summary, the normalized sector values correspond to min–max scaling of the computed Criticality Score values within that dataset:

$$\boldsymbol{N_i = \frac{(CI_i - CI_{min})}{CI_{max} - CI_{min}}} \quad (2)$$

For the supplied dataset, $CI_{min} = \mathbf{21.108805}$ and $CI_{max} = \mathbf{25.520871}$. This dataset-level transformation should be distinguished from the normalization of individual questionnaire responses. Because min–max normalization depends on the comparison set, adding or removing records or changing an observed minimum or maximum can change relative normalized values and may alter quadrant assignments. The four classification intervals used by the model are shown in Table 3.

Table 3: CQAF/MQCIAM Criticality Classification Bands.

Normalized criticality value	Classification	Decision-support interpretation
0.00–0.25	Negligible	Lowest criticality band; lower relative prioritization.
0.26–0.55	Low	Low criticality; monitor and manage proportionately.
0.56–0.75	Moderate	Moderate criticality; consider enhanced attention and mitigation.
0.76–1.00	High	Highest criticality band; prioritize protection and resource allocation.

The classification is intended to guide stakeholder prioritization. It does not mean that an asset in a lower band is unimportant or requires no protection; it indicates its relative position under the assessment data and model configuration applied.

Dynamic Reassessment and Python Implementation

A central feature of CQAF/MQCIAM is that classification is not a permanent label attached to an asset. When an asset's assessment values change and updated values are entered into the CSV dataset, the Python application can rerun the model, recalculate the criticality value and assign the corresponding classification. An asset may therefore move from Low to Moderate or High, or from a higher band to a lower band, as its assessment inputs and computed value change. This dynamic recalculation supports reassessment as asset conditions, dependencies, impacts or other model inputs are updated.

The Python proof-of-concept application operationalizes the data-to-decision workflow: it reads the CSV input, processes factor values and weights, computes criticality values, compares assets, assigns the four classifications and presents the outputs in tables and visualizations. The software demonstrates how updated data can be incorporated without treating previous classifications as fixed. The dynamic update capability should be distinguished from a formal statistical sensitivity experiment: the former recalculates results when input records are updated from a new survey or empirical data, whereas the latter systematically perturbs selected parameters under controlled conditions to quantify output variation.

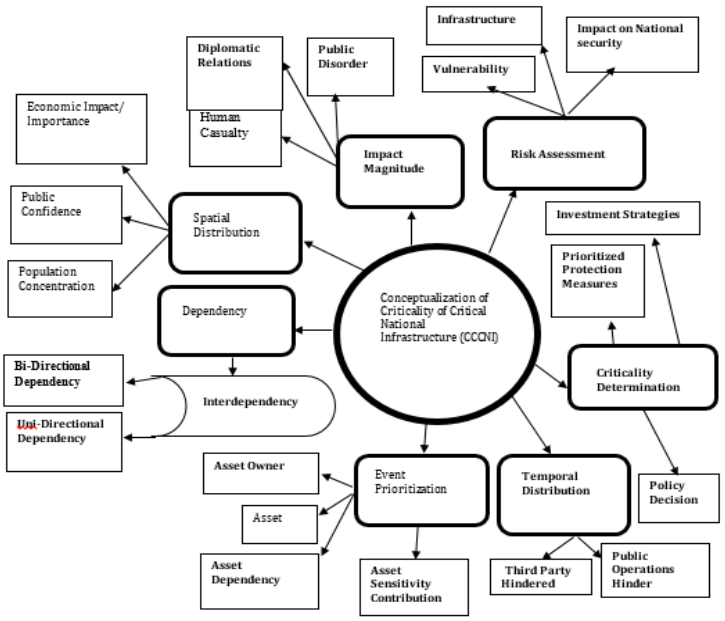

Figure 1: Cqaf/Mqciam End-To-End Workflow: Questionnaire And Asset Data → Factor Assessment → Normalization And Model Weights → Criticality Computation → Asset Comparison → Four-Band Classification → Python Decision-Support Outputs.: (Jafino Et Al., 2020 ; Westhofen Et Al., 2023)

