technologies

MDPI

Article

An Approach to Business Continuity Self-Assessment

Nelson Russo [1,*], Henrique São Mamede [1,2] and Leonilde Reis [3]

[1] Department of Science and Technology, Universidade Aberta, Rua da Escola Politécnica, no. 147, 1269-001 Lisbon, Portugal
[2] Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência (INESC TEC), Rua Dr. Roberto Frias, 4200-465 Porto, Portugal; hsmamede@gmail.com
[3] School of Business Administration, Polytechnic Institute of Setúbal, Campus do IPS, Estefanilha, 2914-503 Setúbal, Portugal; leonilde.reis@esce.ips.pt
* Correspondence: nelsonrusso@gmail.com

Abstract: Business Continuity Management (BCM) is critical for organizations to mitigate disruptions and maintain operations, yet many struggle with fragmented and non-standardized self-assessment tools. Existing frameworks often lack holistic integration, focusing narrowly on isolated components like cyber resilience or risk management, which limits their ability to evaluate BCM maturity comprehensively. This research addresses this gap by proposing a structured Self-Assessment System designed to unify BCM components into an adaptable, standards-aligned methodology. Grounded in Design Science Research, the system integrates a BCM Model comprising eight components and 118 activities, each evaluated through weighted questions to quantify organizational preparedness. The methodology enables organizations to conduct rapid as-is assessments using a 0–100 scoring mechanism with visual indicators (red/yellow/green), benchmark progress over time and against peers, and align with international standards (e.g., ISO 22301, ITIL) while accommodating unique organizational constraints. Demonstrated via focus groups and semi-structured interviews with 10 organizations, the system proved effective in enhancing top management commitment, prioritizing resource allocation, and streamlining BCM implementation—particularly for SMEs with limited resources. Key contributions include a reusable self-assessment tool adaptable to any BCM framework, empirical validation of its utility in identifying weaknesses and guiding continuous improvement, and a pathway from initial assessment to advanced measurement via the Plan-Do-Check-Act cycle. By bridging the gap between theoretical standards and practical application, this research offers a scalable solution for organizations to systematically evaluate and improve BCM resilience.

Keywords: business continuity; disaster recovery; self-assessment; measurement; information and communication technology

Academic Editor: Sotirios K. Goudos

Received: 6 May 2025
Revised: 2 June 2025
Accepted: 9 June 2025
Published: 11 June 2025

Citation: Russo, N.; São Mamede, H.; Reis, L. An Approach to Business Continuity Self-Assessment. *Technologies* **2025**, *13*, 242. https://doi.org/10.3390/technologies13060242

1. Introduction

The effective use of Information and Communication Technologies (ICT) is nowadays essential for organizations, although with various levels of dependence. However, it has become vital to an organization's competitiveness and agility, particularly in critical business processes. As a result, businesses should brace themselves for potential disruptions in productivity and competitiveness, especially concerning ICT-enabled business processes.

According to the Business Continuity Institute [1] and Katsaliaki et al. [2], organizations increasingly face challenges in ensuring business continuity due to the growing complexity of ICT infrastructures and the unpredictability of disruptive events. These

disruptions can severely impact business operations, leading to financial losses, reputational damage, and operational inefficiencies. However, despite the critical importance of BCM, organizations often face challenges in conducting comprehensive and standardized assessments of their BCM capabilities, which hampers their ability to effectively identify gaps and improve resilience. Therefore, it is crucial to establish robust Business Continuity Management (BCM) models that provide resilience and agility in response to unforeseen events.

Business Continuity (BC) is based on the concept that an organization must have the strategic and tactical ability to plan for and respond to incidents and business interruptions [3] to continue operations at a predetermined acceptable level. This ability is critical and must be included in the BCM model for it to be suitable for integration with our Self-Assessment Methodology.

Strategic ability is formalized in BCM, which seeks to guarantee the organization's preparedness for maintaining the continuity of its services, business processes, or purpose during a disaster, through implementation of a contingency plan [4]. As a result, BCM includes effective planning for resuming short-term business processes. The Business Continuity Plan (BCP) is thus implemented to eliminate or reduce the impact of operational interruptions caused by disruptive events [5]. The BCM model associated with our Self-Assessment Methodology must uphold this principle.

