

Article

A Fuzzy AHP-Based Framework for Assessing Cybersecurity Readiness in Smart Circular Economy Systems Aligned with ISO/IEC 27001

Seyedeh Azadeh Alavi-Borazjani ^{1,2,*}  and Muhammad Noman Shafique ^{1,2,3,*} 

¹ Department of Environment and Planning, University of Aveiro, 3810-193 Aveiro, Portugal

² Centre for Environmental and Marine Studies (CESAM), University of Aveiro, 3810-193 Aveiro, Portugal

³ Research Unit on Governance, Competitiveness and Public Policies (GOVCOPP), University of Aveiro, 3810-193 Aveiro, Portugal

* Correspondence: saab@ua.pt (S.A.A.-B.); shafique@ua.pt (M.N.S.)

Abstract

The increasing digitalization of smart circular economy (CE) systems intensifies reliance on interconnected cyber-physical infrastructures, thereby increasing exposure to cybersecurity risks that may affect operational continuity and regulatory compliance. This study proposes a Fuzzy Analytical Hierarchy Process (Fuzzy AHP)-based framework to systematically assess cybersecurity readiness in alignment with the ISO/IEC 27001:2022 Information Security Management System (ISMS) standard. The framework adopts a structured three-level hierarchy consisting of seven main criteria and 39 sub-criteria, derived from ISO/IEC 27001:2022 clause-based requirements and Annex A control families, and expanded with an additional regulatory criterion based on the Cyber Resilience Act (CRA) Requirements Standards Mapping. Expert judgments from ten specialists in cybersecurity and digital systems were elicited using linguistic assessments and converted into triangular fuzzy numbers to compute priority weights under uncertainty. The results indicate that ISMS governance and organizational context are the most influential determinants of cybersecurity readiness, followed by regulatory and compliance alignment, operational oversight, and technological controls, while organizational, human, and physical controls play supportive roles. Consistency and sensitivity analyses confirm the robustness and stability of the weighting structure. Overall, the framework provides a standards-aligned decision-support tool for prioritizing cybersecurity readiness in digitally intensive CE environments.

Keywords: smart circular economy; cybersecurity readiness; ISO/IEC 27001:2022; cyber resilience act; digital sustainability; fuzzy AHP; MCDM



Academic Editors: Paulina Rutecka and Pedro Pinto

Received: 30 March 2026

Revised: 26 April 2026

Accepted: 27 April 2026

Published: 29 April 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and

conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

The ongoing digital transformation toward smart circular economy (CE) systems is redefining how organizations manage resources, optimize production, and sustain environmental performance. By integrating advanced technologies such as the Internet of Things (IoT), artificial intelligence (AI), and data analytics, these systems facilitate dynamic, data-driven resource cycles that enhance efficiency and sustainability. However, the increased digital connectivity that drives the circular economy also introduces new cybersecurity challenges. The extensive data exchange across interconnected networks heightens susceptibility to cyber threats, which can compromise system resilience, operational continuity,

and stakeholder trust [1]. Ensuring cybersecurity readiness is therefore crucial for realizing the promise of smart CE systems. Cybersecurity readiness refers to the degree to which an organization possesses the governance structures, technological capabilities, operational processes, and human competencies required to anticipate, prevent, detect, respond to, and recover from cyber threats while maintaining the confidentiality, integrity, and availability of information systems [2–4].

The ISO/IEC 27001 standard provides a widely accepted framework for establishing and maintaining an Information Security Management System (ISMS), promoting systematic risk management, control implementation, and continuous improvement [5]. The 2022 revision of the standard further reflects the growing importance of resilience, cloud security, and adaptability within emerging digital infrastructures [6]. Nonetheless, organizations continue to face challenges in translating ISO/IEC 27001 controls into actionable strategies for evaluating their cybersecurity readiness, particularly within smart CE environments characterized by complex interactions among people, processes, and technologies.

Existing cybersecurity assessment approaches often rely on deterministic or checklist-based evaluations, which fail to capture the uncertainty, interdependence, and multidimensionality inherent in smart CE systems. In contrast, fuzzy multi-criteria decision-making (MCDM) techniques offer a powerful means of handling ambiguity in expert judgments and supporting more nuanced assessments. The Fuzzy Analytical Hierarchy Process (Fuzzy AHP), in particular, allows for the systematic weighting and prioritization of interrelated factors affecting cybersecurity performance under uncertain conditions [7,8]. In this study, Fuzzy AHP was selected over alternative uncertainty-aware MCDM methods due to its optimal balance between methodological transparency, computational simplicity, and suitability for hierarchical structures [9]. Unlike more complex techniques such as fuzzy Analytic Network Process (ANP), fuzzy Decision Making Trial and Evaluation Laboratory (DEMATEL), or spherical fuzzy extensions—which require modeling extensive interdependencies or impose high cognitive demands on experts—Fuzzy AHP enables clear, structured pairwise judgments while effectively capturing the vagueness inherent in linguistic assessments [10]. Its use of triangular fuzzy numbers allows experts to express uncertainty naturally and intuitively [11], and the resulting normalized weights can be directly aligned with the clause-based structure of ISO/IEC 27001:2022. This makes Fuzzy AHP particularly appropriate for readiness-assessment frameworks that must reflect layered organizational structures, regulatory requirements, and operational control families.

However, current Fuzzy AHP applications in cybersecurity remain narrowly focused, typically addressing single domains such as technical controls in cloud and wireless-sensor environments, or personnel-related awareness programs in financial institutions, often based on older versions of ISO/IEC 27001. These studies do not examine how governance, operational processes, organizational structures, and regulatory obligations collectively influence cybersecurity readiness. Furthermore, none of the available approaches considers the technological and operational characteristics of smart circular-economy systems, where IoT-enabled sensing, AI-driven decision automation, distributed data flows, and cyber-physical resource loops create unique security dependencies. Table 1 summarizes these methodological and contextual constraints and underscores the need for a framework that integrates ISO/IEC 27001:2022 requirements with CRA regulatory expectations while addressing the digital infrastructures that support circular-economy operations.

Table 1. Comparative analysis of Fuzzy AHP cybersecurity frameworks.

Study	Application Context	Criteria Source	Scope of Analysis	Key Contributions	Limitations (Relative to Readiness Assessment)
Tariq et al. [12]	Cloud computing and wireless sensor networks	ISO/IEC 27002:2013	Technical information-security controls	Provides prioritization of security controls for cloud and WSN environments	Focuses only on technical controls; based on ISO 27002:2013; no governance, operational, or regulatory integration
Styoutomo & Ruldeviyani [8]	Financial institution (WFH conditions)	HAIS-Q + ISO/IEC 27001:2013	Human attitudes, knowledge, behavior, and awareness	Identifies weak areas in employee security awareness and provides improvement recommendations	Limited to people-centric factors; no technological, operational, or compliance components
Bhol et al. [13]	Enterprise cybersecurity metrics	Literature + security-metric hierarchies	Cybersecurity performance indicators	Proposes hierarchical evaluation of cybersecurity metrics	Not linked to ISO 27001 structure; not designed for organizational readiness; no Circular Economy or regulatory context
Mızrak [14]	International organizations	Literature-derived strategic criteria	High-level cybersecurity strategy development	Supports strategic prioritization of cybersecurity criteria for international organizations	Strategic focus only; lacks ISMS reference models; no operational or domain-specific (e.g., Circular Economy) application
Simjanović et al. [15]	Active cyber-attack landscape	Attack-type characteristics (frequency, impact, complexity)	Threat and attack prioritization	Ranks social engineering and masquerade attacks as most critical	Focuses on attack types rather than readiness; no ISMS linkage; no organizational governance or regulatory dimension

Recent literature on cybersecurity-governance further reinforces these gaps. Multiple studies highlight ongoing challenges in implementing information-security governance effectively, even in highly digitalized environments. For instance, Magnusson et al. [16] report that many public-sector organizations continue to struggle with establishing consistent governance structures, risk-management procedures, and compliance mechanisms, despite reliance on ISO/IEC 27001, GDPR, and NIS frameworks. Similarly, a recent systematic review on integrating cybersecurity into IT-governance practices emphasizes persistent difficulties in embedding cybersecurity responsibilities within organizational decision-making architectures, resulting in fragmented governance and misalignment between strategic and security objectives [17]. Brezavšček and Baggia [18] also identify a growing reliance on cybersecurity-maturity models but point out challenges in adapting these models to meet evolving regulatory and digital-infrastructure requirements. Earlier research has also identified the absence of unified governance frameworks capable of integrating strategic, operational, and technical dimensions of cybersecurity across complex systems [19]. Collectively, these recent studies underscore the importance of cybersecurity-readiness approaches that integrate governance, operational performance, regulatory compliance, and digital-infrastructure interdependencies—an integration currently lacking in smart CE contexts.

Empirical studies in CE-related fields demonstrate that Fuzzy AHP is already being successfully applied within real-world circular-economy operations, proving its effectiveness in complex CE environments. For example, Demircan and Yetilmezsoy [20] evaluated smart waste-management strategies using a hybrid fuzzy AHP–TOPSIS model with operational data collected from an active municipal CE system. Similarly, Joshi and Deole [21] applied spherical Fuzzy AHP to prioritize barriers to IoT implementation in circular systems, identifying data-security and privacy concerns as major obstacles in real deployments. In addition, Khoshand et al. [22] implemented Fuzzy AHP within Tehran’s municipal e-waste processing infrastructure to evaluate and select waste-management options under uncertainty. Although these studies do not specifically address cybersecurity readiness,

they demonstrate the operational validation of Fuzzy AHP in CE contexts with real data, stakeholders, and circular resource systems.

While the practical applications of Fuzzy AHP in empirical CE scenarios have proven its validity and operational feasibility in real circular-economy settings, there is a notable lack of a cybersecurity-focused readiness framework. This study aims to fill this gap by developing a Fuzzy AHP-based framework for assessing and prioritizing the key factors influencing cybersecurity readiness in smart circular economy systems, in accordance with ISO/IEC 27001 standards. The framework provides a structured and quantitative approach to assessing the importance of factors that shape an organization's cybersecurity posture. By integrating expert judgment with fuzzy logic, it addresses the uncertainties present in complex decision-making environments and translates qualitative assessments into actionable insights. The novelty of the framework lies in its alignment with the clause-level structure of ISO/IEC 27001:2022, allowing for a more comprehensive and traceable representation of governance, leadership, risk planning, operational performance, and control requirements compared to previous FAHP applications based on older standards or partial control sets. Additionally, the integration of requirements introduces a regulatory dimension that has not been incorporated into earlier MCDM-based cybersecurity models. Contextually, this work is the first to adapt cybersecurity-readiness assessment to smart CE digital infrastructures, where IoT-enabled sensing, AI-based optimization, interoperable data flows, and cyber-physical loops create security dependencies that differ from traditional enterprise setups. By linking ISO/IEC 27001:2022 controls and CRA expectations to the digital processes that underpin circular-economy operations, the framework offers a standards-compliant, regulation-aware, and CE-specific approach to readiness assessment that is currently lacking in the literature.

The primary objective of this research is to establish a robust and adaptable framework that enables organizations to systematically evaluate and prioritize the factors influencing their cybersecurity readiness. By doing this, the study advances both theoretical and practical understanding of cybersecurity management in smart CE contexts. The proposed approach contributes by bridging the gap between ISO/IEC 27001 compliance and readiness quantification, introducing a decision-support model that enhances organizational resilience, risk awareness, and governance in sustainable digital environment. Ultimately, this research contributes to the growing discourse on digital sustainability by providing a scientifically grounded methodology for prioritizing cybersecurity readiness factors, supporting the secure and resilient evolution of smart circular economy systems. Accordingly, the study is guided by the following research question:

RQ: How can a structured, ISO/IEC 27001:2022-aligned Fuzzy AHP framework be developed to systematically prioritize the factors determining cybersecurity readiness in smart circular-economy systems?

2. Conceptual Background: Mapping CE Digital Infrastructures to ISO/IEC 27001:2022 Readiness Criteria

Digitalization is crucial for facilitating transitions to a circular economy, transforming how materials, products, and processes are monitored, optimized, and recovered across industrial ecosystems. Smart CE systems increasingly employ IoT devices, sensor networks, cloud computing, machine intelligence, and data-driven coordination platforms to support real-time visibility and automated decision-making. Recent peer-reviewed research shows that IoT infrastructures enhance resource efficiency, condition monitoring, waste-collection optimization, and traceability across CE value chains by continuously acquiring data and integrating cyber-physical systems [23]. Additionally, studies indicate that AI and machine-learning systems are used to improve predictive sorting, optimize reverse-logistics

operations, and support dynamic material-flow analysis in remanufacturing and recycling processes [24].

The integration of digital technologies into CE systems has gained momentum across various sectors. A comprehensive literature review of 95 peer-reviewed studies identified IoT, AI, blockchain, cyber-physical systems, and digital-twin technologies as the most frequently applied enablers in circular supply chains, supporting enhanced traceability, cross-organizational data sharing, and end-to-end lifecycle management [25]. Another systematic review finds that IoT and AI are the most mature CE technologies globally, widely used for real-time monitoring, predictive maintenance, asset recovery, and process optimization, while blockchain and big-data approaches support transparency and stakeholder coordination [26]. Collectively, these studies illustrate that circular economy technologies establish structured, replicable digital infrastructure characteristics that transcend contextual differences and provide a basis for cybersecurity assessment.

The digital structures supporting these CE implementations align closely with the cybersecurity-readiness domains defined by ISO/IEC 27001:2022. IoT-based CE systems rely on distributed sensors, telemetry, and device-to-cloud connectivity, which correspond to ISO requirements for operational monitoring, logging, anomaly detection, and system-integrity assurance. AI-enhanced CE decision systems, including predictive analytics, automated classification, and smart-routing engines, necessitate technological controls related to model integrity, data-quality assurance, access management, and secure configuration of cloud-analytics pipelines. Blockchain-enabled traceability systems, increasingly adopted in circular supply chains, introduce requirements for governance structures, key-management processes, identity validation, and secure distributed-ledger operation. Assessments of digital CE strategies highlight that industrial-symbiosis platforms and multi-actor resource-exchange systems rely on transparent data governance, shared responsibility allocation, and cross-organizational risk-management routines in line with ISO/IEC leadership and organizational-control clauses [27].