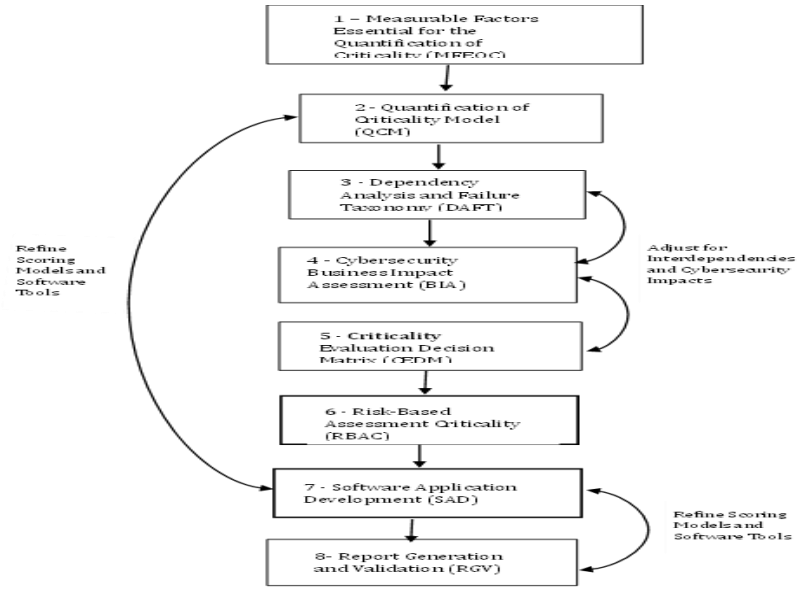

Figure 2: CQAF conceptual framework showing the eight dimensions contributing to infrastructure asset criticality



Figure 3: Python application interface showing CSV input, computed criticality values, asset comparison and classification outputs

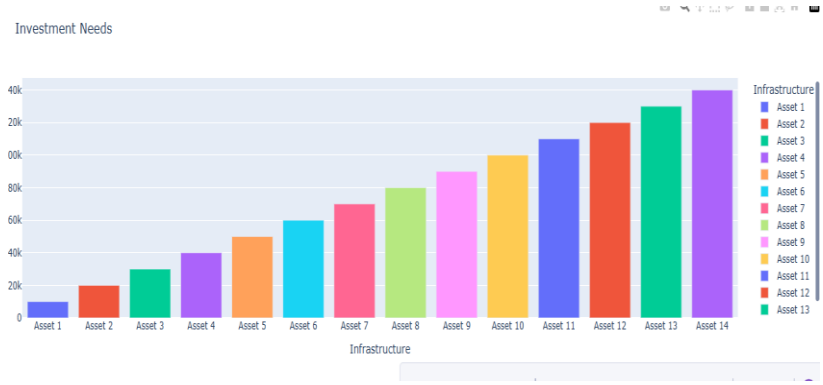

Figure 4: Dynamic classification illustration showing how an updated asset value can change its computed score and criticality band. From the csv table

Evaluation and Evidence Boundaries

The evaluation presented here focuses on computational demonstration and the supplied fourteen-sector output. The thesis describes additional visual analyses, including sensitivity charts and scenario-based illustrations. However, the CSV provided for this article is a single sector-summary snapshot and does not contain repeated parameter-perturbation runs or paired before-and-after scenario values. Accordingly, this article reports the demonstrated ability to recalculate classifications from updated input data as a dynamic software capability, but does not claim numerical sensitivity coefficients or quantified scenario effects that are not present in the supplied output.

The thesis also describes expert review and comparisons with a NIST Cybersecurity Framework-oriented assessment. The materials available for this article do not provide the respondent count, detailed expert profiles, a structured agreement statistic or the complete benchmark dataset. These are therefore treated as supporting development context rather than independent statistical validation. The software prototype demonstrates feasibility of the computational process; external validation across independently sampled assets and sectors remains necessary.

RESULTS AND DISCUSSION

Fourteen-Sector Comparative Output

The Python-generated sector-summary CSV contains fourteen infrastructure-sector records, including raw sector scores, factor-related score fields, selected weight fields, computed Criticality Scores, normalized values and quadrant labels. The normalized values range from 0.0000 to 1.0000. Industrial and Manufacturing has the highest normalized score (1.0000), followed by Safety and Emergency Services (0.9245) and Information (0.8090). Science and Technology (0.6928) and Education (0.6863) are classified as Moderate. Mines and Steel (0.1122) and Health Services (0.0000) are classified as Negligible. The remaining seven sectors are classified as Low.