The BCP, on the other hand, is a by-product of BCM. Thus, to develop it, a set of essential BCM components must be addressed to generate a compelling and valid artifact that an organization can utilize. In this perspective, the BCM Model must provide the components and activities that enable the systematization of BCM and are integrated to follow the iterative management approach Plan-Do-Check-Act (PDCA). Still, existing frameworks tend to focus on isolated BCM components rather than offering a holistic perspective, which is a challenge noted by several authors [6–11].

Current BCM assessment frameworks are fragmented and lack integration, frequently addressing single components or narrowly focused risks such as cyber resilience, without providing a unified, adaptable methodology that encompasses the full spectrum of BCM activities.

With these considerations and an understanding of each of the BC components and their activities in mind, an assessment system can be defined to evaluate each of the intentions specified in BCM activities. The set of all activity components of the assessment system should strategically lead the organization on what should be considered to achieve the activity objective. However, each organization has unique characteristics, constraints, legal or regulatory frameworks, and partnerships with other organizations that may limit the execution or scope of the goal described in a metric.

Existing frameworks address BC self-assessment, particularly in cyber resilience and third-party risk management [12]. The Cyber Resilience Self-Assessment Tool (CR-SAT) helps SMEs assess and improve cyber resilience, while another study highlights deficiencies in self-assessment tools for risk management and suggests the need for a more robust process [13].

Given this gap, our research seeks to address the problem of fragmented and non-standardized BCM assessments by proposing a comprehensive Self-Assessment methodology. This methodology aims to integrate multiple BCM components, providing organizations with a structured and adaptable evaluation tool that can assess their BC maturity and resilience effectively.

In summary, achieving a multidisciplinary BC assessment is relevant to defining an assessment system supported by a BCM model that includes and relates the BC components and activities and their metrics or assessment questions. Thus, organizations can gain the

benefits of having a documented method to conduct an assessment and track the program's continuous improvement and progress [14].

There are international frameworks and standards, referred to as Standards, that support the design of a BCP. Organizations typically seek support from current and widely recognized Standards for designing their BCP to improve processes, ensure compliance, obtain certification, and enhance their brand image. Selecting the most appropriate standard for the organization should be an agile activity that helps define a BC approach. While the Standards guidance focuses on the methods to be used, when, and by whom, its guidelines indicate that organizations must determine what should be measured and assessed. Some organizations cope with constraints when defining what to assess when designing a BCP. These constraints can be addressed by monitoring and assessing the BC activities of a BCM Model and its performance [15] and defining questions to assess both the design and implementation of the BCP [16].

Previously, measuring concerns was handled by proposing BCM frameworks based on questionnaires or diagrams [6], but there has been limited progress in this area since 2018. One solution focuses on assessing the effectiveness and maturity of the organization's BC practices and initiatives in BCP design and execution. It is based on metrics and specific questions that will aid in the design or redesign of BCPs and identify gaps and crucial areas to address in the BC area.

The Self-Assessment methodology presented here was designed to be an economical way to identify gaps, improve the BCM program, and raise awareness. The design process considered how a Self-Assessment System could help to prepare the Business Continuity Management System (BCMS). In an environment of limited resources, we also considered how it could enhance BC preparedness and provide an opportunity to obtain a BCM score, which can be traced in time to capture improvement and identify deficiencies. On its first use, it is intended the capture the as-is state of the organization's BCMS and, in time, to capture the state evolution.

Therefore, this research aims to provide a structured Self-Assessment methodology enabling organizations to systematically evaluate their BC readiness, improve their BCM processes, and enhance their resilience against disruptive events.

Some questions emerged, triggering an analysis and comparison of the Standards establishing the need for an integrated identification of a set of metrics that allow the measurement and qualitative assessment of the essential components of the BCM, as well as the degrees of BC maturity in organizations [17].

The research addressed these issues and adopted a BCM Model, which allows multi-disciplinary BC preparedness and implementation. It attempts to assist organizations and streamline their BCP design and implementation processes.

This paper focuses on the Self-Assessment methodology, enabling compliance evaluation with the BCM Model adopted. This Self-Assessment methodology not only facilitates identification of BCM weaknesses and strengths but also supports continuous improvement by enabling organizations to track progress over time through repeatable, standardized evaluations aligned with internationally recognized BCM standards.

