Eastern European
Journal of Regional Studies
ISSN: 2537-6179; ISSN-L: 1857-436X

Volume 12 / Issue 1/ June 2026
https://doi.org/10.53486/2537-6179.12-1.06

MATHEMATICAL MODEL FOR ASSESSING CYBERSECURITY LEVEL IN CRITICAL CIVILIAN INFORMATION INFRASTRUCTURES: HEALTHCARE, ENERGY AND EDUCATION

Fiodor TIMERCAN*[1]

Abstract: *This paper develops and clarifies a mathematical model for assessing the cybersecurity level of critical civilian information infrastructures in healthcare, energy and education. The objective is to provide a transparent and reproducible composite index that can support institutional diagnosis, cross-sector comparison and regional policy prioritization. The model integrates three normalized dimensions: threat exposure, control effectiveness and operational resilience. Threat exposure is estimated from likelihood and impact indicators and transformed through a bounded calibration function; control effectiveness is derived from implementation and validated operational performance of security controls; and resilience is calculated from recovery and response indicators. The final cybersecurity score is expressed within the interval [0,1] through an explicit weighted aggregation formula. The article also explains the normalization logic, calibration parameter, sector-specific weighting and reproducibility conditions of the model. Because access to institutional cybersecurity datasets is limited, the application presented in this paper is illustrative and hypothetical rather than empirical. To address this limitation, the paper provides complete input tables, intermediate calculations and a sensitivity analysis showing how the final score changes under alternative weighting scenarios. The proposed framework contributes an integrated evaluation logic that links cybersecurity risk assessment, security control maturity and operational continuity into a single policy-oriented metric.*

Keywords: *cybersecurity assessment; critical civilian infrastructure; mathematical model; composite index; threat exposure; control effectiveness; operational resilience; healthcare; energy; education; NIS2.*

Classification JEL: *O3*

UDC: *[004.056.5:330.4]:[338.49:351.84]*

Introduction

Critical civilian information infrastructures constitute essential components of contemporary socio-economic systems. Healthcare institutions rely on digital platforms for patient records, diagnostics, laboratory services, treatment coordination and continuity of care. Energy systems depend on interconnected operational technologies and information systems to maintain stability, safety and uninterrupted supply. Education systems increasingly operate through digital learning environments, administrative platforms and data management services. For regional economies, the continuity of these sectors is not only a technical issue but also a condition for social trust, public welfare and institutional resilience.

The progressive digitalization of civilian infrastructures has expanded their exposure to cyber threats. Ransomware, insider misuse, supply-chain compromise, distributed denial-of-service attacks and exploitation of poorly segmented networks may generate cascading consequences: service disruption, financial losses, compromised data integrity, safety risks and erosion of public confidence. These risks are particularly relevant for regions where

*[1] *PhD Candidate, Head of the Department of Communications and Informatics, "Alexandru cel Bun" Armed Forces Military Academy, timercantudor@yahoo.com, https://orcid.org/0009-0001-6769-3556*

Received: 26.02.2026 Accepted: 29.06.2026 https://csei.ase.md/journal

institutions operate under budgetary constraints, uneven digital maturity and dependence on external technology providers.

From a regulatory perspective, the European cybersecurity agenda has moved from general information security governance toward sectoral resilience and supervision of essential and important entities. The NIS2 Directive enlarges the scope of cybersecurity obligations across essential services, while the Critical Entities Resilience Directive emphasizes continuity and resilience of critical functions. For countries and regions aligned with European policy frameworks, including Eastern European systems, this creates a need for assessment instruments that are comparable, measurable and adaptable to sector-specific realities.

Despite the strategic importance of cybersecurity, assessment within civilian critical infrastructures remains methodologically fragmented. Existing instruments are frequently based on qualitative maturity models, compliance checklists, risk matrices or sector-specific audits. These instruments provide useful guidance, but they often evaluate exposure, control effectiveness and resilience separately. As a result, decision-makers may receive several partial indicators without a unified mathematical score that supports benchmarking across institutions, sectors or regions.

The research gap addressed in this paper is therefore the absence of a transparent quantitative model that integrates three dimensions of cybersecurity level: exposure to threats, effectiveness of implemented controls and operational resilience after an incident. The aim of the paper is to construct and illustrate a normalized composite cybersecurity index suitable for critical civilian information infrastructures.