Physical-security considerations also play a role in CE contexts, as many CE operations involve cyber-physical systems deployed across various locations, such as robotic disassembly plants, automated sorting lines, IoT-equipped collection hubs, and material-recovery units. These infrastructures require physical-asset protection, secure equipment housing, controlled facility access, and environmental safeguards, directly reflecting ISO/IEC 27001 physical-security control families. Human-factor dependencies are also salient: as CE digitalization advances, operators increasingly interact with AI-supported interfaces, automated machinery, and data-centric CE platforms, requiring competence, awareness, and cybersecurity-oriented training. Studies on digital CE transitions emphasize that human-machine interaction and workforce upskilling are critical for safe and effective operation of digitally intensive CE systems [26].

Finally, regulatory and compliance considerations are becoming central to CE digital ecosystems. International analyses indicate that digital CE solutions are intersecting with data-regulation frameworks, digital-product safety requirements, and sustainability reporting obligations. This highlights the need for cybersecurity governance and compliance mechanisms in CE operations [28]. The emergence of intelligent, AI-enhanced circular supply chains—where product tracking, reuse cycles, and resource-flow data are exchanged across organizational boundaries—further accentuates the need for robust regulatory alignment [29].

Taken together, the evidence shows that while CE systems vary operationally across sectors, their digital infrastructures consistently generate identifiable cybersecurity dependencies across governance, operational, organizational, technological, human, physical, and regulatory domains. This establishes a clear analytical foundation for applying ISO/IEC

27001:2022-aligned readiness criteria to smart CE environments, addressing the reviewer's observation that CE is contextual by demonstrating that its digital architectures exhibit structurally consistent cybersecurity requirements.

3. Materials and Methods

3.1. Development of the Hierarchical Framework

The hierarchical framework was developed through a structured decomposition process to translate cybersecurity requirements for smart CE systems into a multi-level decision structure suitable for Fuzzy AHP analysis. The process ensured that the hierarchy is conceptually coherent, traceable to authoritative sources, and detailed enough to support expert-based evaluation under uncertainty.

At the top level, the main goal of the model was defined as assessing cybersecurity readiness in smart CE systems. This goal reflects the importance of assessing the ability of digitally intensive CE environments to maintain secure, resilient, and trustworthy operations.

At the second level, the framework consists of seven main criteria, each representing a major functional domain of cybersecurity management. These domains were derived directly from the structural components of ISO/IEC 27001:2022 [30], specifically its clause-based ISMS requirements and Annex A control categories, which together define the essential organizational, human, physical, and technological control areas required for effective information security management. Although ISO/IEC 27001:2022 forms the basis of the hierarchy, the proposed Fuzzy AHP framework is inherently extensible and can be adapted to incorporate alternative cybersecurity standards, such as NIST CSF and NIST SP 800-53, by mapping their control families into the same hierarchical decision structure. An additional criterion related to regulatory and compliance alignment was included based on the Cyber Resilience Act (CRA) Requirements Standards Mapping developed by ENISA and the Joint Research Centre (JRC) [31]. This resulted in a set of criteria that collectively reflect both established information security practices and emerging regulatory expectations relevant to digitalized CE environments.

At Level 3, the seven main criteria were broken down into 39 sub-criteria, each corresponding to a distinct requirement area linked to underlying clause or control family. These sub-criteria were identified through a systematic extraction of requirement elements from ISO/IEC 27001:2022, such as context definition, leadership responsibilities, risk assessment, operational control, monitoring and audit processes, awareness and training, physical protections, access control, vulnerability management, logging, backup, secure development, and regulatory considerations outlined in the CRA mapping analysis. This structure ensures that the model covers a comprehensive and balanced representation of cybersecurity readiness factors applicable to smart CE systems.

The complete three-level hierarchy is presented in Figure 1, illustrating how the cybersecurity readiness objective is operationalized through the associated requirement domains. This hierarchical organization forms the analytical foundation for the subsequent fuzzy pairwise comparison process. In an applied setting, this structure also serves as the reference model for assessing and aggregating cybersecurity readiness across organizational domains.



Figure 1. Hierarchical structure used for the cybersecurity readiness assessment in smart circular economy systems.

3.2. Expert Panel and Selection Process

The evaluation of the hierarchical framework involved gathering expert opinions to create fuzzy pairwise comparison matrices. Ten academic experts were chosen based on their expertise in cybersecurity, information systems, smart technologies, or digital

infrastructures related to the circular economy. The experts held academic positions such as professor, associate professor, senior researcher, or postdoctoral researcher, and their research focused on cybersecurity governance, digital risk assessment, or the development and evaluation of smart digital systems.

Each expert independently assessed the importance of criteria and sub-criteria in the hierarchical model using a predefined linguistic scale commonly used in fuzzy multi-criteria decision-making. These assessments were then converted into triangular fuzzy numbers for quantitative analysis. Table 2 displays the linguistic terms and their corresponding TFNs utilized in the study, which were used to create the fuzzy pairwise comparison matrices for further analysis.

Table 2. Linguistic terms and corresponding TFNs used in this study (adapted from Chou et al. [32]).

Linguistic Terms	TFNs
Equally important	(1,1,1)
Moderately important	(2,3,4)
Important	(4,5,6)
Very important	(6,7,8)
Extremely important	(8,9,10)
Intermediate	(1,2,3), (3,4,5), (5,6,7), (7,8,9)

The expert panel included academic specialists in cybersecurity governance, information systems management, and multi-criteria decision-making. However, industry practitioners, ISO/IEC 27001 auditors, and CE system operators were not part of the panel. The academic experts were chosen to maintain methodological consistency and conceptual rigor in the FAHP pairwise-comparison process. It is important to note that the lack of operational and audit-driven perspectives could impact the practical interpretation of certain readiness criteria. This limitation is recognized, and it is suggested that future iterations of the framework involve a more diverse stakeholder group.

3.3. Fuzzy AHP and Computational Procedure

The criteria and sub-criteria were weighted using the Fuzzy AHP method based on the formulation by Buckley [33]. Expert opinions expressed in linguistic terms were converted into TFNs to create fuzzy pairwise comparison matrices and calculate the weights.

Each expert's linguistic input was translated into a TFN $\tilde{A} = (l, m, u)$, with a membership function defined as:

$$\mu(x) = \begin{cases} (x - l) / (m - l), & l \leq x \leq m \\ (u - x) / (u - m), & m \leq x \leq u \\ 0, & \text{otherwise} \end{cases} \quad (1)$$

These TFNs populate the fuzzy pairwise comparison matrix $\tilde{A}$. In this matrix, each entry $a_{ij} = (l_{ij}, m_{ij}, u_{ij})$ represents the relative importance of element i compared to element j as judged by experts.

- $\tilde{a}_{ij}$ reflects the comparative preference of criterion i over criterion j in fuzzy form.
- $\tilde{a}_{ji}$ is its reciprocal, representing the inverse importance.
- $\tilde{a}_{ii} = (1, 1, 1)$ indicates that each element is equally important with itself.

The general structure of the matrix is:

$$\tilde{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} = \begin{bmatrix} (1, 1, 1) & (l_{12}, m_{12}, u_{12}) & \cdots & (l_{1n}, m_{1n}, u_{1n}) \\ (l_{21}, m_{21}, u_{21}) & (1, 1, 1) & \cdots & (l_{2n}, m_{2n}, u_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ (l_{n1}, m_{n1}, u_{n1}) & (l_{n2}, m_{n2}, u_{n2}) & \cdots & (1, 1, 1) \end{bmatrix} \quad (2)$$

When multiple experts provide assessments, their fuzzy judgments for each pair (i, j) are aggregated using the fuzzy geometric mean:

$$l_{ij} = \left(\prod_{k=1}^k l_{ijk} \right)^{1/k}, m_{ij} = \left(\prod_{k=1}^k m_{ijk} \right)^{1/k}, u_{ij} = \left(\prod_{k=1}^k u_{ijk} \right)^{1/k} \quad (3)$$

where l_{ijk} , m_{ijk} , u_{ijk} denote the lower, middle, and upper bounds provided by expert k .

Following Buckley's method, the fuzzy geometric mean for each element i is calculated as:

$$\tilde{r}_i = \left(\prod_{j=1}^n \tilde{a}_{ij} \right)^{1/n}, i = 1, 2, \dots, n \quad (4)$$

The fuzzy weights are then obtained by normalizing the geometric means:

$$\tilde{w}_i = \tilde{r}_i \otimes \left(\tilde{r}_1 \oplus \tilde{r}_2 \oplus \cdots \oplus \tilde{r}_n \right)^{-1} \quad (5)$$

To derive single-valued priority weights, the fuzzy weights are defuzzified using the center-of-area (COA) method:

$$w_i = \frac{lw_i + mw_i + uw_i}{3} \quad (6)$$

The resulting crisp weights are normalized to ensure comparability:

$$w_r = \frac{w_i}{\sum_{i=1}^n w_i} \quad (7)$$

These normalized weights indicate the ultimate quantitative priorities of all criteria and sub-criteria in the cybersecurity readiness framework and serve as the foundation for further analysis. In practice, these weights are combined with organization-specific performance scores given to each sub-criterion, which are determined by evidence like audits, self-assessments, or documented controls. By combining these weighted scores, an overall cybersecurity readiness level can be calculated, allowing for the prioritization of enhancement efforts.

3.4. Reliability Assessment

To ensure the methodological rigor of the Fuzzy AHP evaluation and to strengthen confidence in the resulting priority weights, a reliability assessment was conducted focusing on (i) the internal consistency of expert-derived pairwise comparison matrices and (ii) the stability and robustness of the computed weights under controlled perturbations.

3.4.1. Consistency Assessment

The consistency of the pairwise comparison matrices was evaluated following defuzzification. Each triangular fuzzy value (l, m, u) in the aggregated comparison matrix was initially converted into a crisp value using the center-of-area method:

$$\text{Crisp value} = \frac{(l + m + u)}{3} \quad (8)$$

These crisp values were then used to compute the maximum eigenvalue $\lambda_{\max}$, from which the Consistency Index (CI) was derived:

$$\text{CI} = \frac{\lambda_{\max} - n}{n - 1} \quad (9)$$

The Consistency Ratio (CR) was subsequently calculated using:

$$\text{CR} = \frac{\text{CI}}{\text{RI}} \quad (10)$$

where RI denotes the Random Index for a matrix of order n , as established in AHP literature [34,35]. A CR value of 0.10 or below was adopted as the threshold for acceptable consistency.

3.4.2. Sensitivity and Robustness Assessment

To evaluate the stability of the weighting structure derived from FAHP, a combined sensitivity and robustness assessment was conducted. The normalized weight w_p of each main criterion was independently perturbed by $\pm 10\%$, representing a moderate and analytically meaningful deviation in expert judgment. After each perturbation, the remaining weights were adjusted proportionally using Equation (11) to maintain a total weight of one:

$$w'_j = \frac{1 - w_p - \Delta_p}{1 - w_p} \times w_j \quad j = 1, 2, \dots, k \quad j \neq p \quad (11)$$

where Δ_p denotes the magnitude of the increase or decrease applied to criterion p [36,37]. This procedure enabled examination of how local changes propagate through the hierarchical structure and whether any criterion exerts disproportionate influence on the model.

In addition to observing weight redistribution patterns, various quantitative indicators were computed to assess ranking and structural robustness. Ranking consistency was evaluated using Spearman's rank correlation coefficient (ρ):

$$\rho = 1 - \frac{6 \sum_{i=1}^n (r_i - r'_i)^2}{n(n^2 - 1)} \quad (12)$$

where r_i and r'_i represent the original and perturbed rank of criterion i , and n is the number of criteria. Values of ρ approaching 1 indicate that the ranking order remains consistent despite perturbations [38].

Global rank stability was further assessed through the ranking stability index (RSI), which quantifies the proportion of preserved rank relationships:

$$\text{RSI} = 1 - \frac{\sum_{i=1}^n |r_i - r'_i|}{n(n - 1)} \quad (13)$$

RSI values close to 1 indicate minimal rank displacement, consistent with stability measures used in comparative MCDM evaluations [39].

Weight-level sensitivity was evaluated using the maximum deviation percentage (MDP) based on the deviation percentage (DP) of each criterion or sub-criterion:

$$DP_i = \frac{|w_i - \bar{w}|}{\bar{w}} \times 100\% \quad (14)$$

where w_i represents the normalized weight of criterion i and $\bar{w}$ is the average weight of all criteria (or sub-criteria). The MDP reflects the highest DP observed among all elements, indicating the maximum proportional deviation compared to the mean. This approach provides a clear measure of the relative influence of individual elements on the overall weighting structure and captures the degree to which any single criterion or sub-criterion dominates the hierarchy.

Finally, critical stability threshold (CST) was computed using Equation (15):

$$CST = \min\{\Delta\% | r'_i(\Delta\%) \neq r_i\} \quad (15)$$

where $\Delta\%$ represents the magnitude of the weight perturbation applied to a criterion, r_i denotes the original baseline rank of criterion i , and $r'_i(\Delta\%)$ indicates the rank of that criterion after the applied perturbation. The CST corresponds to the smallest perturbation level at which any criterion's perturbed rank differs from its baseline rank, providing a direct measure of how sensitive the ranking structure is to perturbation-induced reversals.

Together, the perturbation analysis and robustness indicators provide a comprehensive evaluation of the model's stability by examining weight redistribution, ranking consistency, structural reliability, and susceptibility to rank changes.

4. Results

4.1. Prioritization of Main Criteria

The fuzzy AHP analysis yielded a distinct ranking of the seven primary criteria influencing cybersecurity preparedness. As depicted in Table 3, the findings reveal significant variations in the significance of governance, compliance, operations, and organizational safeguards.

Table 3. Fuzzy AHP results for main criteria.

Criterion	Fuzzy Geometric Mean	Fuzzy Weight	Crisp Weight	Normalized Weight	Rank
C1	(2.0830, 2.5221, 2.9487)	(0.2078, 0.2941, 0.4163)	0.3061	0.2941	1
C2	(1.2514, 1.5152, 1.7715)	(0.1248, 0.1767, 0.2501)	0.1839	0.1767	3
C3	(0.6883, 0.8333, 0.9743)	(0.0687, 0.0972, 0.1376)	0.1011	0.0972	5
C4	(0.4143, 0.5016, 0.5865)	(0.0413, 0.0585, 0.0828)	0.0609	0.0585	6
C5	(0.2762, 0.3342, 0.3908)	(0.0276, 0.0390, 0.0552)	0.0406	0.0390	7
C6	(0.8327, 1.0083, 1.1788)	(0.0831, 0.1176, 0.1664)	0.1224	0.1176	4
C7	(1.5367, 1.8606, 2.1754)	(0.1533, 0.2170, 0.3071)	0.2258	0.2170	2

The highest-ranked criterion is C1 (ISMS governance and organization) with a normalized weight of 0.2941, indicating that governance structures, strategic oversight, and leadership engagement are seen as the key drivers of cybersecurity maturity. The second most influential dimension is C7 (regulatory and compliance alignment) with a normalized weight of 0.2170, underscoring the importance of external mandates, conformity requirements, and adherence to evolving regulatory obligations. Together, C1 and C7 make up over 51% of the total weight, highlighting the dominant role of top-level governance and regulatory alignment in structuring organizational cybersecurity posture.