This article is structured as follows: Section 1 introduces the research topic, outlining the significance of BC and the necessity for a structured approach to its assessment. Section 2 provides background research, covering fundamental BC concepts, the BCP, and BCM, along with a review of relevant standards and best practice models. Additionally, it discusses measurement challenges within the BCM scope. Section 3 details the methodology applied in the research. Section 4 identifies the problem and its motivation, setting the stage for the proposed solution presented in Section 5. This section defines the objectives and requirements, explains the transition from self-assessment to measurement, and

introduces the Self-Assessment System and its components. Section 6 demonstrates the proposed approach, Section 7 presents its evaluation, and Section 8 concludes the paper by summarizing the findings and their implications. Finally, the References section lists all cited sources.

2. Background Research

This section presents the theoretical background for the relevant research topics.

2.1. Business Continuity

BC is described as examining an organization's critical functions, identifying potential disaster scenarios, and developing procedures to handle these concerns [18]. Businesses are increasingly being required to prepare for risks that threaten the existence of crucial business activities. This results from the increasing frequency of natural disasters, threats from terrorist attacks and other criminal attacks, and changing legislation and regulations [19]. The economy and increased competition impact the organization's need to improve and devote additional attention to developments that may disrupt critical business operations. Even minor disruptions can seriously affect the organization and its reputation [20].

Despite growing awareness of these risks, many organizations struggle to operationalize BC in a consistent, measurable, and strategic manner. The challenge lies not only in developing continuity procedures but also in ensuring they are effectively implemented, maintained, and aligned with business objectives.

This difficulty is compounded by the growing complexity of threats, limited internal expertise, and the lack of practical tools that support decision-making in business continuity planning.

The ability of an organization to continue its essential activities after or during a disaster, as well as the speed with which it may restore full performance, might be the difference between success and failure [21]. Hence, BC includes an organization's ability to plan for and respond to disruptions and emergencies, such as keeping things running and recovering to normal [22].

Consequently, BC is a significant challenge for all organizations, regardless of the activity sector in which they operate, concerning competitiveness objectives, profitability, and market position.

While the existing literature and international standards emphasize the importance of BC, they often fall short of offering actionable frameworks that support organizations—particularly SMEs—in evaluating their continuity readiness.

Furthermore, there is a noticeable absence of self-assessment mechanisms that connect BC activities with performance indicators, maturity levels, or business value, limiting strategic engagement from top management.

However, BC relies on the premise that disruptions will occur at some time. As defined by Arduini & Morabit [23], BC is a framework of disciplines, processes, and techniques to provide continuous operation for critical business functions under all conditions. BC specifies how an organization will function following a disruption until its usual facilities are restored [24]. The central focus is BC's stress on establishing other solutions for continuing operations during a disaster.

A successful contingency plan must include disaster recovery and BC components. Disaster recovery generally concerns technical recovery processes, whereas BC concerns logistical processes that temporarily bypass damaged technical elements [24]. Consequently, for BC to be solid, it must be planned.

To address this gap, this study introduces a novel Self-Assessment System grounded in BC maturity models and aligned with international standards. This system provides

quantifiable metrics across preparedness, response, and recovery phases and supports organizations in benchmarking their continuity capabilities.

By translating complex standards into structured evaluation criteria, the proposed system empowers organizations to identify weaknesses, prioritize improvements, and communicate the value of BC efforts to decision-makers.

2.2. Business Continuity Plan

BC refers to the specific business plans and actions that allow an organization to respond to a crisis so that functions, sub-functions, and processes are recovered and resumed following a predetermined plan, prioritized by their criticality towards the economic viability of the business [25]. BC also establishes the strategies, procedures, and critical actions required to respond to and manage crises [26]. The authors of [27] state that the overall purpose of BC is to identify, plan, implement, and sustain multiple modes of operation in the event of a crisis.

BC provides a method for organizations to anticipate and overcome disruptions, lowering the risk of loss and allowing business operations to continue [28]. Planning, however, involves understanding potential outcomes and the risks an organization faces. To safeguard the business and the interests of its stakeholders, the authors of [29] emphasize that BC entails anticipating failures, taking planned measures, and testing.

The usefulness of a BCP is debatable [30]. Some authors emphasize organizational BCP awareness or training [31] and preparatory steps for BCP design and implementation [32]. Other works address security issues, focusing on cybersecurity [33] and risk-mitigation procedures [34]. Additionally, security policies are defined to encourage a safety culture and advocate improving ICT professionals' preparation with training and practice [35]. Instead of being tailored to a specific type of disaster, the BCP should be designed to respond to the impact on the organization [36].