The study is guided by the following research questions:

- RQ1 - How can threat exposure, control effectiveness and operational resilience be expressed in a common normalized structure?
- RQ2 - How can these dimensions be aggregated without losing sector-specific adaptability?
- RQ3 - How sensitive is the resulting score to changes in weighting assumptions?

The expected contribution is threefold. First, the paper proposes an explicit mathematical aggregation logic with all variables, coefficients and calibration parameters defined. Second, it connects the model to existing cybersecurity standards, risk assessment approaches and composite indicator methodology. Third, it provides a reproducible illustrative application, including input values, intermediate calculations and sensitivity analysis. The application is hypothetical and does not claim empirical validation; rather, it demonstrates the internal logic and practical usability of the model and establishes a basis for future empirical calibration.

Literature Review and Positioning of the Model

Cybersecurity assessment in critical infrastructures is influenced by three major analytical traditions: security control frameworks, risk assessment methods and composite

Volume 12 / Issue 1/ June 2026
https://doi.org/10.53486/2537-6179.12-1.06

indicator methodology. The model proposed in this paper is positioned at the intersection of these traditions, but it does not replace them. Its purpose is to translate their complementary logic into a reproducible index suitable for institutional and regional comparison.

Control-oriented frameworks provide the normative foundation for cybersecurity governance. The NIST Cybersecurity Framework 2.0 offers a taxonomy of outcomes for governing, identifying, protecting, detecting, responding to and recovering from cybersecurity risks (NIST, 2024). ISO/IEC 27001:2022 defines requirements for establishing and continuously improving an information security management system (ISO, 2022). IEC 62443 is especially relevant for industrial automation and operational technology environments, which are essential for energy systems (IEC, 2018). These standards help identify what domains and controls should be assessed, but they do not by themselves generate a single comparable mathematical score across healthcare, energy and education infrastructures.

Risk assessment literature contributes the logic of threat likelihood, vulnerability and impact. NIST SP 800-30 Rev. 1 conceptualizes risk assessment through threat sources, threat events, vulnerabilities, likelihood and impact (NIST, 2012). Böhme, Laube and Riek (2019) show that information security risk assessment methods vary substantially in assumptions, inputs and levels of quantification. This literature supports the model's exposure component, where threat scenarios are translated into a cumulative exposure index. However, risk alone is insufficient because a high-risk environment may still be well defended if controls and recovery mechanisms are effective.

Maturity and compliance assessment frameworks are particularly relevant for critical infrastructure governance. Drivas et al. (2020) proposed a cybersecurity maturity assessment framework aligned with the NIS Directive for operators of essential services. Such approaches are useful for supervisory practice, but they often remain domain-specific or compliance-oriented. The present model differs by integrating exposure, control effectiveness and operational resilience into one composite score, while allowing the domains and weights to be adjusted by sector.

The regulatory and regional relevance of the model is strengthened by the NIS2 Directive, which requires stronger cybersecurity governance, risk management and incident reporting for essential and important entities (European Parliament and Council of the European Union, 2022). ENISA's recent sectoral work also highlights the need to understand the maturity and criticality of NIS2 sectors and to support cybersecurity stress testing and resilience planning (ENISA, 2025, 2026). Healthcare is a particularly exposed sector because ENISA's health threat landscape identifies ransomware, data breaches and service disruption as central risks (ENISA, 2023). Energy infrastructures require special attention because operational technology security and continuity constraints create a different risk profile from ordinary IT systems. Education infrastructures also present distinctive risks due to open networks, distributed users, valuable personal and research data and dependence on third-party platforms (Lallie et al., 2023).

Eastern European
Journal of Regional Studies
ISSN: 2537-6179; ISSN-L: 1857-436X
Volume 12 / Issue 1/ June 2026
https://doi.org/10.53486/2537-6179.12-1.06

Composite indicator methodology offers the aggregation logic required for regional and cross-sector benchmarking. The OECD and Joint Research Centre handbook emphasises normalization, weighting, aggregation and sensitivity analysis as essential steps in building composite indicators (OECD & JRC, 2008). Sensitivity analysis is also a standard method for testing whether conclusions remain stable when assumptions change (Saltelli et al., 2008). This literature directly informs the proposed use of normalized indicators, explicit weights and scenario-based sensitivity testing.