Table 4: Fourteen-Sector Criticality Summary. Source: Uploaded Python-Generated Sector-Summary CSV

Infrastructure sector	Criticality Score	Normalized score	Classification
Industrial and Manufacturing	25.5209	1.0000	High
Safety and Emergency Services	25.1878	0.9245	High
Information	24.6780	0.8090	High
Science and Technology	24.1653	0.6928	Moderate
Education	24.1370	0.6863	Moderate
Water	23.1738	0.4680	Low
Financial Services	23.1303	0.4582	Low
Power and Energy	23.0094	0.4308	Low
Defence and Security	22.9911	0.4266	Low
Transportation	22.9803	0.4242	Low
Public Administration	22.5570	0.3282	Low
Food and Agriculture	22.4652	0.3074	Low
Mines and Steel	21.6036	0.1122	Negligible
Health Services	21.1088	0.0000	Negligible

The distribution is three High sectors (21.4%), two Moderate sectors (14.3%), seven Low sectors (50.0%) and two Negligible sectors (14.3%). These proportions describe the supplied fourteen-sector dataset. The maximum normalized value identifies the highest observed sector in this comparison set; it should not be interpreted as proof that the sector has reached a universal theoretical maximum of criticality. Likewise, the minimum value identifies the lowest observed sector in this dataset, not an absence of societal importance.

Dynamic Classification as A Decision-Support Output

The four-band output translates computed values into categories that stakeholders can interpret for prioritization. Because the Python application recalculates the index when updated CSV values are supplied, the classification can change when the underlying assessment changes. This supports repeated assessment rather than one-time designation. For example, a sector or asset whose normalized value crosses the 0.55/0.56 boundary moves between Low and Moderate; a value crossing 0.75/0.76 moves between Moderate and High. The software's role is to make such recalculation and reclassification repeatable and visible.

The supplied summary provides one comparative snapshot and does not contain a time series. Therefore, the article demonstrates the classification logic and describes the dynamic update mechanism, but it does not claim to measure longitudinal changes or report a quantified before-and-after case. Such a demonstration can be added when timestamped input and output records are available.

Discussion

The findings illustrate the practical distinction between identifying infrastructure as critical and measuring its degree of criticality. The CQAF provides a structured set of conceptual dimensions, while MQCIAM translates the applicable factor values into a composite index. The four-band classification then communicates the relative criticality of assets in a form that can support stakeholder prioritization. This is consistent with literature emphasizing the consequences of infrastructure disruption and the significance of interdependencies (Rinaldi et al., 2001; Theoharidou et al., 2010; Kruse et al., 2021).

The model's central contribution is its integrated workflow: empirical and asset-level inputs are assessed through the CQAF, processed by MQCIAM, compared on a common criticality scale, classified into four bands and presented through a Python-based decision-support application. The comparison is between computed asset criticality values, not between criteria. This distinction defines the model's operation and its decision-support purpose.

Dynamic reassessment is another practical contribution. An asset's classification is conditional on its current assessment values and the model configuration. When updated values are supplied, the application can recalculate the index and update the classification. This allows stakeholders to identify when a change in impact, dependency, risk or another assessed dimension changes an asset's relative priority. It also means that classifications should be read with their data date, model configuration and comparison set in view. In particular, when min–max normalization is applied across the current dataset, changes in the observed minimum or maximum can alter normalized scores across the comparison set.

The fourteen-sector results provide a concrete example of comparative output. Industrial and Manufacturing, Safety and Emergency Services and Information occupy the three highest normalized positions in the supplied dataset, while Mines and Steel and Health Services occupy the two lowest. The distribution does not establish that all assets within a sector share the same criticality; asset-level assessment remains necessary. Sector-level aggregation is useful for an overview, but should not replace the assessment of individual facilities and services.

Several limitations should guide interpretation. First, the supplied sector summary contains seven named score dimensions and only three explicit weight fields; it does not provide the complete model configuration or a transparent mapping of every CSV column to all eight conceptual CQAF dimensions. Second, the respondent count and respondent profile for the 109-item questionnaire are not documented in the materials available for this article. Third, the supplied CSV is a single snapshot and does not contain the underlying questionnaire response matrix, time-stamped updates, controlled sensitivity perturbations or numerical scenario comparisons. Fourth, the complete weight vector and full factor-specific scoring anchors should accompany future publication or replication. Finally, the additive weighted aggregation does not by itself quantify nonlinear interactions or cascading failures across a full infrastructure network.