The next set of criteria holds a moderate level of influence. C2 (operational controls) ranks third with a weight of 0.1767, highlighting its crucial role in implementing governance decisions into practical safeguards. C6 (technological controls) comes in fourth at 0.1176,

stressing the importance of system-level defenses like secure configurations, intrusion monitoring, and protective technologies. While essential, these mechanisms are viewed as supporting elements rather than primary strategic drivers.

Less weighted criteria include C3 (organizational controls) at 0.0972, indicating its supportive but less dominant role in readiness; C4 (People controls) at 0.0585, which is still important but not as high a priority; and C5 (Physical controls), the least weighted criterion at 0.0390, aligning with the increasingly digital and interconnected nature of modern CE environments.

To visualize the overall importance distribution, Figure 2 presents the normalized weights of the seven criteria, showing a distinct separation between the top-tier (governance and compliance), mid-tier (operational and technological), and supportive-tier (organizational, people, and physical) factors.

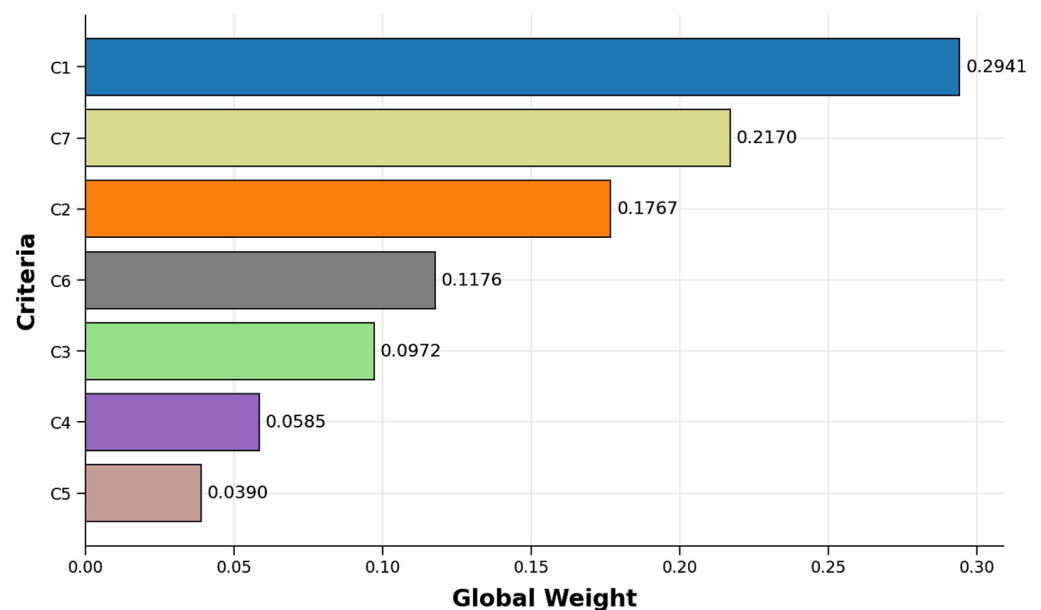


Figure 2. Global weights for the main criteria.

4.2. Prioritization of Sub-Criteria

4.2.1. Local Weight Ranking of Sub-Criteria

To further enhance the prioritization of factors impacting cybersecurity readiness in Smart CE systems, the study evaluated the relative importance of sub-criteria within each main criterion. The rankings in Table 4 were based on normalized weights, providing valuable insights into the key elements influencing the effectiveness of information security management aligned with ISO/IEC 27001.

In C1 (ISMS governance and organization), the sub-criterion C1.3 (risk assessment and risk treatment planning) had the highest local weight (0.3160), indicating that effective risk management is crucial for governance in smart CE systems. C1.1 (understanding context of the organization) and C1.2 (leadership and information security policy) followed with weights of 0.2950 and 0.2620, respectively. C1.4 (support: competence, awareness, communication, documentation) had the lowest influence within the group, with a weight of 0.2220.

Within C2 (operational controls and performance management), C2.2 (monitoring, measurement, internal audit, and management review) ranked highest (0.1730), emphasizing the importance of continuous evaluation and operational oversight. C2.1 (operational planning and control) had a moderate weight (0.1580), while C2.3 (improvement, corrective actions, and continual improvement) received the lowest weight (0.1210).

For C3 (organizational controls), C3.4 (information classification, labeling, and handling) was the most significant sub-criterion (0.1160), highlighting the role of proper data management in secure smart CE operations. Other important sub-criteria included C3.2 (roles, responsibilities, segregation of duties) (0.1060) and C3.1 (information security policies) (0.0960). Sub-criteria such as C3.3 (contact with authorities and special interest groups) (0.0720) and C3.5 (supplier and ICT supply chain security) (0.0650) were considered less critical within the organizational domain.

In C4 (people controls), C4.2 (awareness, education, and training) received the highest weight (0.0540), highlighting the importance of personnel knowledge and competence. C4.1 (screening and employment conditions) and C4.5 (remote working and confidentiality agreements) followed closely (0.0510 each), while C4.3 (disciplinary process) (0.0440) and C4.4 (responsibilities after termination) (0.0410) were less influential.

Within C5 (physical controls), C5.2 (securing offices, rooms, and facilities) and C5.1 (physical security perimeters and entry controls) had the highest weights (0.0410 each), underscoring the need for robust physical security measures. Other sub-criteria, including C5.4 (equipment protection, off-site assets, and maintenance) and C5.5 (secure storage, cabling, disposal, and supporting utilities), had moderate weights ranging from 0.0320 to 0.0340.

Table 4. Fuzzy AHP results for sub-criteria.

Sub-Criterion	Fuzzy Geometric Mean	Fuzzy Weight	Crisp Weight	Normalized Weight	Rank
C1.1	(2.1500, 2.8000, 3.4000)	(0.2200, 0.2800, 0.3500)	0.2833	0.2950	2
C1.2	(1.8500, 2.4500, 3.0500)	(0.1900, 0.2500, 0.3100)	0.2517	0.2620	3
C1.3	(2.3500, 3.0500, 3.7000)	(0.2400, 0.3000, 0.3700)	0.3033	0.3160	1
C1.4	(1.6500, 2.1500, 2.7500)	(0.1700, 0.2100, 0.2700)	0.2130	0.2220	4
C2.1	(1.2000, 1.5500, 1.9000)	(0.1200, 0.1600, 0.1900)	0.1550	0.1580	2
C2.2	(1.3500, 1.7500, 2.1500)	(0.1300, 0.1700, 0.2100)	0.1700	0.1730	1
C2.3	(0.9500, 1.2500, 1.5500)	(0.0900, 0.1200, 0.1500)	0.1187	0.1210	3
C3.1	(0.6500, 0.8500, 1.0500)	(0.0700, 0.0900, 0.1100)	0.0933	0.0960	3
C3.2	(0.8000, 1.0500, 1.3000)	(0.0800, 0.1000, 0.1300)	0.1030	0.1060	2
C3.3	(0.5500, 0.7000, 0.8500)	(0.0500, 0.0700, 0.0900)	0.0707	0.0720	7
C3.4	(0.9000, 1.1500, 1.4000)	(0.0900, 0.1100, 0.1400)	0.1133	0.1160	1
C3.5	(0.5000, 0.6500, 0.8000)	(0.0500, 0.0600, 0.0800)	0.0633	0.0650	8
C3.6	(0.6000, 0.7500, 0.9000)	(0.0600, 0.0800, 0.0900)	0.0733	0.0750	6
C3.7	(0.7000, 0.9000, 1.1000)	(0.0600, 0.0900, 0.1100)	0.0867	0.0890	4
C3.8	(0.6500, 0.8500, 1.0500)	(0.0600, 0.0800, 0.1000)	0.0867	0.0890	5
C4.1	(0.4000, 0.5000, 0.6000)	(0.0400, 0.0500, 0.0600)	0.0500	0.0510	2
C4.2	(0.4500, 0.5500, 0.6500)	(0.0400, 0.0500, 0.0600)	0.0533	0.0540	1
C4.3	(0.3500, 0.4500, 0.5500)	(0.0300, 0.0400, 0.0500)	0.0433	0.0440	4
C4.4	(0.3000, 0.4000, 0.5000)	(0.0300, 0.0400, 0.0500)	0.0400	0.0410	5
C4.5	(0.4000, 0.5000, 0.6000)	(0.0400, 0.0500, 0.0600)	0.0500	0.0510	3
C5.1	(0.2762, 0.3342, 0.3908)	(0.0276, 0.0390, 0.0552)	0.0406	0.0410	2
C5.2	(0.3000, 0.3600, 0.4200)	(0.0300, 0.0400, 0.0500)	0.0400	0.0410	1
C5.3	(0.2500, 0.3000, 0.3500)	(0.0250, 0.0300, 0.0400)	0.0317	0.0320	5
C5.4	(0.2700, 0.3300, 0.3900)	(0.0270, 0.0330, 0.0390)	0.0337	0.0340	3
C5.5	(0.2600, 0.3200, 0.3800)	(0.0260, 0.0320, 0.0380)	0.0320	0.0330	4
C6.1	(0.8327, 1.0083, 1.1788)	(0.0831, 0.1176, 0.1664)	0.1224	0.1240	2
C6.2	(0.9000, 1.1000, 1.3000)	(0.0900, 0.1200, 0.1500)	0.1200	0.1220	1
C6.3	(0.8500, 1.0200, 1.1900)	(0.0850, 0.1020, 0.1190)	0.1020	0.1040	3
C6.4	(0.8000, 0.9500, 1.1000)	(0.0800, 0.0950, 0.1100)	0.0950	0.0970	4
C6.5	(0.7600, 0.9000, 1.0400)	(0.0760, 0.0900, 0.1040)	0.0900	0.0920	5
C6.6	(0.7000, 0.8400, 0.9800)	(0.0700, 0.0840, 0.0980)	0.0840	0.0860	6
C6.7	(0.6500, 0.7800, 0.9100)	(0.0650, 0.0780, 0.0910)	0.0780	0.0800	7
C6.8	(0.6000, 0.7200, 0.8400)	(0.0600, 0.0720, 0.0840)	0.0720	0.0740	8
C6.9	(0.5500, 0.6600, 0.7700)	(0.0550, 0.0660, 0.0770)	0.0660	0.0680	9
C6.10	(0.5000, 0.6000, 0.7000)	(0.0500, 0.0600, 0.0700)	0.0600	0.0620	10
C6.11	(0.4800, 0.5700, 0.6600)	(0.0480, 0.0570, 0.0660)	0.0550	0.0560	11
C7.1	(1.5367, 1.8606, 2.1754)	(0.1533, 0.2170, 0.3071)	0.2258	0.2169	1
C7.2	(1.2000, 1.5000, 1.8000)	(0.1200, 0.1500, 0.1800)	0.1500	0.1445	3
C7.3	(1.0000, 1.2500, 1.5000)	(0.1000, 0.1250, 0.1500)	0.1250	0.1204	2

For C6 (technological controls), C6.1 (user endpoint and privileged access management) (0.1240) and C6.2 (access restrictions and source-code controls) (0.1220) were identified as the most critical technological measures, highlighting the importance of access management and protection of privileged accounts. Other technological sub-criteria, such as C6.3 (secure authentication and identity management), C6.4 (malware protection and secure configuration), and C6.5 (vulnerability management and patching), showed descending weights from 0.1040 to 0.0920, indicating varying priorities within the technological domain. Additional sub-criteria, including C6.6–C6.11, received lower weights, emphasizing their supportive roles in the overall technological controls framework.

Lastly, in C7 (regulatory and compliance alignment), C7.1 (standards coverage against CRA requirements) had the highest local weight (0.2169), followed by C7.2 (identification of regulatory compliance gaps) (0.1445) and C7.3 (harmonization readiness and conformity expectations) (0.1204). This underscores the importance of standard compliance and regulatory alignment for the cybersecurity readiness of smart CE systems.

4.2.2. Global Weight Ranking of Sub-Criteria

The global weighting of the 39 sub-criteria, achieved by combining their local weights with the normalized weights of their corresponding main criteria, offers a comprehensive view of the factors that significantly impact cybersecurity readiness in smart CE systems. This integrated prioritization allows for the identification of overarching requirements that transcend individual domains and have a substantial impact on the organization's overall security posture aligned with ISO/IEC 27001. The distribution of normalized global weights is depicted in Figure 3, with sub-criteria listed in descending order of influence.

The analysis reveals that C1.3 (risk assessment and risk treatment planning) holds the highest global weight (0.1309), underscoring the pivotal role of systematic risk management in shaping cybersecurity readiness. This is closely followed by C1.1 (understanding the organization's context) at 0.1222 and C1.2 (leadership and information security policy) at 0.1085, confirming that the most influential factors stem from ISMS governance and leadership-driven oversight. Together, these three governance sub-criteria account for a significant portion of the total influence, emphasizing the importance of organizational context, leadership commitment, and risk-informed decision-making in secure CE environments.

The most influential sub-criterion outside the governance domain is C7.1 (standards coverage against CRA requirements), with a global weight of 0.0663, highlighting the continued importance of regulatory alignment in cybersecurity posture, especially in the context of emerging EU frameworks like the Cyber Resilience Act. Other regulatory elements, including C7.2 (identification of regulatory compliance gaps) at 0.0442 and C7.3 (harmonization readiness and conformity expectations) at 0.0368, also demonstrate significant influence, emphasizing the critical role of compliance assurance and lifecycle-aligned conformity.

Operational and technological controls occupy the next level of influence. C2.2 (monitoring, measurement, internal audit, and management review) has a global weight of 0.0431, followed by C2.1 (operational planning and control) at 0.0393, and C2.3 (improvement, corrective actions, and continual improvement) at 0.0301. These results underscore the importance of continuous oversight, process discipline, and operational governance in maintaining ISMS effectiveness. In the technological domain, C6.1 (user endpoint and privileged access management) at 0.0205, C6.2 (access restrictions and source-code controls) at 0.0202, and C6.3 (secure authentication and identity management) at 0.0172 emerge as leading sub-criteria, highlighting the essential role of technical access controls, secure configurations, and user identity protection in digitally interconnected CE infrastructures.