The originality of the proposed model is not the introduction of a completely new cybersecurity standard, but the integration of existing assessment logics into a single reproducible mathematical structure. In contrast to approaches that separately report risk exposure, compliance maturity or recovery capability, the model expresses cybersecurity level as the interaction between (1) the external and internal threat environment, (2) the effectiveness of implemented controls and (3) the ability to sustain or restore essential functions. This makes the model suitable for institutional self-assessment, regional policy comparison and prioritisation of cybersecurity investments.

Table 1. Positioning of the proposed model in relation to existing approaches

Approach	Main contribution	Limitation addressed by the proposed model
NIST CSF 2.0 / ISO/IEC 27001	Structured governance and control domains	No single sector-comparable mathematical index
Risk assessment methods	Likelihood-impact logic and scenario prioritisation	Often asset- or scenario-level; limited aggregation of controls and resilience
Cybersecurity maturity models	Institutional diagnosis and compliance monitoring	May remain qualitative or compliance-centred
Composite indicators	Normalization, weighting, aggregation and benchmarking	Require domain-specific cybersecurity variables
Proposed model	Integrates exposure, controls and resilience into one score	Requires empirical calibration in future applications

***Source**: elaborated by the author*

Methodology

The model conceptualizes cybersecurity level as a composite function of three measurable components: threat exposure, control effectiveness and operational resilience. To avoid notation ambiguity, operational resilience is denoted by O, while Rraw denotes aggregated raw risk. The symbol λ is used exclusively as the exposure calibration parameter.

Let S represent the overall cybersecurity level of an assessed institution or sector. S is bounded within the interval [0,1], where values closer to 1 indicate a higher assessed

Eastern European
Journal of Regional Studies
ISSN: 2537-6179; ISSN-L: 1857-436X
Volume 12 / Issue 1/ June 2026
https://doi.org/10.53486/2537-6179.12-1.06

cybersecurity level under the defined model assumptions. The model uses the following aggregation formula:

$$S = \alpha U + \beta O + \gamma(1 - E), \quad \alpha, \beta, \gamma \geq 0, \quad \alpha + \beta + \gamma = 1 \qquad (1)$$

where U is the Control Effectiveness Index, O is the Operational Resilience Index, E is the Threat Exposure Index, and α, β and γ are aggregation weights. The term (1 - E) transforms exposure into an exposure-resistance component, ensuring that higher exposure reduces the final score while preserving the [0,1] interval. This formulation avoids the possibility of negative scores that could occur if exposure were subtracted directly.

Normalization principles

All input indicators are normalized before aggregation. For benefit indicators, where higher values indicate a better cybersecurity condition, min-max normalization may be expressed as:

$$x'_i = (x_i - x\ \min) / (x\ \max - x\ \min) \qquad (2)$$

For cost indicators, where lower values indicate better performance, such as mean time to detect or mean time to recover, the inverse form may be used:

$$x'_i = (x\ \max - x_i) / (x\ \max - x\ \min) \qquad (3)$$

In practical institutional assessments, normalization thresholds may be derived from regulatory requirements, sectoral benchmarks, expert judgement or historical performance data. For illustrative purposes, the present paper uses normalized values directly and reports them transparently in the calculation tables.

Threat Exposure Index

Let T = {t1, t2, ..., tn} denote the set of relevant cyber threat scenarios applicable to the assessed sector. For each threat scenario ti, two normalized parameters are estimated: ρi ∈ [0,1], representing likelihood within the assessment period, and Ii ∈ [0,1], representing normalized impact.

Impact may be decomposed into confidentiality, integrity, availability, safety, financial and reputational consequences. If v(i,l) denotes the normalized impact value of threat i on consequence category l and c(l) is the category weight, then:

$$I(i) = c(1)*v(i,1) + c(2)*v(i,2) + ... + c(m)*v(i,m),\ \text{sum}\ c(l) = 1 \qquad (4)$$

Aggregated raw risk is calculated as the sum of likelihood-impact products:

$$Rraw = rho(1)*I(1) + rho(2)*I(2) + ... + rho(n)*I(n) \qquad (5)$$

Because Rraw may increase with the number of scenarios, it is transformed into a bounded Threat Exposure Index:

$$E = 1 - \exp[-lambda * Rraw], \quad lambda > 0 \qquad (6)$$

Eastern European
Journal of Regional Studies
ISSN: 2537-6179; ISSN-L: 1857-436X
Volume 12 / Issue 1/ June 2026
https://doi.org/10.53486/2537-6179.12-1.06

The calibration parameter λ controls the sensitivity of the exposure function. A practical calibration rule is λ = ln(2) / R*, where R* is the reference raw-risk level at which exposure should reach 0.5. If empirical incident data are unavailable, λ can be set through expert judgement and then tested through sensitivity analysis. In this paper, λ is used only for exposure calibration and not as an aggregation weight.