However, the definition of BCPs changes depending on the research objectives mentioned above. ISO 22301:2019 provides a comprehensive definition stating that the BCP is the documented information that guides an organization to respond to disruption and resume, recover, and restore the delivery of products and services consistent with BC objectives [37].

BCPs are documented procedures, from the perspective of preparing ICT for BC, that guide organizations to respond, recover, resume, and restore to a predefined level of operation following an interruption, according to ISO/IEC 27031:2011 [38]. Objectives to plan, establish, implement, operate, monitor, review, maintain, and continually improve a documented management system to protect against and mitigate the effects of disruptions and prepare for and respond to them are examples of how BC planning may be structured [39].

In terms of understanding the organization, one crucial aspect of developing a business contingency plan is accurately identifying the company's assets and determining which are critical to the business and must be prioritized. The BCP encompasses various aspects, including risk assessment, Business Impact Analysis (BIA), recovery strategies, plan development, documentation, testing, implementing, and maintaining the plan [40]. Before conducting the BIA, it is crucial to gather essential information [41]. This information is instrumental in determining critical processes and establishing the appropriate BCP recovery sequence.

However, despite the growing body of literature on BCP components, risk mitigation strategies, and international standards, organizations continue to face difficulties in translating these guidelines into actionable and measurable practices.

The practical implementation of BCP remains fragmented and inconsistent, especially among small and medium-sized enterprises (SMEs), which often lack the re-

sources and expertise to interpret complex standards or evaluate the effectiveness of their preparedness measures.

The BCP must undergo an annual review and receive approval from the organization's top management. Furthermore, it should be readily available to all key employees responsible for supporting the business during recovery [42].

This gap highlights the need for a structured, metrics-based approach to assess BCP maturity and guide organizations in implementing effective continuity strategies.

Existing frameworks, while comprehensive in theory, often fall short in offering concrete self-assessment tools that align continuity efforts with measurable business outcomes.

In response, this study proposes a novel Self-Assessment System that operationalizes BCM components through quantifiable metrics. The system enables organizations to evaluate their readiness across all phases—preparedness, response, and recovery—while ensuring alignment with standards like ISO 22301 and ISO/IEC 27031.

2.3. Business Continuity Management

The BCP must be integrated into a comprehensive management process known as BCM to attain its goals effectively. BCM involves the systematic implementation and continuous maintenance of BC [39]. Thus, BCM is a holistic management process that identifies potential threats to an organization and the impacts on business operations which they might cause [38]. To ensure these threats are managed proactively and systematically, international standards emphasize the importance of embedding continuity practices within the organization's broader management systems.

According to ISO 22300:2021 [39], a BCMS is an integral component of the overall management system, responsible for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving BC. Additionally, a BC Program is an ongoing management and governance process supported by top management and adequately resourced to implement and maintain the BCM. Consequently, implementing an adequate and effective BCMS is challenging, demanding, time-consuming, and holistic [43]. It is necessary to streamline the organizational process of establishing a BCP and support organizations in achieving this goal. This underscores the relevance of exploring existing frameworks and models that can facilitate more structured and efficient BCM implementation.

In this context, exploring the components and requirements of a BCM Model is pertinent in the quest to identify means of mitigating the identified gaps and addressing the identified constraints [17]. The BCM components and activities employed in the Self-Assessment System draw upon the framework for the Multidisciplinary Assessment of Organizational Maturity in Business Continuity Management [44], which pays particular attention to the scientific literature and Standards since 2016 [45]. The framework's BCM Model incorporates a set of strategic guidelines written and presented in a way that aims to simplify the organizational processes for the BCP design. Organizations can then focus efforts on improving their BCM program and better prepare for business continuity events.

While the theoretical foundations and standardization efforts are well-established, practical implementation continues to face persistent barriers. Despite these advancements, significant challenges remain that hinder widespread adoption and effective execution of BCM practices, particularly in resource-constrained environments.