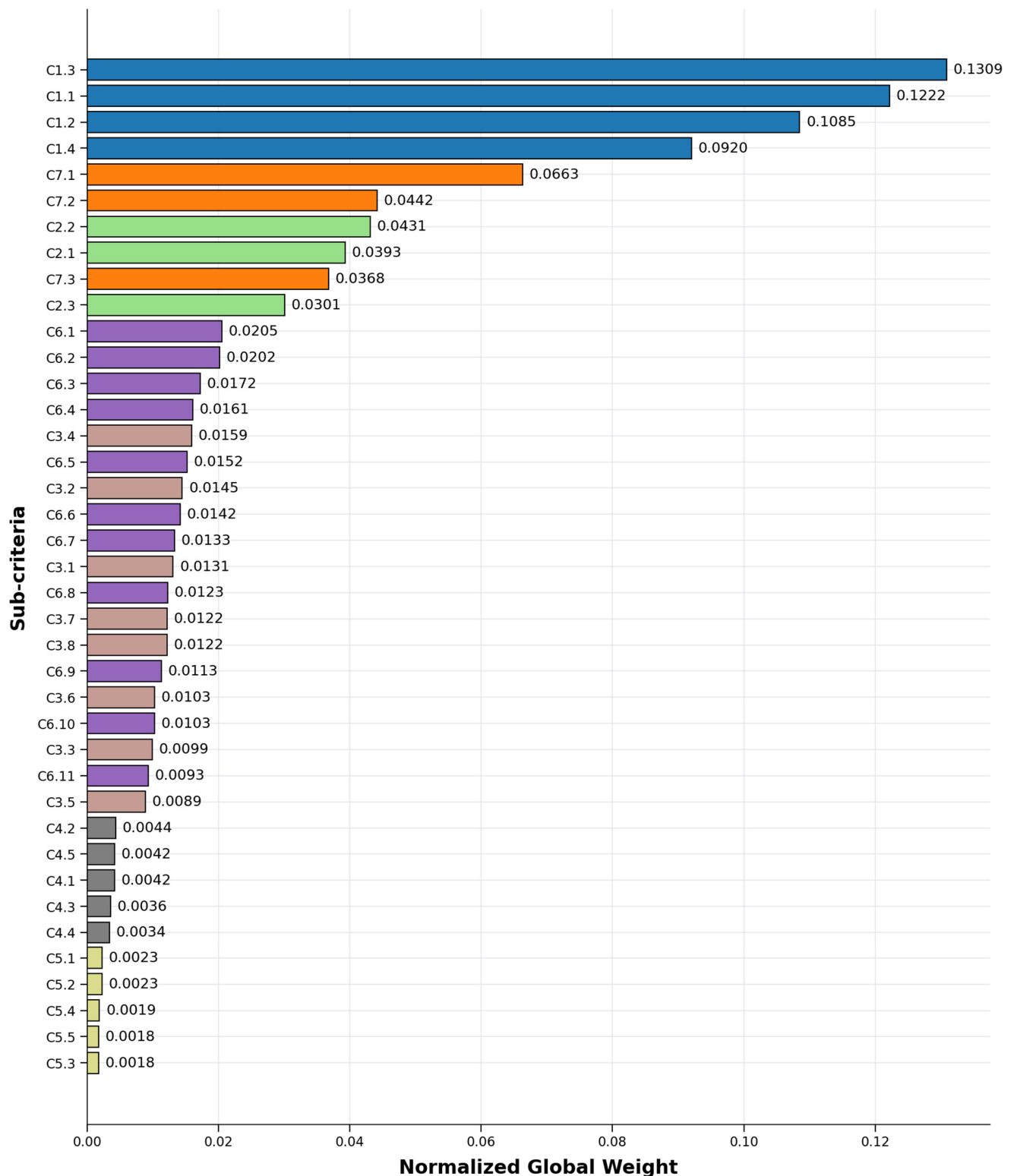


Figure 3. Normalized Global weights for the sub-criteria.

Organizational controls contribute a moderate level of global influence. Noteworthy examples include C3.4 (information classification, labeling, and handling) at 0.0159, C3.2 (Roles, responsibilities, segregation of duties) at 0.0145, and C3.1 (information security policies) at 0.0131, all reinforcing structured information governance and clear responsibility assignment. Lower-weighted but still relevant organizational sub-criteria include C3.7 (incident management planning and readiness) and C3.8 (legal, regulatory, and IP

compliance) at 0.0122, C3.6 (information transfer, acceptable use, asset management) at 0.0103, and C3.3 (contact with authorities and special interest groups) at 0.0099.

People and physical controls are positioned in the lower tier of the global ranking. Sub-criteria like C4.2 (awareness, education, and training) at 0.0044, C4.1 (screening and employment conditions) and C4.5 (remote working and confidentiality agreements) at 0.0042 each contribute modest yet crucial influence. Physical protections—C5.1 (physical security perimeters and entry controls) and C5.2 (securing offices, rooms, and facilities) at 0.0023, and C5.3–C5.5 ranging from 0.0018 to 0.0019—play supportive roles consistent with the digitalized nature of CE systems, where cyber-physical exposure remains relevant but less dominant than governance, regulatory, and technological elements.

In summary, the global weight ranking highlights a clear trend. The most influential sub-criteria stem from ISMS governance and regulatory alignment, followed by critical technological and operational controls, with organizational, people, and physical measures forming the supportive layers of the hierarchy. This distribution underscores that cyber-security readiness in smart circular economy systems is fundamentally shaped by robust governance foundations, regulatory compliance, and technical access management, all of which are essential for building resilient and trustworthy digital ecosystems.

4.3. Consistency Assessment and Sensitivity-Robustness Evaluation

The consistency ratios (CR) for all pairwise comparison matrices in the Fuzzy AHP were calculated to assess the logical soundness and reliability of expert evaluations. Figure 4 shows that the CR value for the main criteria matrix was 0.0535, indicating that the corresponding judgments meet the standard consistency requirement. Likewise, the CR values for all sub-criteria matrices across the seven main categories were below the accepted threshold of 0.1, ranging from 0.0199 to 0.0736. These results suggest that all comparison matrices exhibit satisfactory consistency, thereby reinforcing the robustness and credibility of the applied Fuzzy AHP decision-making framework.

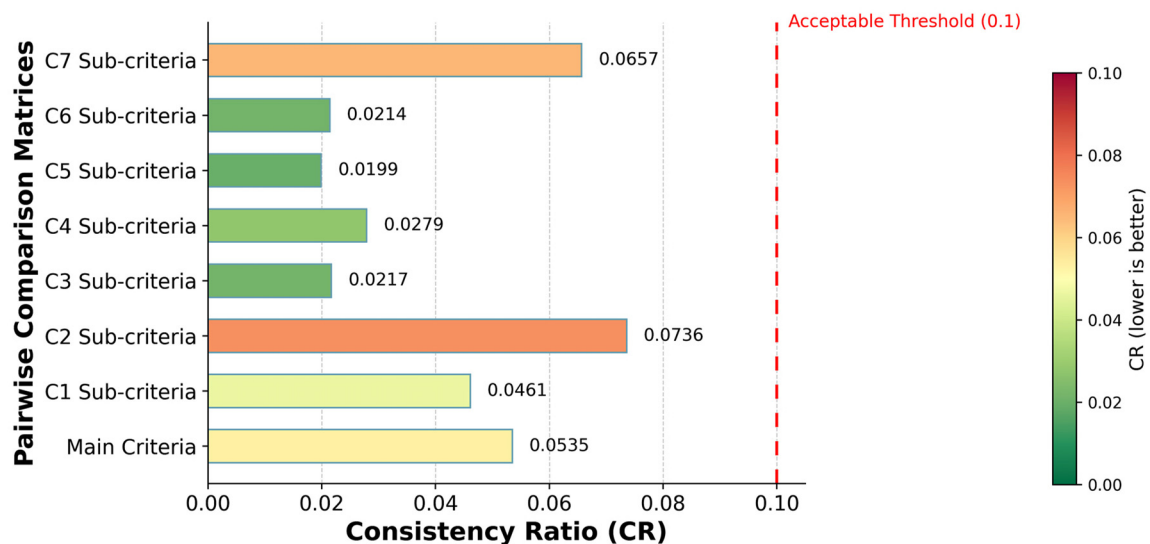


Figure 4. Consistency ratio (CR) results for AHP pairwise comparison matrices.

To evaluate the robustness and stability of the weighting structure assigned to the main criteria, a sensitivity analysis was carried out by perturbing each criterion's weight by $\pm 10\%$ and observing the resulting redistribution of the remaining weights. The adjustment process followed a proportional recalibration formula described in Equation (11), which ensures that the total weight always sums to one, thereby preserving the internal balance and mathematical consistency of the model.

When the weight of each criterion was increased by 10%, the results (shown in the corresponding heatmap, Figure 5a demonstrated a systematic and predictable reallocation among the other criteria. Increasing the weight of a criterion led to a reduction in the weights of the remaining criteria, with the extent of reduction dependent on the original influence of the increased criterion. Notably, boosting the weight of C1 (ISMS governance and organization), a highly influential criterion in the original model, caused a significant decrease in the weights of all other criteria. Conversely, adjusting a lower-weighted criterion like C5 (physical controls) resulted in minor changes. This consistent and proportional redistribution pattern indicates that the model can withstand moderate increases without becoming overly sensitive, even when applied to dominant criteria.

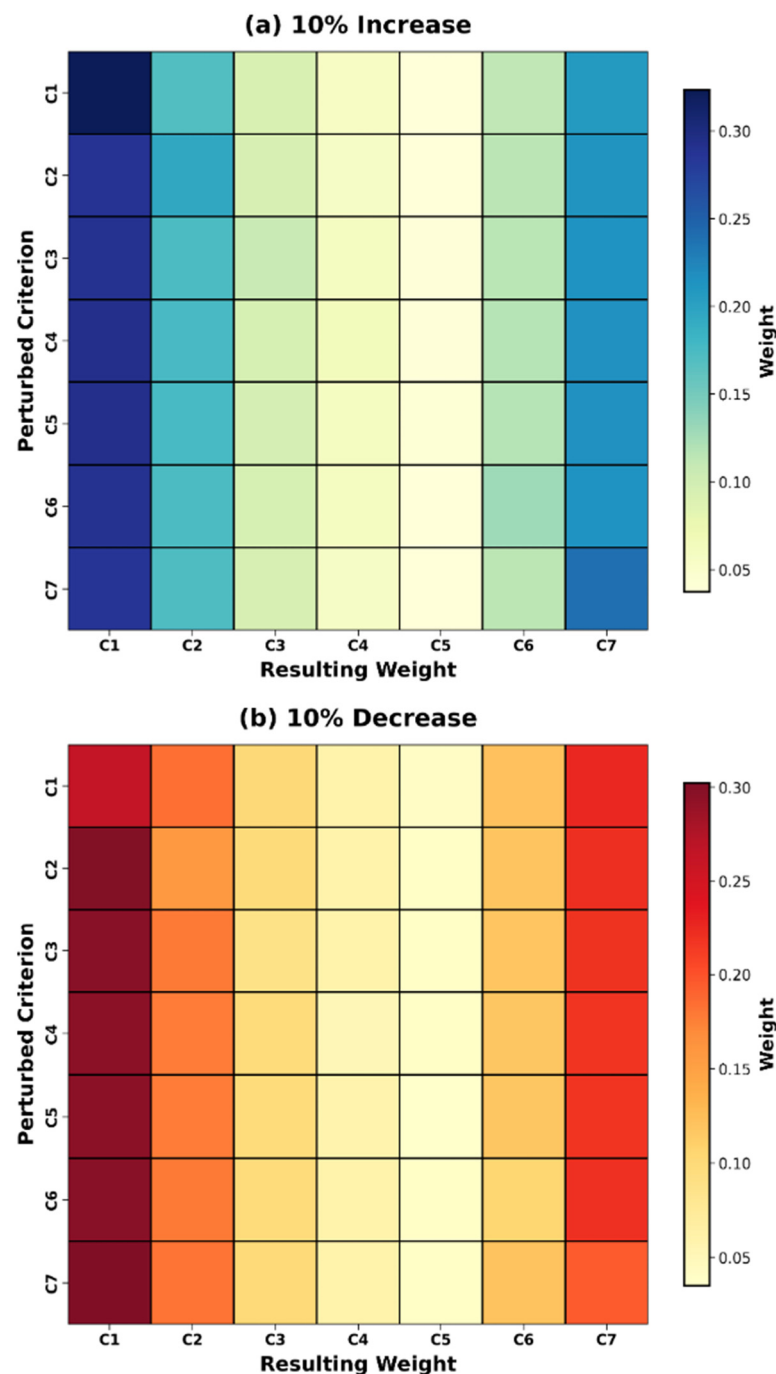


Figure 5. Sensitivity analysis of main criteria weights: (a) impact of 10% increase, (b) impact of 10% decrease.

A similar proportional response was observed when each criterion's weight was decreased by 10%, as depicted in Figure 5b. Decreasing the weights of higher-weight criteria, particularly C1 and C7, led to more substantial increases in the remaining criteria to compensate for their larger initial share of the total weight. On the other hand, reducing the weights of criteria like C4 (people controls) or C5 (physical controls), which had lower weights initially, caused minimal shifts in the redistribution. The model exhibited a controlled and linear behavior, with no irregular or disproportionate effects observed during any of the decreases.

To assess the reliability and stability of the decision-making structure at a more granular level, a sensitivity analysis was conducted for all 39 sub-criteria forming the lowest tier of the cybersecurity readiness hierarchy. In this analysis, each sub-criterion's global weight was independently increased and decreased by 10%, after which the remaining weights were proportionally redistributed to preserve the overall consistency of the weighting system. The results are illustrated in Figure 6a,b, demonstrating how changes in the importance of specific sub-criteria impact the entire hierarchy.