Control Effectiveness Index

Control effectiveness reflects the extent to which security measures are both implemented and operationally effective. Let the cybersecurity programme be divided into K control domains, such as governance, access control, monitoring, incident response, asset management, network segmentation and backup/recovery. For each control j in domain k, define mkj ∈ [0,1] as implementation level, ekj ∈ [0,1] as operational effectiveness and wkj as the within-domain control weight.

$$C(k) = w(k,1)*m(k,1)*e(k,1) + ... + w(k,p)*m(k,p)*e(k,p), \quad \text{sum } w(k,j) = 1 \qquad (7)$$

The overall Control Effectiveness Index is then calculated by aggregating domain-level effectiveness scores:

$$U = W(1)*C(1) + W(2)*C(2) + ... + W(K)*C(K),$$

$$\text{sum } W(k) = 1 \qquad (8)$$

This structure distinguishes between the presence of a control and its tested performance. For example, a backup system that exists but is not regularly restored during tests will receive a lower effectiveness score than a backup system whose recovery capability is validated.

Operational Resilience Index

Operational resilience measures the capacity of the institution to maintain or restore essential services after a cyber incident. Let o_s ∈ [0,1] represent normalized resilience indicators and θ_s their weights. Examples include RTO compliance, RPO compliance, backup restoration success, incident detection timeliness, incident response timeliness and continuity-plan testing.

$$O = \text{theta}(1)*o(1) + \text{theta}(2)*o(2) + ... + \text{theta}(q)*o(q),$$

$$\text{sum theta}(s) = 1 \qquad (9)$$

Weights may differ by sector. Energy systems may place greater emphasis on continuity and recovery time; healthcare institutions may prioritise data integrity, patient safety and restoration reliability; education institutions may emphasise identity management, endpoint protection and learning-platform continuity. Sectoral weights should be documented and justified by regulatory priorities, expert panels, historical incident data or institutional risk appetite.

Eastern European Journal of Regional Studies
ISSN: 2537-6179; ISSN-L: 1857-436X
Volume 12 / Issue 1/ June 2026
https://doi.org/10.53486/2537-6179.12-1.06

Table 2. Illustrative sector-specific aggregation weights

Sector	α controls	β resilience	γ exposure resistance	Justification
Healthcare	0.35	0.35	0.30	Balanced controls and resilience because service continuity and data integrity are both critical.
Energy	0.30	0.40	0.30	Higher resilience weight because operational continuity and recovery speed are decisive.
Education	0.45	0.25	0.30	Higher control weight due to access management, endpoint protection and platform governance needs.
Baseline illustrative case	0.40	0.30	0.30	Used for reproducible demonstration and tested through sensitivity analysis.

***Source**: elaborated by the author*

Illustrative Application and Sensitivity Analysis

This section demonstrates the internal logic of the model using hypothetical but plausible values for a civilian healthcare infrastructure. The calculation is illustrative rather than empirical. Its purpose is to show how the model can be reproduced, audited and adapted when institutional data become available.

The hypothetical institution is assessed against four threat scenarios: ransomware, insider misuse, third-party compromise and distributed denial-of-service attack. The normalized likelihood and impact values are shown in Table 3.

Table 3. Hypothetical threat exposure inputs

Threat scenario	Likelihood ρ_i	Impact I_i	$\rho_i \times I_i$
Ransomware	0.70	0.90	0.630
Insider misuse	0.40	0.60	0.240
Third-party compromise	0.50	0.80	0.400
DDoS attack	0.35	0.55	0.193

***Source**: elaborated by the author*

Using Equation (5), aggregated raw risk is:

$$R_{raw} = 0.630 + 0.240 + 0.400 + 0.193 = 1.462 \quad (5)$$

With $\lambda = 0.5$, Equation (6) gives:

$$E = 1 - \exp(-0.5 \times 1.462) = 0.519 \quad (6)$$

Eastern European Journal of Regional Studies
ISSN: 2537-6179; ISSN-L: 1857-436X
Volume 12 / Issue 1 / June 2026
https://doi.org/10.53486/2537-6179.12-1.06