2.4. Standards and Models of Best Practices

This research examined strategic guidelines from the Capability Maturity Model Integration (CMMI), which offers a set of best practices enabling companies to improve the performance of their primary business processes [46]. Additionally, it explored the Information Technology Infrastructure Library (ITIL) as a framework designed to align

ICT services with business needs [47]. The research also considered the Control Objectives for Information and Related Technology (COBIT), serving as a valuable reference guide for implementing ICT Governance, encompassing the technical part, processes, and people [48].

Furthermore, several relevant Standards for BC were reviewed. ISO 22301:2019 outlines the structure and requirements for implementing and maintaining a BCMS. The NFPA 1600 provides essential criteria for preparedness and resilience [14]. Lastly, NIST 800-34 Rev.1 offers instructions, recommendations, and considerations for information systems contingency planning [49].

Despite the comprehensiveness of existing standards and frameworks, their effective application in organizations—especially SMEs—remains a challenge. Many struggle to operationalize these guidelines in a way that supports decision-making, performance tracking, and alignment with business goals.

In practice, organizations often lack the tools to translate high-level frameworks into actionable procedures and quantifiable metrics that support self-evaluation, continuous improvement, and strategic oversight.

The Standard ISO 22301:2019 states that the organization shall evaluate the performance and effectiveness of the BCMS. Concerning performance evaluation, ISO 22301 [37] states that the organization shall determine what needs to be monitored and measured and the methods to ensure valid results. It must also be determined when and by whom the monitoring and measuring shall be performed and the results analyzed and evaluated. Thus, the standard suggests that the organization retain appropriate documentary information as evidence of the results.

Considering the measurement perspective in ITIL, within the general practice of Continual Improvement management, many techniques can be employed when assessing the current state—such as a balanced scorecard review, internal and external assessments, and audits [47].

To assess where the organization is, services and methods already in place should be measured and/or observed directly to properly understand their current state and what can be reused from them [47]. Decisions on how to proceed should be based on information that is as accurate as possible. Therefore, the road to optimization of practices and services must follow high-level steps, which include executing the improvements iteratively. This comprises the use of metrics and other feedback to check progress, stay on track, and adjust the approach to optimization as needed [47].

In the COBIT 2019 domain Monitor, Evaluate, and Assess, the management objective Managed Performance and Conformance Monitoring defines five practices and their activities [48]. The Management Practice MEA01.04—Analyse and Report Performance suggests that the organization uses a method that provides a succinct view of ICT performance and fits within the enterprise monitoring system [48]. To facilitate effective, timely decision-making, scorecards or traffic light reports are suggested. Regarding the performance measurement policy, COBIT states that a balanced scorecard translates strategy into action to achieve enterprise goals, streamline internal functions, create operational efficiencies, and develop staff skills. This holistic view of operations helps link long-term strategic objectives and short-term actions.

While standards like ISO 22301, COBIT, ITIL, and CMMI encourage performance measurement and continual improvement, they do not explicitly define unified self-assessment models for BC maturity evaluation.

Moreover, there is little integration across these models to support BC-specific maturity assessments that simultaneously address ICT alignment, operational continuity, and

governance reporting. This leaves a gap in how organizations can consistently monitor BC preparedness using a single, holistic approach.

NFPA 1600 argues that an internal assessment of the development, implementation, and progress made in a business continuity/continuity of operations program is a vital part of an entity's growth and success. There are benefits in developing a documented method to conduct an assessment that tracks the program's continuous improvement and progress [14]. There must be a commitment to monitoring for tracking progress through a defined period. Therefore, NFPA 1600 advises maintaining a documented program with scope, goals, performance, objectives, and metrics for program evaluation [14]. Regardless of the selected approach, a continuous focus on a quantifiable process and its use at all levels of the organization will provide the maximum benefits.

Monitoring the present state can help the organization to set short-term through long-term goals, track progress, and eliminate waste in cost and effort [14]. It can also help justify expenses and substantiate the need for capital, personnel, and other process components that can help improve the implementation of business continuity. Thus, a specific method of applying a self-assessment (and maturity model) must define the key concepts and their elements. It also must define a scoring process method to record its compliance with the model. Finally, it must implement a method to distribute the model, train the participants, gather results, and prepare a summary for all interested parties. Best practices, lessons learned, and other criteria discovered during the assessment can be shared throughout, resulting in process improvement for the organization.

To bridge this gap, this study proposes a structured self-assessment model grounded in BC standards and ICT governance frameworks.