In the 10% increase scenario, each sub-criterion's weight was increased individually while the other 38 sub-criteria were reduced proportionally. The redistribution pattern shown in Figure 6a highlights that sub-criteria with higher original weights, particularly those in governance, organizational controls, and key technological areas, produce the most noticeable system-wide shifts. For example, C1.3 (risk assessment and risk treatment planning), C1.1 (understanding context of the organization), and C1.2 (leadership and information security policy) generated more substantial downward adjustments across the other sub-criteria due to their strong initial impact within the hierarchy. Similarly, within the technological domain, sub-criteria such as C6.1 (user endpoint and privileged access management) and C6.2 (access restrictions and source-code controls) caused noticeable weight reductions in other areas, reflecting their high global importance. Sub-criteria with lower original weights, such as C5.3 (environmental and physical threat protection), C4.3 (disciplinary process), or C4.4 (responsibilities after termination), had only minimal effects when their weights were increased. Throughout these adjustments, the system maintained a proportional and stable recalibration, without any sudden or erratic shifts, indicating that the model remains predictable even with moderate changes in weights.

The scenario of 10% decrease resulted in a corresponding behavior. When the weight of each sub-criterion was reduced, the weights of the remaining sub-criteria were increased proportionally. Figure 6b shows that sub-criteria with stronger original influence again produced more pronounced redistributions across the system. Decreasing high-impact elements such as C1.3 (risk assessment and risk treatment planning), C7.1 (standards coverage against CRA requirements), and C1.1 (understanding context of the organization) resulted in visible weight increases among numerous other sub-criteria, since reducing a dominant factor creates more available weight to be redistributed. In the realm of technology, reductions in C6.3 (secure authentication and identity management) or C6.4 (malware protection and secure configuration) also resulted in visible adjustments in the remaining sub-criteria. Conversely, reducing low-weight sub-criteria, including C5.1 (physical security perimeters and entry controls), C4.5 (remote working and confidentiality agreements), or C3.6 (information transfer, acceptable use, and asset management), generated only marginal effects. This proportional and monotonic response confirms that the model behaves coherently and does not exaggerate the influence of low-weight sub-criteria when subjected to decreases.

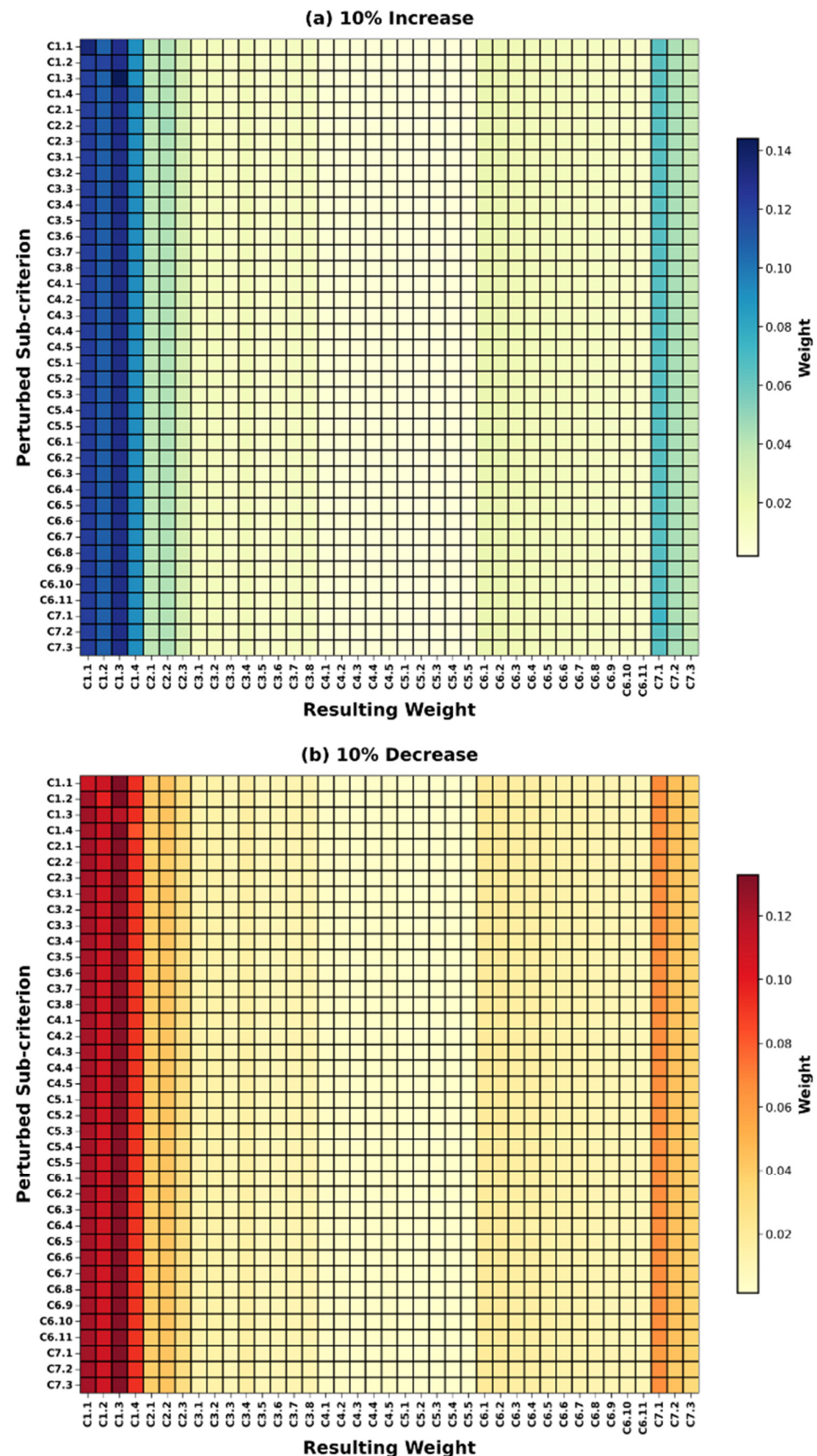


Figure 6. Sensitivity analysis of sub-criteria weights: (a) impact of 10% increase, (b) impact of 10% decrease.

In addition to the sensitivity analysis, a robustness evaluation was performed using various indicators, including Spearman ρ , RSI, MDP, and CST. The results in Table 5 show that the order of criteria rankings remained consistent even with $\pm 10\%$ weight

perturbations, with ρ and RSI both equal to 1.00, indicating a stable rank order despite slight variations in weights. The DP of the criteria ranged from 17.70% for C6 to 105.70% for C1, highlighting the varying importance of each criterion relative to the others. The MDP of 105.70% corresponds to C1, indicating its dominance within the system. No changes in rank order occurred within a 10% perturbation, as the CST for all criteria exceeded 10%. The first potential rank change would occur for C3 at a 21% perturbation, demonstrating the robustness of the ranking structure.

Table 5. Robustness results for main criteria.

Criterion	DP (%)	Spearman ρ	RSI
C1	105.70	1.00	1.00
C2	23.60	1.00	1.00
C3	32.00	1.00	1.00
C4	59.00	1.00	1.00
C5	72.70	1.00	1.00
C6	17.70	1.00	1.00
C7	51.90	1.00	1.00
Overall			
MDP (%)	105.7	—	—
CST (%)	—	—	21

Table 6 displays the robustness indicators for the 39 sub-criteria, showing that all perturbation scenarios maintained full ordinal equivalence ($\rho = 1.00$, RSI = 1.00). The DP values varied from 17.4% for C2.3 to 410.4% for C1.3, indicating the diverse importance levels among sub criteria. The maximum deviation, MDP, was associated with C1.3, emphasizing its significant role in the hierarchy. No changes in ranking occurred with the $\pm 10\%$ perturbations, demonstrating the stability of the sub criteria order. CST values for all sub criteria exceeded 10%, confirming the robustness of the hierarchy under moderate perturbations.

Table 6. Robustness results for sub-criteria.

Criterion	DP (%)	Spearman ρ	RSI
C1.1	376.50	1.00	1.00
C1.2	323.10	1.00	1.00
C1.3	410.40	1.00	1.00
C1.4	258.70	1.00	1.00
C2.1	53.20	1.00	1.00
C2.2	68.10	1.00	1.00
C2.3	17.40	1.00	1.00
C3.1	48.90	1.00	1.00
C3.2	43.50	1.00	1.00
C3.3	61.40	1.00	1.00
C3.4	38.00	1.00	1.00
C3.5	65.30	1.00	1.00
C3.6	59.80	1.00	1.00
C3.7	52.40	1.00	1.00
C3.8	52.40	1.00	1.00
C4.1	83.60	1.00	1.00
C4.2	82.80	1.00	1.00
C4.3	86.00	1.00	1.00
C4.4	86.70	1.00	1.00
C4.5	83.60	1.00	1.00
C5.1	91.00	1.00	1.00

Table 6. *Cont.*

Criterion	DP (%)	Spearman ρ	RSI
C5.2	91.00	1.00	1.00
C5.3	93.00	1.00	1.00
C5.4	92.60	1.00	1.00
C5.5	93.00	1.00	1.00
C6.1	20.10	1.00	1.00
C6.2	21.20	1.00	1.00
C6.3	32.90	1.00	1.00
C6.4	37.20	1.00	1.00
C6.5	40.70	1.00	1.00
C6.6	44.60	1.00	1.00
C6.7	48.10	1.00	1.00
C6.8	52.00	1.00	1.00
C6.9	55.90	1.00	1.00
C6.10	59.80	1.00	1.00
C6.11	63.70	1.00	1.00
C7.1	158.50	1.00	1.00
C7.2	72.30	1.00	1.00
C7.3	43.50	1.00	1.00
Overall			
MDP (%)	410.40	—	—
CST (%)	—	—	>10

Collectively, these findings demonstrate that the hierarchical weighting structure maintains both the relative importance of main criteria and sub-criteria, as well as the overall ranking order, providing strong confidence in the reliability, robustness, and resilience of the derived model under moderate perturbations.

5. Discussion and Implications

5.1. Governance and Regulatory Alignment as Foundational Determinants

The analysis clearly indicates that organizational governance and regulatory compliance are key factors in determining of cybersecurity readiness in smart CE systems. This aligns with previous studies on ISO/IEC 27001:2022, which emphasize that the revised standard reinforces the primacy of organizational context, leadership accountability, and risk-based planning as central pillars of an effective ISMS [6]. Stakeholder-focused research additionally demonstrates that ISO/IEC 27001:2022 should be viewed as a governance system, rather than just a technical compliance mechanism, emphasizing the need for managerial engagement, capability building, and strategic coherence [40].

The prominence of governance in these findings is also consistent with broader empirical research showing that governance deficiencies are frequently the root cause of cybersecurity failures, whereas robust governance frameworks foster accountability, strategic alignment, and effective risk oversight. A systematic review of public-sector information-security governance highlights the necessity of aligning security initiatives with recognized governance frameworks and regulatory expectations for sustainable security outcomes [16]. Complementary analyses of cybersecurity governance frameworks further emphasize that resilient digital ecosystems require integrated and adaptive governance mechanisms capable of regulating cross-functional risk, coordinating interdependent systems, and responding to dynamically evolving threat landscapes [41].

The significance of regulatory alignment observed in the results must be interpreted in light of recent European cybersecurity legislation. The EU Cyber Resilience Act (CRA),

which entered into force in December 2024, introduces binding cybersecurity requirements for products with digital elements across their entire lifecycle, representing a significant shift from voluntary best practices to mandatory compliance requirements [42]. Legal analyses of the CRA describe it as a horizontally applied, risk-based, product-safety-inspired framework, imposing obligations related to secure-by-design engineering, vulnerability mitigation, conformity assessments, and post-market surveillance [43]. This body of research emphasizes that CRA compliance cannot be isolated as a legal function but must be structurally integrated into product development, engineering workflows, supply-chain management, and operational assurance processes. Technical analyses of the CRA's risk-management provisions also demonstrate that the regulation requires organizations to embed risk governance directly into their software-development and system-engineering practices to ensure durable conformity under changing operational conditions [44].

Taken together, these findings show that cybersecurity readiness in smart CE systems results from the interplay between internal governance capabilities and external regulatory obligations. Governance provides the foundation for cybersecurity efforts, while regulatory alignment, particularly through the CRA, shapes system design, implementation, and ongoing practices. This underscores that cybersecurity in smart CE environments is not just a technical challenge but a governance-regulated business function that requires ongoing leadership involvement, risk-aware planning, and continuous regulatory compliance.

5.2. Operational and Technological Controls as Mechanisms for Enacting Governance

The study's results position operational and technological safeguards within the middle tier of influence. While they may not define readiness at the strategic level, they are essential or implementing governance intentions in daily operations. Monitoring, internal auditing, and performance-review activities are highlighted in this tier, emphasizing the importance of ongoing oversight to ensure that security measures function effectively in dynamic operational environments [45]. This interpretation is consistent with analyses of ISO/IEC 27001:2022, which emphasize that continuous evaluation and the structured feedback loop of the standard's performance-evaluation clauses are critical for maintaining the alignment between intended policy direction and actual security outcomes [6].

The study also shows that technical safeguards, particularly those governing endpoints, privileged access, and authentication, carry significant influence within this middle tier. These findings reflect evidence from enterprise identity-management research, which identifies access governance as a cornerstone of actual breach-prevention capability in increasingly interconnected digital systems [46]. Similarly, peer-reviewed analyses of IoT-dense and cyber-physical infrastructures underscore that disciplined access control, secure configuration, and continuous monitoring are essential for limiting lateral movement across heterogeneous devices and distributed data flows—conditions characteristic of circular-economy digital ecosystems [47].

Further reinforcement for this structural pattern comes from multi-criteria decision-making studies, which repeatedly identify monitoring, vulnerability management, and access governance as high-impact domains for organizations prioritizing controls under uncertainty [12]. These analytical approaches demonstrate that the effectiveness of technical safeguards depends on the existence of an accompanying operational review cycle capable of detecting anomalies, verifying performance, and triggering managerial action. The study's observed configuration—where operational oversight and technical enforcement jointly anchor the middle tier—aligns with this conceptualization, illustrating that readiness in digitally intensive CE systems is sustained through the coordinated interplay of visibility, verification, and technical control execution [47].

5.3. Organizational, Human, and Physical Controls as Contextual Stabilizers

The study's empirical distribution of control importance indicates that organizational, human, and physical controls play a complementary role in cybersecurity readiness rather than a determinative one. These controls contribute to procedural clarity, behavioral consistency, and baseline environmental protection, but they do not have as significant an impact on cybersecurity readiness as governance-focused or technologically mediated domains. This moderated influence is due to the operational characteristics of digitally intensive CE systems, where cyber-technical interactions and automated data processes drive systemic exposure, reducing the comparative leverage of controls grounded in administrative structures, human behavior, or physical premises [48].