Table 4. Hypothetical control effectiveness calculation

Control domain	Domain score C_k	Domain weight W_k	Weighted contribution
Governance and risk management	0.70	0.20	0.140
Identity and access control	0.75	0.25	0.188
Monitoring and detection	0.65	0.20	0.130
Incident response	0.70	0.20	0.140
Backup and recovery controls	0.80	0.15	0.120

***Source**: elaborated by the author*

Using Equation (8),

$$U = 0.140 + 0.188 + 0.130 + 0.140 + 0.120 = 0.718.$$

Table 5. Hypothetical operational resilience calculation

Resilience indicator	Normalized score o_s	Weight θ_s	Weighted contribution
RTO compliance	0.75	0.30	0.225
RPO compliance	0.80	0.25	0.200
Backup restoration success	0.70	0.25	0.175
Detection and response timeliness	0.65	0.20	0.130

***Source**: elaborated by the author*

Using Equation (9),

$$O = 0.225 + 0.200 + 0.175 + 0.130 = 0.730 \quad (9)$$

Table 6. Intermediate model values

Component	Symbol	Value	Interpretation
Control Effectiveness Index	U	0.718	Positive contribution
Operational Resilience Index	O	0.730	Positive contribution
Threat Exposure Index	E	0.519	Penalized through 1 - E
Exposure-resistance component	1 - E	0.481	Positive value decreases when exposure increases

***Source**: elaborated by the author*

For the baseline illustrative aggregation weights $\alpha = 0.40$, $\beta = 0.30$ and $\gamma = 0.30$, the final score is calculated as follows:

$$S = 0.40 \times 0.718 + 0.30 \times 0.730 + 0.30 \times (1 - 0.519) = 0.651 \quad (10)$$

The resulting value indicates a moderate cybersecurity level. The institution benefits from relatively solid control and resilience scores, but the final index is limited by accumulated threat exposure. The calculation also shows why exposure should not be interpreted in isolation: high exposure does not automatically imply low cybersecurity if compensating controls and recovery capabilities are strong.

Received: 26.02.2026 Accepted: 29.06.2026 https://csei.ase.md/journal

Eastern European
Journal of Regional Studies
ISSN: 2537-6179; ISSN-L: 1857-436X
Volume 12 / Issue 1/ June 2026
https://doi.org/10.53486/2537-6179.12-1.06

Table 7. Sensitivity analysis under alternative weighting scenarios

Scenario	α	β	γ	S	Interpretation
Baseline	0.40	0.30	0.30	0.651	Balanced emphasis
Control-centred	0.50	0.25	0.25	0.662	Higher priority for implemented controls
Resilience-centred	0.30	0.50	0.20	0.677	Higher priority for continuity and recovery
Exposure-sensitive	0.30	0.25	0.45	0.614	Higher penalty for threat exposure

***Source**: elaborated by the author*

The sensitivity analysis indicates that the final score remains within a relatively narrow interval, from 0.614 to 0.677, under the tested weighting scenarios. The ranking of the cybersecurity condition remains moderate across scenarios, which suggests that the illustrative result is not entirely dependent on a single weighting assumption. However, the exposure-sensitive scenario produces the lowest score, confirming that the model reacts logically when accumulated threat exposure receives higher importance. In empirical applications, such sensitivity testing should be complemented with expert validation, sector benchmarks and institutional data.

Discussion

The proposed model responds to the need for a cybersecurity assessment structure that is quantitative, reproducible and adaptable to sector-specific realities. Its main advantage is the integration of three components that are often assessed separately: threat exposure, control effectiveness and operational resilience. This integrated structure allows decision-makers to identify whether a low final score is caused mainly by high exposure, weak controls, limited recovery capacity or a combination of these factors.

The model also supports regional studies by enabling comparison across institutions and sectors using a common normalized scale. This is relevant for regional cybersecurity planning because healthcare, energy and education infrastructures may compete for limited investment resources while facing different risk profiles. A common index can support prioritisation, but it should not replace qualitative expert judgement or sector-specific audits.

Compared with compliance-based assessments, the model gives more explicit attention to operational performance. A control is not considered fully effective merely because it exists; it must also perform under testing, monitoring or incident-response conditions. Compared with scenario-based risk assessment, the model adds recovery and continuity logic, which is essential in critical services. Compared with general composite indicators, the model defines cybersecurity-specific variables and incorporates an exposure penalty.