The model integrates concepts from ISO 22301, CMMI, COBIT, and ITIL to form a coherent evaluation system that enables organizations to assess their BC maturity, track performance, and guide continuous improvement.

It introduces a scoring methodology and evaluation procedures that transform abstract standards into concrete metrics, thereby supporting operational decision-making, transparency, and strategic alignment.

Performance must be managed at all levels of the business and be a key factor for process change. CMMI recognizes the importance of understanding an organization's current level of performance and the extent to which it aligns with actual business needs and goals [46]. If performance does not correspond to business needs and goals, process improvement is used to raise performance to the necessary level. In this sense, CMMI was built with a focus on performance and continuous improvement, making it easier for organizations to measure performance frequently to assess the impact on the business over time.

From the perspective that measurement is necessary to achieve business results, CMMI emphasizes that "what gets measured gets done" and that measurement requires investment. Therefore, it must be ensured that there is a reason for every measurement that is collected and that provides business value and performance improvement. It must be ensured that people understand why measurements are collected and how they are helpful for the project and the organization. However, measurement directs people's behavior and can affect the quality of the measurement system, so more analysis should be prioritized over more measures.

As the measurement is relevant, top management must identify its needs and use the information collected to provide governance and an overview of improving and effectively implementing processes. As an example of an activity, top management supervises the appropriate integration of measurement and analysis activities into the organization's processes [46]. The use of measurement supports the following:

- Objective planning and estimation;
- Effective monitoring of progress and performance against plans and objectives;
- Identification and resolution of process-related issues;
- Providing a basis for incorporating measurement into additional processes in the future.

2.5. Discussion on Measurement in the BCM Scope

In terms of measurement, we highlight multiple works within the BCM scope that impacted the research artifacts proposed. Starting in 2018, a few publications mentioned metrics, Key Performance Indicators (KPIs), or measurement concepts. Thus, some authors consider measurement for specific issues, covering only some of BCM [50–52].

Despite the acknowledged importance of measurement within BCM, there remains no consensus on a standardized, comprehensive approach to assess the maturity or performance of BCPs across organizations.

In other publications [53–57], measurement is focused on Recovery Time Objective, Recovery Point Objective, and Risk Assessment, not on specific metrics or assessment of the BCMS. For example, some focus on metrics for evaluating Disaster Recovery Plan performance [56].

There are other papers focused on understanding the organization's preparedness which propose metrics or KPIs for ICT systems, although they need to consider the latest versions of the Standards [58–60]. Some authors focus on loss prevention, the BCM program, or project justification [61], proposing a risk index based on metrics. For example, they propose metrics for BCM or BCP justification [62], readiness, or financial loss, focusing on maintaining management support and engagement. Therefore, most of the cited studies that address metrics or KPIs for BCM or BCP are focused on financial or loss justification to maintain top management support and engagement.

Harding [55] states that measurement is to answer whether the organization can recover. Measurement provides top management with information on how the organization will recover from an incident. The BCP is improved by identifying deficiencies and awareness-raising for decision-making so that the organization can choose between accepting the risk or reducing it by applying relevant controls.

The BCP assessment is crucial for developing a supplier management program [50]. If a third-party service provider is affected by an incident or disaster, it is relevant to understand how this will affect the continuity of the organization's business operations. Thus, Marshall [50] defines test questions for how the organization considers risk. Regarding risk drivers, Marshall [50] considers the following relevant to the supplier score: recovery time frame, unmitigated risks, adequate BCP documentation, supplier BCP testing, BCP program suitability, supplier BCP management, and a signed commitment letter to the BCP. Each risk level is assigned (low, medium, medium-high, and high) according to an interpretation given to the realization or implementation of risk drivers.

Tomsic [52] considers that effective mechanisms can be explored as long as they reflect and support organizational management standards, including a relatively informal measurement process focused on the organization's perception of the program's key performance indicators. Regarding formal audit approaches such as questionnaires, effective measurement depends on establishing expectations and standards for the purpose, scope, roles and responsibilities, training requirements, and activity for identified individuals or positions. An emergency management standard that establishes these measurable components allows transparent and sustainable improvements in organizational preparedness directly related to its stated objectives. Regular measurement and prioritization of resource allocation promote a cycle of continuous improvement of the Emergency Management Program [52].