Among these controls, those related to awareness, education, and training are positioned more strongly, indicating that human-centric interventions are strategically valuable in mitigating social-engineering risks and supporting compliance behaviors across organizational units. Empirical analyses of cybersecurity-awareness programs consistently show that continuous, scenario-based education produces more substantive and durable reductions in user-level vulnerability than one-off or punitive approaches [49]. Complementary systematic reviews further highlight that, although training effectiveness can decay without reinforcement, it remains an essential enabler of secure practices, particularly in environments where technological and operational controls depend on correct user behavior to function effectively [50]. The study's prioritization within human-related controls therefore aligns with broader empirical findings that emphasize proactive competence-building as a necessary, though not independently decisive, dimension of organizational security.

Organizational controls, such as policies, role definitions, and information-classification routines, have a lower range of influence as they primarily shape the context rather than directly reduce risks. In cyber-physical and hybrid digital systems, administrative measures provide internal coherence but have less control over attack surfaces compared to measures influencing access pathways, system configuration, or real-time monitoring functionality [51]. This distinction is particularly relevant in CE ecosystems where risk propagates through technical interfaces and interconnected devices.

Physical controls, such as facility protection, environmental safeguards, and equipment-security measures, are considered to have the least influence within the study's hierarchy. This aligns with current analyses of cyber-physical and IoT-integrated systems, which show that the majority of modern attack vectors exploit digital pathways, remote connectivity, or identity-based vulnerabilities rather than breaches of physical perimeters [52]. Although necessary to provide baseline protection, physical controls exert limited influence on readiness in environments where software, data flows, and device interconnectivity dominate the operational risk landscape.

In sum, these findings indicate that organizational, human, and physical controls play a supporting role in the readiness model. They bolster the more influential governance, operational, and technological domains but do not drive significant improvements in overall cybersecurity posture on their own. Despite this, their role is crucial in maintaining coherence, aligning user behavior with technical requirements, and establishing the foundational conditions for higher-impact controls to function effectively.

5.4. Integrated Perspective from the Global Ranking of Factors

The global prioritization pattern produced in this study—derived by integrating local sub-factor preferences with their broader categorical domains—indicates that factors related to risk assessment and treatment, organizational contextual analysis, and leadership-driven information-security policy have the strongest influence on cybersecurity readiness within digitally intensive CE settings. This aligns with contemporary analyses of security-

management standards, emphasizing that readiness is rooted in governance structures that shape risk interpretation, how strategic priorities, and policy implementation within organizations [5]. The prominence of these high-level elements in the global ordering therefore reflects an architecture in which readiness originates from strategic direction and institutional coordination.

A central insight emerging from the prioritization is the elevated position of regulatory alignment, particularly concerning the European Union's evolving cybersecurity framework. Analyses of the CRA show that the regulation applies horizontally to "products with digital elements," mandating secure-by-design development, coordinated vulnerability handling, conformity assessment, and post-market security obligations that extend across the entire product lifecycle [53]. These requirements effectively bind engineering, maintenance, supplier management, and documentation practices to compliance-driven expectations that must be demonstrably fulfilled for continued market access. Complementary legal scholarship on the NIS2 Directive highlights strengthened risk-management obligations, incident-reporting duties, supply-chain oversight, and heightened enforcement mechanisms—factors that further integrate regulatory compliance with organizational governance practices [54]. The global prioritization produced in this study mirrors this regulatory landscape by placing lifecycle conformity among the most influential determinants of readiness, thereby showing that CE cybersecurity is not merely a matter of internal policy but also of externally imposed obligations.

The global results also shed light on the operational and technical pathways through which governance and regulatory direction are enacted in practice. The prominence of monitoring, internal auditing, and management review within the operational domain is consistent with established evaluation frameworks that emphasize continuous assessment and structured review cycles as foundational mechanisms for validating the effectiveness of implemented controls. Studies of cyber-physical-human systems highlight that system performance and security integrity depend on iterative feedback loops that detect deviations and support timely corrective action, particularly in environments characterized by tightly coupled digital and organizational processes [55]. Parallel analyses within zero-trust and IoT security research similarly position ongoing control verification and dynamic reassessment as prerequisites for maintaining alignment between intended security objectives and observed system behavior, especially as threat conditions and device interactions evolve in real time [56]. These converging perspectives provide a conceptual basis for the strong influence attributed to evaluation-centric operational elements in the global configuration.

From a technical standpoint, the influence attributed to access-centric enforcement corresponds with dominant threat patterns in interconnected CE infrastructures. In IoT-dense contexts, scholarship shows that the combination of robust identity governance, advanced authentication, and fine-grained authorization is central to preventing credential-driven escalation and inhibiting cross-device propagation of compromise in heterogeneous device ecosystems [46]. Broader treatments of identity management evolution and challenges converge on the need to operationalize principled access discipline, spanning account lifecycle controls, entitlement hygiene, and privileged-access regulation, to sustain resilience as device populations, integration points, and usage patterns evolve [57].

The prioritization also reflects the growing significance of software-supply-chain assurance, particularly in CE infrastructures with distributed components and nested dependencies. Recent work examining the linkage between software bills of materials (SBOMs) and EU cybersecurity regulations highlights the embedding of transparency and component-level traceability within compliance regimes, reinforcing the notion that readiness increasingly depends on the organization's capacity to produce verifiable evidence of component integrity and vulnerability status throughout the product lifecycle [58]. These

insights correspond with the influential position of regulatory-alignment factors in the global ordering, as supply-chain assurance becomes a core component of compliance under the CRA and NIS2 frameworks.

Overall, the synthesized global configuration outlines a coherent structure of readiness within CE systems. Strategic governance establishes risk priorities and directs resource allocation. Regulatory alignment sets binding expectations that shape product design, development, and lifecycle oversight. Operational monitoring provides the feedback mechanisms necessary for validating performance and sustaining conformity. Access-focused technical controls enforce the boundary conditions of trust across heterogeneous device ecosystems. This system-level alignment is essential for stability and resilience in interconnected cyber-physical-human processes within CE environments.

5.5. Theoretical Implications for Cybersecurity Readiness in CE Systems

The study's prioritization structure provides valuable theoretical insights into how cybersecurity readiness emerges within CE systems, which are characterized as highly interconnected socio-technical environments. A first implication concerns the systemic nature of readiness. Rather than arising from isolated technical measures or discrete organizational practices, the findings suggest that readiness is fundamentally shaped by the interactions among multiple interdependent subsystems across social, technical, organizational, and environmental layers. This interpretation is consistent with recent extensions of socio-technical systems theory, which conceptualize cybersecurity challenges as emergent properties of complex assemblages involving human actors, institutional structures, technological infrastructures, and external environmental factors [59]. Such work underscores that governance conditions, institutional expectations, and contextual dynamics co-produce system behavior in ways that cannot be reduced to technology alone.

A second implication relates to the role of regulatory structures in shaping theoretical models of readiness. Contemporary analyses of cyber crisis-management capabilities emphasize that regulatory design, institutional clarity, and formalized security expectations function as structural anchors that shape the strategic, operational, and tactical dimensions of cybersecurity across complex ecosystems [60]. These findings correspond with the study's identification of regulatory alignment as an influential determinant, implying that readiness in CE contexts is best theorized not as an internally generated organizational capability but as a co-regulated outcome, shaped by multi-level institutional frameworks, compliance architectures, and cross-sector governance mechanisms.

A third theoretical contribution highlights the significance of adaptive feedback processes as fundamental mechanisms within CE security ecosystems. Research on cyber-physical-social systems (CPSS) demonstrates that system reliability and resilience depend on the continuous circulation of information across cyber, physical, and social layers, enabling dynamic adjustment to changes in system state, user behavior, and contextual conditions [61]. This theoretical framing aligns with the study's emphasis on operational evaluation mechanisms, such as monitoring and management review, as readiness-enhancing components—not because they act as controls themselves but because they sustain the feedback loops needed to maintain coherence in evolving system conditions.

The fourth contribution pertains to theories of identity governance and access regulation within distributed digital ecosystems. Recent work in industrial identity-management research indicates that authentication robustness, access-control granularity, and identity lifecycle governance constitute foundational elements for mitigating security risks in industrial and IoT-intensive environments where device heterogeneity and machine-to-machine interactions challenge traditional security assumptions [62]. This body of literature posits that identity governance serves not merely as a technical safeguard but as a structural regu-

lator of trust relationships among components, thereby providing a theoretical foundation that views access control as a determinant of risk propagation patterns within complex cybersecurity infrastructures.

Lastly, the role of supply-chain assurance in the prioritization emphasizes theoretical discussions regarding interconnected cyber-risk ecologies. Research in supply chain cyber-risk management demonstrates that resilience emerges from coordinated internal and external integration mechanisms, linking suppliers, customers, and organizational units. Furthermore, effective governance structures can synchronize risk management routines across distributed networks. This perspective promotes an ecosystem-level understanding of cybersecurity rather than a firm-bound approach [63]. Accordingly, it aligns with the study's findings by framing supply chain assurance as an ecosystem-level capability rather than a firm-bounded function.

5.6. Practical and Managerial Implications for CE Cybersecurity Readiness

Enhancing cybersecurity readiness in CE environments necessitates that managers translate prioritization outcomes into concrete, repeatable operational routines. Instead of perceiving security as merely an endeavor, organizations must emphasize daily operational behaviors, including task execution, responsibility assignment, and coordination across teams and partners. In CE settings, where digital processes interact continuously with material flows, readiness significantly contingent upon whether routine operational decisions consistently incorporate security requirements.

A primary implication of this approach is the integration of cybersecurity tasks into existing operational workflows, rather than treating them as separate procedures. Empirical evidence indicates that embedding security checks into standard work routines, such as maintenance approvals, shift handovers, configuration updates, and production scheduling, mitigates oversight gaps and enhances execution consistency [64]. This approach ensures that cybersecurity considerations are not postponed, isolated, or addressed in a reactive manner, but instead become intrinsic to CE operational cycles.

Furthermore, clear task ownership is vital. Numerous CE environments consist of dispersed teams responsible for equipment, data, transport, and digital services, which increases the likelihood of routine security actions becoming neglected. Research in high-reliability digital operations demonstrate that formally assigning responsibility for routine activities, such as daily log review, configuration integrity checks, user verification, and contract compliance, reduces ambiguity and ensures accountability throughout the system lifecycle [65]. Consequently, managers should meticulously delineate tasks, specifying who is responsible for each task, the frequency of completion, and the expected evidence of performance.

The results of prioritization also underscore the importance of structured operational sequencing to guide resource allocation. As not all actions can be prioritized simultaneously, CE organizations often operate under significant staffing and time constraints. Studies on operational decision-support methods reveal that understanding the interrelationships between tasks helps managers identify which actions drive the greatest downstream effect, thereby enabling the allocation of limited resources to interventions that provide the highest operational leverage [66]. This strategic focus allows CE managers to prioritize tasks that reinforce the overarching readiness framework, such as enhancing oversight routines, improving internal communication channels, or standardizing review processes.

Another critical factor is maintaining discipline in routine verification. Regularly scheduled assessments—such as daily oversight of system states, weekly anomaly evaluations, monthly access reviews, and quarterly operational drills—have proven effective in sustaining stable performance within dynamic digital-physical environments. Research derived from hybrid decision-support studies suggests that verification routines are more

reliable when supported by structured checklists, simple record-keeping templates, and predefined review intervals [67]. CE organizations can implement these methodologies to achieve consistent security performance, even amidst fluctuating operational conditions.

Given that CE systems often rely on external service providers, refurbishers, and logistics partners, effective readiness also depends on coordinated interaction with external parties. Empirical research on cyber-crisis coordination demonstrates that predefined communication protocols, shared response expectations, and mutual availability commitments significantly improve response effectiveness during disruptions [60]. Therefore, managers must ensure that agreements with partners clearly define escalation paths, notification timelines, and operational constraints.

Finally, CE initiatives that leverage shared data platforms and involve multiple organizations benefit from mechanisms that promote operational transparency. These include maintaining accessible audit trails, consistent reporting routines, and clear privacy-protection practices. Research on public-sector cyber-physical infrastructures indicates that such transparency mechanisms foster trust among participants and support consistent operational behavior across organizational boundaries [68]. CE operators should consider adopting these measures to align expectations and mitigate friction in cross-organizational collaborations.

To illustrate how these implications may be operationalized in practice, consider a hypothetical circular-economy organization operating a digitally enabled material-recovery and logistics system. Such an organization could apply the proposed framework by assessing its current performance against the identified cybersecurity readiness criteria using existing operational evidence, including maintenance records, audit documentation, access logs, training registers, and partner agreements. The FAHP-derived weights would then be used to aggregate these assessments into domain-level readiness scores, allowing managers to distinguish between high-priority governance or coordination gaps and lower-impact technical deficiencies. For example, the results may reveal that while core technological controls are routinely implemented, insufficient task ownership for risk assessment activities or incomplete coordination protocols with external logistics partners represent critical vulnerabilities due to their higher operational leverage. In response, managers could prioritize formalizing responsibility assignments, strengthening verification routines, or clarifying contractual communication procedures rather than expanding technical controls in isolation. In this way, the framework supports structured decision-making by translating prioritized cybersecurity factors into concrete, repeatable operational actions aligned with the realities of CE system operations.

Together, these implications emphasize that cybersecurity readiness in CE systems is contingent not upon isolated technical interventions but rather upon predictable, accountable, and well-structured operational practices. Essential actions include integrating cybersecurity into routine workflows, clarifying ownership responsibilities, sequencing initiatives based on operational impact, enforcing a culture of verification, strengthening partner coordination, and enhancing transparency measures. These practices are critical to sustaining robust cybersecurity performance across the interconnected operations that characterize CE systems.

5.7. Limitations of the Study

The approach adopted in this study presents a structured and transparent methodology for prioritizing cybersecurity-readiness factors. However, it is essential to recognize that, like any expert-based decision-analysis method, the conclusions derived from this study are influenced by several inherent characteristics.

Firstly, the hierarchical structure of the model arranges readiness factors in a clear top-down format. While this organization enhances interpretability and consistency, it does not explicitly address the reciprocal influences that may occur among certain factors, a limitation that is characteristic of all hierarchical MCDM approaches [67].

Secondly, the application of fuzzy logic in pairwise comparisons introduces a systematic means of capturing uncertainty in expert judgments. However, this method necessitates adherence to the mathematical properties of fuzzy numbers. Prior methodological analyses have indicated that the behavior of fuzzy arithmetic, especially the widening of intervals during aggregation, should be viewed as an expression of expert uncertainty managed transparently, rather than as a methodological deficiency [69]. This characteristic is typical in evaluations based on fuzzy sets.