At the same time, the model has limitations. The current application is hypothetical and does not validate the index against observed incidents, audit results or institutional performance data. Likelihood and impact estimates may be uncertain, especially where incident reporting is incomplete. Weighting decisions may also influence results, which is why sensitivity analysis is required. The model does not yet include network

interdependencies between sectors, although such interdependencies may amplify cascading effects during major cyber incidents.

Future research should therefore focus on empirical calibration. Possible approaches include expert elicitation using the Delphi method, AHP-based weighting, pilot application in one healthcare institution or energy operator, or calibration against incident data and audit results. A comparative regional study could also test whether the index discriminates meaningfully between institutions with different maturity levels.

Conclusions

This study developed a mathematical model for assessing cybersecurity level in critical civilian information infrastructures, with a focus on healthcare, energy and education. The revised model integrates threat exposure, control effectiveness and operational resilience into a normalized composite index bounded within [0,1]. All variables, coefficients and parameters are explicitly defined, and the aggregation formula uses α, β and γ as weights while reserving λ only for exposure calibration.

The illustrative application demonstrates the internal coherence and reproducibility of the model. By presenting the input values, intermediate calculations and sensitivity analysis, the paper shows how the index can be calculated and interpreted. The results should not be read as empirical evidence about a specific institution; they represent a structured demonstration of the model's logic.

The model's main contribution is its integrated assessment logic. It links cybersecurity risk exposure with implemented control effectiveness and operational recovery capacity, thereby moving beyond isolated compliance scoring or standalone risk matrices. For regional policy, the model may support benchmarking, investment prioritisation and structured dialogue between institutions and supervisory authorities.

The conclusions must be interpreted within the limits of the study. The model requires empirical validation before strong policy claims can be made. Future work should apply the framework to real institutional data, compare it with existing maturity models, test alternative weighting methods and incorporate interdependencies between infrastructures. With such calibration, the model could become a practical instrument for regional cybersecurity governance and critical infrastructure protection.

References

Anderson, R. (2021). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Cambridge University Press.

Böhme, R., & Moore, T. (2012). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection, 5*(3-4), 138-143. https://doi.org/10.1016/j.ijcip.2012.09.002

Böhme, R., Laube, S., & Riek, M. (2019). A systematic review of information security risk assessment methods. *Computers & Security, 89*, Article 101637. https://doi.org/10.1016/j.cose.2019.101637

Drivas, G., Chatzopoulou, A., Maglaras, L., Lambrinoudakis, C., Cook, A., & Janicke, H. (2020). *A NIS Directive compliant cybersecurity maturity assessment framework.* arXiv. https://arxiv.org/abs/2004.10411

ENISA. (2023). *ENISA threat landscape: Health sector.* https://www.enisa.europa.eu/sites/default/files/publications/Health%20Threat%20Landscape.pdf

ENISA. (2024). *ENISA threat landscape 2024*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

ENISA. (2025). Handbook for cyber stress tests. https://www.enisa.europa.eu/publications/handbook-for-cyber-stress-tests

ENISA. (2026). *ENISA NIS360*: *Latest insights in the cybersecurity maturity and criticality of NIS sectors of high criticality.* https://www.enisa.europa.eu/enisa-nis360-2026

European Parliament and Council of the European Union. (2022a). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*, L 333.

European Parliament and Council of the European Union. (2022b). Directive (EU) 2022/2557 on the resilience of critical entities. *Official Journal of the European Union*, L 333.

International Electrotechnical Commission. (2018). *IEC 62443-3-3: Security for industrial automation and control systems*.

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements.*

Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2023). *Understanding cyber threats against the universities, colleges, and schools*. arXiv. https://arxiv.org/abs/2307.07755

National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments (SP 800-30 Rev. 1)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-30r1

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

OECD. (2020). *Digital security risk management in critical activities.* OECD Publishing.

OECD & Joint Research Centre. (2008). *Handbook on constructing composite indicators*: *Methodology and user guide*. OECD Publishing.

Saltelli, A., Ratto, M., Andres, T., Campolongo, F., Cariboni, J., Gatelli, D., Saisana, M., & Tarantola, S. (2008). *Global sensitivity analysis: The primer*. Wiley.

Solms, R. V., & Niekerk, J. V. (2013). From information security to cyber security. *Computers & Security, 38,* 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Sommestad, T., Ekstedt, M., & Johnson, P. (2010). A probabilistic relational model for security risk analysis. *Computers & Security, 29*(6), 659-679. https://doi.org/10.1016/j.cose.2010.02.009