These limitations do not negate the demonstrated computational workflow, but they constrain claims about external validity and robustness. Further evaluation should publish the complete questionnaire-to-factor mapping, model configuration, weights, respondent characteristics, asset-level input/output records and independent comparison results. A controlled sensitivity study should vary one or more model parameters systematically and report score and classification changes separately from routine dynamic data updates.

CONCLUSION

This study presents CQAF and MQCIAM as an integrated model for computing, comparing and classifying the criticality of infrastructure assets. The CQAF organizes eight conceptual dimensions, while MQCIAM combines assessed factor values and model-defined weights to produce a criticality index. The index is interpreted through four bands—Negligible, Low, Moderate and High—to guide stakeholder prioritization. The 109-item questionnaire provides empirical assessment inputs measured on a five-point Likert scale. A Python-based proof of concept demonstrates how the model can process CSV data, compute asset criticality, compare outputs and update classifications when assessment values change.

The fourteen-sector output contains three High, two Moderate, seven Low and two Negligible classifications. These results illustrate the model's comparative reporting capability, but the available CSV does not fully document the mapping and weights needed to treat the sector summary as an independent validation of every CQAF dimension. The principal contribution is therefore the integrated and dynamically updateable computational decision-support process. Future work should document the complete model configuration and respondent profile, preserve time-stamped asset records, conduct controlled sensitivity and scenario analyses, and evaluate the framework independently across a broader range of assets and sectors.

REFERENCES

Almaleh, A., & Tipper, D. (2022). Risk-based criticality assessment for smart critical infrastructures. *Infrastructures, 7*(1), Article 3. https://doi.org/10.3390/infrastructures7010003

Ed-daoui, I., Itmi, M., El Hami, A., Hmina, N., & Mazri, T. (2018). A deterministic approach for systems-of-systems resilience quantification. *International Journal of Critical Infrastructures, 14*(1), 80–99. https://doi.org/10.1504/IJCIS.2018.10011743

Grafius, D. R., Varga, L., & Jude, S. (2020). Infrastructure interdependencies: Opportunities from complexity. *Journal of Infrastructure Systems, 26*(4), Article 04020036. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000575

Kruse, P. M., Schmitt, H. C., & Greiving, S. (2021). Systemic criticality a new assessment concept improving the evidence basis for CI protection. *Climatic Change, 165*, Article 2. https://doi.org/10.1007/s10584-021-03019-x

Kulugh, V. E., Mbanaso, U. M., & Chukwudebe, G. (2022). Cybersecurity resilience maturity assessment model for critical national information infrastructure. *SN Computer Science, 3*(3), Article 217. https://doi.org/10.1007/s42979-022-01108-x

Mbanaso, U. M., Kulugh, V. E., Musa, H., & Aimufua, G. I. O. (2019). Conceptual framework for the assessment of the degree of dependency of critical national infrastructure on ICT in Nigeria. In *2019 15th International Conference on Electronics, Computer and Computation (ICECCO)*. https://doi.org/10.1109/ICECCO48375.2019.9043230

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine, 21*(6), 11–25. https://doi.org/10.1109/37.969131

Theoharidou, M., Kotzanikolaou, P., & Gritzalis, D. (2010). A multi-layer criticality assessment methodology based on interdependencies. *Computers & Security, 29*(6), 643–658. https://doi.org/10.1016/j.cose.2010.02.003

Weir, A. M., Wilson, T. M., Bebbington, M. S., Campbell-Smart, C., Williams, J. H., & Fairclough, R. (2024). Quantifying systemic vulnerability of interdependent critical infrastructure networks: A case study for volcanic hazards. *International Journal of Disaster Risk Reduction, 114*, Article 104997. https://doi.org/10.1016/j.ijdrr.2024.104997

©2026 This is an Open Access article distributed under the terms of the Creative Commons Attribution 4.0 International license viewed via https://creativecommons.org/licenses/by/4.0/ which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is cited appropriately.