Thirdly, the insights derived from experts reflect the perspectives of academic specialists with demonstrated experience in cybersecurity and CE-related digital systems. While this ensures a certain level of conceptual rigor, it may not encapsulate the full spectrum of viewpoints from operational personnel, CE industry practitioners, or regulatory actors. Existing reviews of decision-making in cybersecurity emphasize that expert-based approaches naturally reflect the background of the panel involved, and results should therefore be interpreted as representing this specific expert cohort [70].

Fourthly, the study relies predominantly on expert judgment rather than empirical operational metrics. This aligns with the normative intent of readiness assessment but means that the resulting weights reflect perceived importance rather than observed performance trends. The literature in information systems decision support notes that this characteristic is typical of expert-driven models and does not undermine their efficacy for strategic and managerial decision-making [71].

Finally, although the sensitivity analysis confirmed the internal stability of the obtained priorities, the study adopts a hierarchical modeling structure that assumes independence among evaluation criteria, which is inherent to AHP and FAHP-based approaches. In practice, cybersecurity domains such as governance, operations, supply-chain security, and regulatory compliance may exhibit interdependencies that are not explicitly represented in a hierarchical framework. For this reason, alternative modeling structures, such as network-based approaches including the Analytic Network Process (ANP), were not incorporated in the present study, as they fall outside the scope of the selected methodological framework and would introduce additional complexity at this stage of framework development. Comparative research shows that hierarchical and network-based approaches each highlight different aspects of complex systems, and the selection of one framework necessarily defines how relationships are represented [66]. The proposed framework is therefore intended as a universal, standards-based reference model, and its application in specific sectors or organizational contexts may require contextual tailoring to reflect sector-specific risks, regulatory environments, and operational characteristics.

6. Future Research Directions

Building upon the findings of this study, several avenues exist for extending the analytical depth and practical applicability of cybersecurity-readiness assessment within CE systems. One significant area for advancement is the development of models that accurately capture interdependencies among readiness factors, particularly in light of the interconnected nature of digital technologies and CE operational loops. Although hierarchical models provide transparency, there is substantial value in adopting approaches that represent mutual influences, cascading effects, and cross-domain feedback mechanisms. Recent research examining digital technologies in the context of CE transitions emphasizes that dependencies across organizational, technological, and lifecycle processes profoundly affect overall system

performance. This underscores the necessity for modeling techniques that can adequately reflect such interconnected dynamics [72], thereby fostering a more holistic understanding of how security-related changes in one domain may impact the broader CE landscape.

Furthermore, an essential direction for future inquiry involves broadening stakeholder representation within cybersecurity readiness evaluations. CE systems inherently encompass a diverse range of actors, including manufacturers, refurbishers, platform operators, logistics partners, and regulatory bodies. By expanding expert panels to reflect this diversity, more operationally grounded and widely applicable readiness profiles may be developed. Systematic analyses of the challenges faced during CE implementation highlight the critical importance of cross-actor coordination and inclusive governance structures for establishing reliable and scalable circular-economy practices [73]. Incorporating these varied perspectives into cybersecurity assessments would enhance decision-making processes and strengthen the legitimacy of resulting priorities.

A significant future direction for this research involves the empirical validation of readiness scores. While the current study emphasizes the construction and validation of the weighting logic through consistency and robustness analysis, demonstrating readiness scores prior to and following prioritization—and comparing these scores with actual audit outcomes—necessitates access to detailed cybersecurity audit data. Such data are typically confidential, organization-specific, and subject to regulatory or contractual restrictions, thereby limiting their inclusion in this study.

Future work may also enhance the adaptability of the proposed model by incorporating evolving cybersecurity frameworks and domain-specific guidance. As cybersecurity threats, technologies, and regulatory obligations continue to progress, it will be essential to periodically recalibrate the weighting structure established in this study. The hierarchical framework may be expanded to incorporate alternative standards, such as the NIST Cybersecurity Framework or NIST SP 800-53. This would facilitate comparative analyses across different governance ecosystems and ensure the model's ongoing relevance in dynamic CE environments. Moreover, it is advisable to regularly update the expert panel and refresh readiness weights over time to bolster the model's responsiveness to emerging risks, innovative technologies, and shifts in digital infrastructure practices within the CE.

An additional opportunity exists in the exploration of diverse MCDM formulations that can complement or extend hierarchical techniques. Comparative analyses of modeling approaches in CE and digital-transition research show that methods capturing causal relations, network effects, or temporal sequences can reveal insights not evident in strictly hierarchical structures [74]. Implementing such approaches within CE cybersecurity contexts could support methodological triangulation and validate whether different analytical perspectives yield consistent prioritization outcomes.

Extending this trajectory, future investigations may consider the development of sector-specific or platform-specific readiness models tailored to CE domains characterized by distinct technological and operational profiles. Research on digital-platforms and CE systems indicates that data governance structures, coordination requirements, and infrastructure maturity can vary widely across application areas such as waste-exchange platforms, reverse-logistics systems, or refurbishment marketplaces [75]. Consequently, developing domain-adapted assessment tools would enhance practical relevance and ensure that cybersecurity-readiness guidance aligns with the operational realities of diverse CE implementations.

7. Conclusions

This study presents a structured framework for evaluating cybersecurity readiness in smart CE systems, integrating the requirements of ISO/IEC 27001 with CRA-aligned regulatory expectations. By extracting criteria and sub-criteria from clause-based ISMS provisions,

Annex A controls, and CRA standards-mapping, the research offered a comprehensive and logically grounded representation of the multidimensional factors that shaped cybersecurity posture in digitally intensive CE environments. The evaluation process employs Fuzzy AHP to prioritize these criteria effectively. The analysis reveals that readiness is shaped by the interplay of governance capacity, regulatory compliance, operational oversight, and technological enforcement, all supported by organizational, human, and physical safeguards.

The findings provided several practical implications. Firstly, enhancing governance-driven elements such as risk assessment practices, contextual analysis, and leadership-led policy direction is crucial, as these elements serve as the structural foundation for other controls. Secondly, the significant emphasis on regulatory alignment underscores the necessity for proactive adaptation to evolving EU cybersecurity legislation, particularly the CRA. Thirdly, the prioritization of operational and technical controls suggests that readiness is contingent not only on robust technologies but also on consistent oversight mechanisms capable of sustaining secure performance over time.

Looking ahead, future research should consider modeling approaches that capture the interdependencies among factors contributing to readiness, expand assessments to incorporate empirical operational data, and tailor frameworks to sector-specific CE domains. Such advancements would refine analytical precision and enhance the practical relevance of readiness evaluations within increasingly complex and interconnected cyber-physical ecosystems.

Author Contributions: Conceptualization, S.A.A.-B. and M.N.S.; methodology, S.A.A.-B. and M.N.S.; software, S.A.A.-B.; data curation, S.A.A.-B. and M.N.S.; writing—original draft preparation, S.A.A.-B. and M.N.S.; writing—review and editing, S.A.A.-B. and M.N.S.; visualization, S.A.A.-B. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by national funds through FCT—Fundação para a Ciência e a Tecnologia I.P., under the project CESAM—Centro de Estudos do Ambiente e do Mar, references UID/50017/2025 (<https://doi.org/10.54499/UID/50017/2025>) and LA/P/0094/2020 (<https://doi.org/10.54499/LA/P/0094/2020>), and by the ERA Chair BESIDE project financed by the European Union's Horizon 2020 research and innovation program under grant agreement No. 951389 (<https://doi.org/10.3030/951389>).

Institutional Review Board Statement: According to EU GDPR (Regulation (EU) 2016/679) and national regulations in Portugal, anonymous expert-opinion studies that do not involve personal data are exempt from Ethics Committee/IRB approval. Ethical review and approval were waived for this study because it involved only anonymous expert judgments and collected no personal or sensitive data.

Informed Consent Statement: According to EU GDPR (Regulation (EU) 2016/679) and national regulations in Portugal, anonymous expert-opinion studies that do not involve personal data are exempt from Ethics Committee/IRB approval. Informed consent was not required because no personal data were collected and expert contributions were fully anonymous.

Data Availability Statement: The original data presented in the study are openly available in Zenodo at <https://zenodo.org/records/18769991>, accessed on 25 February 2026.

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

References

1. Ozturk, I.; Topuz, E. Quantification of Sustainability Index for the Wastewater Recovery Technologies: A Decision Support Approach for Circular City Adaptations. *Int. J. Environ. Sci. Technol.* **2023**, *20*, 9963–9980. [CrossRef]
2. Noor, A.F.M.; Moghavvemi, S.; Tajudeen, F.P. Identifying Key Factors of Cybersecurity Readiness in Organizations: Insights from Malaysian Critical Infrastructure. *Comput. Secur.* **2025**, *159*, 104674. [CrossRef]

3. Shah, M.H.; Muhammad, R.; Ameen, N. Cybersecurity Readiness of E-Tail Organisations: A Technical Perspective. In *Responsible Design, Implementation and Use of Information and Communication Technology (I3E 2020); Lecture Notes in Computer Science*; Hattingh, M., Matthee, M., Smuts, H., Pappas, I., Dwivedi, Y., Mäntymäki, M., Eds.; Springer: Cham, Switzerland, 2020; Volume 12066, pp. 153–160.
4. Perozzo, H.; Zaghloul, F.; Ravarini, A. CyberSecurity Readiness: A Model for SMEs Based on the Socio-Technical Perspective. *Complex Syst. Inform. Model. Q.* **2022**, *33*, 53–66. [\[CrossRef\]](#)
5. Folorunso, A.; Mohammed, V.; Wada, I.; Samuel, B. The Impact of ISO Security Standards on Enhancing Cybersecurity Posture in Organizations. *World J. Adv. Res. Rev.* **2024**, *24*, 2582–2595. [\[CrossRef\]](#)
6. Malatji, M. Management of Enterprise Cyber Security: A Review of ISO/IEC 27001:2022. In *Proceedings of the 2023 International Conference on Cyber Management and Engineering (CyMaEn)*; IEEE: New York, NY, USA, 2023; pp. 117–122.
7. Tariq, M.I.; Tayyaba, S.; De-la-Hoz-Franco, E.; Ashraf, M.W.; Rad, D.V.; Butt, S.A.; Santarcangelo, V. Evaluation and Prioritization of Information Security Controls of ISO/IEC 27002:2013 for SMEs Through Fuzzy TOPSIS. In *Advances in Intelligent Data Analysis and Applications*; Springer: Singapore, 2022; pp. 271–289.
8. Styoutomo, Y.A.; Ruldeviyani, Y. Information Security Awareness Raising Strategy Using Fuzzy AHP Method with HAIS-Q and ISO/IEC 27001:2013: A Case Study of XYZ Financial Institution. *CommIT (Commun. Inf. Technol.) J.* **2023**, *17*, 133–149. [\[CrossRef\]](#)
9. Kahraman, C.; Cebeci, U.; Ulukan, Z. Multi-criteria Supplier Selection Using Fuzzy AHP. *Logist. Inf. Manag.* **2003**, *16*, 382–394. [\[CrossRef\]](#)
10. Büyüközkan, G.; Göçer, F. Digital Supply Chain: Literature Review and a Proposed Framework for Future Research. *Comput. Ind.* **2018**, *97*, 157–177. [\[CrossRef\]](#)
11. Chen, S.-J.; Hwang, C.-L. Fuzzy Multiple Attribute Decision Making Methods. In *Fuzzy Multiple Attribute Decision Making; Lecture Notes in Economics and Mathematical Systems*; Springer: Berlin/Heidelberg, Germany, 1992; pp. 289–486.
12. Tariq, M.I.; Ahmed, S.; Memon, N.A.; Tayyaba, S.; Ashraf, M.W.; Nazir, M.; Hussain, A.; Balas, V.E.; Balas, M.M. Prioritization of Information Security Controls through Fuzzy AHP for Cloud Computing Networks and Wireless Sensor Networks. *Sensors* **2020**, *20*, 1310. [\[CrossRef\]](#) [\[PubMed\]](#)
13. Bhol, S.G.; Mohanty, J.R.; Pattnaik, P.K. Enhancing Cybersecurity Metrics Evaluation Through the Application of Fuzzy Ahp Methodology. In *Intelligent Computing Systems and Applications (ICICSA 2023); Lecture Notes in Networks and Systems*; Bandyopadhyay, S., Balas, V.E., Biswas, S.K., Saha, A.K., Thounaojam, D.M., Eds.; Springer: Singapore, 2024; Volume 1010, pp. 135–147.
14. Mızrak, F. Premium E-Journal of Social Sciences. *Prem. E-J. Soc. Sci.* **2023**, *7*, 1272–1292. [\[CrossRef\]](#)
15. Simjanović, D.; Ristić, L.; Milovanović, A.; Jovanović, A. The Fuzzy AHP Approach to Evaluation of Criteria Related to Active Cyber Attacks. In *Proceedings of the BISEC 2024—15th International Conference on Business Information Security*, Niš, Serbia, 28–29 November 2024; pp. 1–9.
16. Magnusson, L.; Iqbal, S.; Elm, P.; Dalipi, F. Information Security Governance in the Public Sector: Investigations, Approaches, Measures, and Trends. *Int. J. Inf. Secur.* **2025**, *24*, 177. [\[CrossRef\]](#)
17. Kekgathetse, M.; Lucas, B.; Sebapalo, M. A Systematic Review on Cyber Security Integration in Information Technology Governance. In *Proceedings of the 2024 International Conference on Electrical and Computer Engineering Researches (ICECER)*; IEEE: Gaborone, Botswana, 2024; pp. 1–6.
18. Brezavšček, A.; Baggia, A. Recent Trends in Information and Cyber Security Maturity Assessment: A Systematic Literature Review. *Systems* **2025**, *13*, 52. [\[CrossRef\]](#)
19. Savaş, S.; Karataş, S. Cyber Governance Studies in Ensuring Cybersecurity: An Overview of Cybersecurity Governance. *Int. Cybersecur. Law Rev.* **2022**, *3*, 7–34. [\[CrossRef\]](#)
20. Demircan, B.G.; Yetilmezsoy, K. A Hybrid Fuzzy AHP-TOPSIS Approach for Implementation of Smart Sustainable Waste Management Strategies. *Sustainability* **2023**, *15*, 6526. [\[CrossRef\]](#)
21. Joshi, M.; Deole, P. Assessing Barriers to IoT Implementation in Circular Systems Using Spherical Fuzzy AHP Approach. *J. Sci. Ind. Res.* **2025**, *84*, 1088–1094. [\[CrossRef\]](#)
22. Khoshand, A.; Rahimi, K.; Ehteshami, M.; Gharaei, S. Fuzzy AHP Approach for Prioritizing Electronic Waste Management Options: A Case Study of Tehran, Iran. *Environ. Sci. Pollut. Res.* **2019**, *26*, 9649–9660. [\[CrossRef\]](#) [\[PubMed\]](#)
23. Turskis, Z.; Šniokienė, V. IoT-Driven Transformation of Circular Economy Efficiency: An Overview. *Math. Comput. Appl.* **2024**, *29*, 49. [\[CrossRef\]](#)
24. Kristoffersen, E.; Blomsma, F.; Mikalef, P.; Li, J. The Smart Circular Economy: A Digital-Enabled Circular Strategies Framework for Manufacturing Companies. *J. Bus. Res.* **2020**, *120*, 241–261. [\[CrossRef\]](#)
25. Morshedi, M.; Hargaden, V.; Papakostas, N.; Ghadimi, P. The Adoption of Digital Technologies in Circular Supply Chains: From Theoretical Developments to Practical Applications. *Logistics* **2026**, *10*, 18. [\[CrossRef\]](#)
26. Handoyo, S.; Sueb, M. Integrating Digital Technologies Into the Circular Economy: A Systematic Literature Review of Trends, Challenges, and Opportunities. *Circ. Econ. Sustain.* **2026**, *6*, 111. [\[CrossRef\]](#)

27. Trevisan, A.H.; Zacharias, I.S.; Liu, Q.; Yang, M.; Mascarenhas, J. Circular Economy and Digital Technologies: A Review of the Current Research Streams. *Proc. Des. Soc.* **2021**, *1*, 621–630. [\[CrossRef\]](#)
28. GACERE. *Circular Economy and Digitalization—Working Paper*; GACERE: Nairobi, Kenya, 2025.
29. Iruku, V.M. Smart Supply Chains for a Circular Future: AI and IoT for Greener Commerce for Sustainable Development. In *Sustainable Development Through Machine Learning, AI and IoT (ICSD 2025); Communications in Computer and Information Science*; Whig, P., Silva, N., Ahmad, A.E., Aneja, N., Sharma, P., Eds.; Springer: Cham, Switzerland, 2026; Volume 2888, pp. 128–139.
30. ISO/IEC 27001:2022; Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. International Organization for Standardization: Geneva, Switzerland, 2022.
31. Hernandez Ramos, J.L.; Karopoulos, G.; Nai Fovino, I.; Spigolon, R.; Sportiello, L.; Steri, G.; Gorniak, S.; Magnabosco, P.; Atoui, R.; Crippa Martinez, C. *Cyber Resilience Act Requirements Standards Mapping*; Publication Office of the European Union: Luxembourg, 2024.
32. Chou, Y.-C.; Sun, C.-C.; Yen, H.-Y. Evaluating the Criteria for Human Resource for Science and Technology (HRST) Based on an Integrated Fuzzy AHP and Fuzzy DEMATEL Approach. *Appl. Soft Comput.* **2012**, *12*, 64–71. [\[CrossRef\]](#)
33. Buckley, J.J. Fuzzy Hierarchical Analysis. *Fuzzy Sets Syst.* **1985**, *17*, 233–247. [\[CrossRef\]](#)
34. Saaty, R.W. The Analytic Hierarchy Process—What It Is and How It Is Used. *Math. Model.* **1987**, *9*, 161–176. [\[CrossRef\]](#)
35. Saaty, T.L. *Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process*; RWS Publications: Pittsburgh, PA, USA, 1994; Volume 6.
36. Alinezhad, A.; Amini, A.; Alinezhad, A. Sensitivity Analysis of Simple Additive Weighting Method (SAW): The Results of Change in the Weight of One Attribute on the Final Ranking of Alternatives. *J. Ind. Eng.* **2009**, *4*, 13–18.
37. Banda, W. An Integrated Framework Comprising of AHP, Expert Questionnaire Survey and Sensitivity Analysis for Risk Assessment in Mining Projects. *Int. J. Manag. Sci. Eng. Manag.* **2019**, *14*, 180–192. [\[CrossRef\]](#)
38. Spearman, C. The Proof and Measurement of Association between Two Things. *Int. J. Epidemiol.* **2010**, *39*, 1137–1150. [\[CrossRef\]](#)
39. Selmi, M.; Kormi, T.; Ali, N.B.H. Comparing Multi-Criteria Decision Aid Methods through a Ranking Stability Index. In *Proceedings of the 2013 5th International Conference on Modeling, Simulation and Applied Optimization (ICMSAO)*; IEEE: Hammamet, Tunisia, 2013; pp. 1–5.
40. Kamil, Y.; Lund, S.; Islam, M.S. Information Security Objectives and the Output Legitimacy of ISO/IEC 27001: Stakeholders' Perspective on Expectations in Private Organizations in Sweden. *Inf. Syst. E-Bus. Manag.* **2023**, *21*, 699–722. [\[CrossRef\]](#)
41. Qudus, L. Cybersecurity Governance: Strengthening Policy Frameworks to Address Global Cybercrime and Data Privacy Challenges. *Int. J. Sci. Res. Arch.* **2025**, *14*, 1146–1163. [\[CrossRef\]](#)
42. Chiara, P.G. Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise? *Eur. J. Risk Regul.* **2025**, *16*, 469–484. [\[CrossRef\]](#)
43. Teichmann, F. The Cyber Resilience Act as a New Paradigm for Product Security: A Compliance Roadmap. *Int. Cybersecur. Law Rev.* **2026**, *7*, 1–17. [\[CrossRef\]](#)
44. Arzt, S.; Gkoktsis, G.; Kreutzer, M.; Scheel, K.; Schreiber, L.; Simo Fhom, H. *Cyber Resilience Act: Risk Management—Recommendations for the Implementation of Risk Management Under the CRA*; National Research Center for Applied: Darmstadt, Germany, 2025.
45. Chaudhary, S.; Gkioulos, V.; Katsikas, S. Developing Metrics to Assess the Effectiveness of Cybersecurity Awareness Program. *J. Cybersecur.* **2022**, *8*, tyac006. [\[CrossRef\]](#)
46. Glöckler, J.; Sedlmeir, J.; Frank, M.; Fridgen, G. A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity. *Bus. Inf. Syst. Eng.* **2024**, *66*, 421–440. [\[CrossRef\]](#)
47. Tariq, U.; Ahmed, I.; Bashir, A.K.; Shaukat, K. A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. *Sensors* **2023**, *23*, 4117. [\[CrossRef\]](#)
48. Sobbo, T.; Turnbull, B.; Moustafa, N. A Holistic Review of Cyber-Physical-Social Systems: New Directions and Opportunities. *Sensors* **2023**, *23*, 7391. [\[CrossRef\]](#)
49. Alluqmani, K.; Karrar, A.E.; Alhaidari, M.; Alharbi, R.; Alharbi, S. Assessing the Efficacy of Security Awareness Training in Mitigating Phishing Attacks: A Review. *Int. J. Adv. Trends Comput. Sci. Eng.* **2025**, *14*, 177–184. [\[CrossRef\]](#)
50. Mudau, P.; Mpekoa, N.; Gcaza, N. Identifying Gaps in the Evaluation of Security Education, Training and Awareness (SETA) Programs: A Systematic Literature Review. In *Advancing Innovative Cybersecurity Solutions and Approaches to Protect Digital Ecosystems (IFIP-UNIVEN-CSIR ICC 2025); IFIP Advances in Information and Communication Technology*; Mtsweni, J., Kanyane, M., Phahlamohlaka, J., Munyoka, W., Thomson, K.-L., Fletcher, L., van Vuuren, J.J., Eds.; Springer: Cham, Switzerland, 2026; Volume 777, pp. 141–153.
51. Fitzgerald, J.; Morisset, C. Can We Develop Holistic Approaches to Delivering Cyber-Physical Systems Security? *Res. Dir. Cyber-Phys. Syst.* **2024**, *2*, e2. [\[CrossRef\]](#)
52. Choudhury, A.; Kaushik, K.; Kumar, V.; Singh, B.K. *Cyber-Physical Systems Security*, 1st ed.; Springer: Singapore, 2025; Volume 154.
53. Shaffique, M.R. Cyber Resilience Act 2022: A Silver Bullet for Cybersecurity of IoT Devices or a Shot in the Dark? *Comput. Law Secur. Rev.* **2024**, *54*, 106009. [\[CrossRef\]](#)

54. Teichmann, F. Cybersecurity of Critical Infrastructure in Europe: The NIS2 Directive in Focus. *Int. Cybersecur. Law Rev.* **2025**, *6*, 207–220. [\[CrossRef\]](#)
55. Cao, M.; Ye, M.; Zino, L. Control of Networked Cyber–Physical–Human Systems. *Nat. Rev. Electr. Eng.* **2025**, *3*, 32–45. [\[CrossRef\]](#)
56. Liu, C.; Tan, R.; Wu, Y.; Feng, Y.; Jin, Z.; Zhang, F.; Liu, Y.; Liu, Q. Dissecting Zero Trust: Research Landscape and Its Implementation in IoT. *Cybersecurity* **2024**, *7*, 20. [\[CrossRef\]](#)
57. Pöhn, D.; Hommel, W. New Directions and Challenges within Identity and Access Management. *IEEE Commun. Stand. Mag.* **2023**, *7*, 84–90. [\[CrossRef\]](#)
58. Larrucea, X.; Santamaria, I. Towards the Analysis of Software Supply Chain and EU Regulations. In *Systems, Software and Services Process Improvement (EuroSPI 2025); Communications in Computer and Information Science*; Yilmaz, M., Clarke, P., Riel, A., Messnarz, R., Zelmenis, M., Buce, I.A., Eds.; Springer: Cham, Switzerland, 2026; Volume 2658, pp. 170–183.
59. Mahmood, S.; Chadhar, M.; Firmin, S. Addressing Cybersecurity Challenges in Times of Crisis: Extending the Sociotechnical Systems Perspective. *Appl. Sci.* **2024**, *14*, 11610. [\[CrossRef\]](#)
60. Prabaswari, R.; Ali, Y.; Gultom, R.A.G.; Simbolon, L.; Gunawan, A.A.N. A Novel Socio-Technical Framework for Enhancing Cyber Crisis Management Capabilities. *Int. J. Saf. Secur. Eng.* **2024**, *14*, 1181–1193. [\[CrossRef\]](#)
61. Huang, Y.; Lu, X. Editorial: Security, Governance, and Challenges of the New Generation of Cyber-Physical-Social Systems. *Front. Phys.* **2024**, *12*, 1464919. [\[CrossRef\]](#)
62. Al Qurashi, M. Decentralized Identity Management for Industrial Internet of Things Utilizing Blockchain-Enhanced Multi-Factor Authentication. *Int. J. Comput. Netw. Appl.* **2024**, *11*, 519–526. [\[CrossRef\]](#)
63. Jazairy, A.; Brho, M.; Manuj, I.; Goldsby, T.J. Cyber Risk Management Strategies and Integration: Toward Supply Chain Cyber Resilience and Robustness. *Int. J. Phys. Distrib. Logist. Manag.* **2024**, *54*, 1–29. [\[CrossRef\]](#)
64. Bahmanova, A.; Lace, N. Modelling Cyber Resilience in SMEs as a Socio-Technical System: A Systemic Approach to Adaptive Digital Risk Management. *Systems* **2026**, *14*, 151. [\[CrossRef\]](#)
65. Van Zomeren, M.; Deane, F.; Joiner, K.F.; Qiao, L.; Horne, R.; Suprun, E. Regulating Cyberworthiness: Governance Frameworks for Safety-Critical Cyber-Physical Systems. *Systems* **2025**, *13*, 862. [\[CrossRef\]](#)
66. Huang, J.; Li, L.; Jiang, P.; Zhang, S. DEMATEL-Based ANP Model for Identifying Critical Indicators in Sustainable Emergency Material Reserve Systems. *Sustainability* **2024**, *16*, 5263. [\[CrossRef\]](#)
67. Shi, Y.; Yu, S.; Mei, J. Strategic Decision-Making Enhancement through Graph-Optimized DEMATEL-AHP with Pruning. *Group Decis. Negot.* **2025**, *34*, 105–133. [\[CrossRef\]](#)
68. Androutsopoulou, M.; Carayannis, E.G.; Askounis, D.; Zotas, N. Towards AI-Enabled Cyber-Physical Infrastructures—Challenges, Opportunities, and Implications for a Data-Driven EGovernment Theory, Policy, and Practice. *J. Knowl. Econ.* **2025**, 1–38. [\[CrossRef\]](#)
69. Mukherjee, K. A Note on Limitations of FAHP. In *Supplier Selection; Studies in Systems, Decision and Control*; Springer: New Delhi, India, 2017; Volume 88, pp. 101–111.
70. Bhol, S.G. Applications of Multi Criteria Decision Making Methods in Cyber Security. In *Cyber-Physical Systems Security; Studies in Big Data*; Choudhury, A., Kaushik, K., Kumar, V., Singh, B.K., Eds.; Springer: Singapore, 2025; Volume 154, pp. 233–258.
71. Madanchian, M.; Taherdoost, H. Applications of Multi-Criteria Decision Making in Information Systems for Strategic and Operational Decisions. *Computers* **2025**, *14*, 208. [\[CrossRef\]](#)
72. Scholtysik, M.; Rasor, A.; Petzke, L.; Koldewey, C.; Dumitrescu, R. An Integrative Perspective on Digital Technologies and Circular Economy: A Systematic Literature Review. *Proc. Des. Soc.* **2025**, *5*, 541–550. [\[CrossRef\]](#)
73. Teixeira, N. Circular Economy Perspectives: Challenges, Innovations, and Sustainable Futures. *Discov. Sustain.* **2025**, *6*, 738. [\[CrossRef\]](#)
74. Seyi-Lande, O.B.; Layode, O.; Naiho, H.N.N.; Adeleke, G.S.; Udeh, E.O.; Labake, T.T.; Johnson, E. Circular Economy and Cybersecurity: Safeguarding Information and Resources in Sustainable Business Models. *Financ. Account. Res. J.* **2024**, *6*, 953–977. [\[CrossRef\]](#)
75. Nemilentseva, M.; Tariq, A.; Tariq, W.; Aghajani, D.; Torkkeli, M. A Review of Digital Platform and Circular Economy. In *Human Perspectives of Industry 4.0 Organizations: Reviewing Sustainable Performance*; CRC Press: New York, NY, USA, 2024; pp. 38–67.

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