However, existing studies and frameworks tend to focus on isolated metrics (e.g., RTO, RPO, risk index), specific organizational contexts (such as ICT systems), or management perceptions, rather than offering a reusable, structured system for self-assessing the overall state and maturity of the BCM program.

Regarding the measurement of a BC program, Stourac [63] suggests that a scorecard can offer benefits beyond periodic measurement by acting as a program hub. Building an effective and efficient program involves adopting a strategic vision of the accomplishments, maintaining consistent communication, providing regular reports to top management, and adhering to a well-defined yet flexible process.

In their proposal, Olson & Anderson [62] introduce a resilience scoring methodology designed to evaluate the BCP by analyzing its alignment with a predefined set of criteria, which can be tailored to suit the organization's specific requirements. This scoring approach effectively encourages active involvement, enhances reporting capabilities, identifies risks, and assesses the overall organizational resilience. A resilience score assesses how resilient a team would be in performing its critical function if confronted with an interruption event that would require the implementation/activation of the BC plan.

After implementing the resilience score, Olson & Anderson [62] stated that the planner's involvement significantly improved, as evidenced by the improvement in the plan's content and greater participation in program requirements and activities. The authors argue that the score encouraged and provided additional responsibilities in that the continuity team improved communication with top management about plan content. The score also provided the ability to identify trends and make informed decisions. The highlighting of risk areas and opportunities leveraged the prioritization of resources and appropriate focus on improvement efforts. The resilience score provided the ability to assess the plan's quality quickly.

One objective of the BIA process is to establish recovery objectives. The next step is to determine whether ICTs can match those objectives. A customizable model is presented by Ricks & Boswell [56], suitable for application in any organization, enabling adoption of an ICT-centric approach and assessing resilience capabilities effectively. The model's output is a composite score (based on an aggregated capability score and a weighting factor) for each application that identifies these ICT services in the portfolio and their most significant gaps in capabilities. The score categories can be interpreted and communicated as follows: Inadequate (red), with a score between 0 and 18; Needs improvement (yellow), with a score between 19 and 25; and Good (green), with a score of 26 or higher. In the last stage of the assessment model, a prioritized list of corrective measures is developed for each application, considering the capability assessment [56]. Moreover, although some authors suggest score-based evaluations or checklists, few offer guidance on integrating such approaches into a scalable, user-friendly self-assessment methodology that aligns with current Standards and supports benchmarking across different organizational sizes and sectors.

We identify a set of publications addressing measurement in BC-related programs [64], although published frameworks or methods that address the question of self-assessment are limited in number. From this set of publications, we identified two methods for self-assessment: a quick self-assessment preparedness questionnaire with a score, and a questionnaire with a score for the BC-related program evolution or the initiatives for compliance.

To address these limitations, we propose a Self-Assessment System that consolidates fragmented approaches into a cohesive, standards-aligned framework. This system enables organizations to rapidly assess their preparedness using a scoring model supported by well-defined guidelines, key success factors, and metrics.

In 2003, Gallagher [58] introduced a rapid method to assess an organization's preparedness to ensure its continuity after a severe incident. This approach involved a questionnaire to assess whether the organization had reasonable measures to reduce risks and an effective BC program. The set of 20 questions establishes where the organization stands regarding BCM. Each question has a score between 0 and 5, where 0 indicates that the topic was not addressed and 5 indicates that it reached a good point regarding the main issues addressed. The total score is qualitatively evaluated; where below 50, there is considerable work to reach a satisfactory state. Between 50 and 65, there still needs to be compliance with reasonable governance requirements. Between 65 and 80, BCM requirements are unlikely to be met. Above 80, it indicates that there is likely an effective and efficient BCM program [58].

Despite its usefulness, the self-assessment method has limitations and does not replace an independent audit of a BC program [51]. However, identifying gaps, improving the program, and raising awareness can be cost-effective. Self-assessment helps prepare the program and team members for an independent audit. Self-assessment might provide an opportunity, in a resource-constrained context, to obtain quantitative outputs about the current state that can be tracked over time to capture improvement or highlight shortcomings. Self-assessment holds significant value within any BC program. The program's maturity level, Organizational Culture, and Management expectations will determine its specific role, as outlined in [51].

Even if proposing measurement for specific issues [51], when defining the objectives for self-assessment, one should consider the organization's mission, vision, values and culture, the goal or purpose of self-assessment, the audience, and the scope. The output must determine the questions, how to ask them, and in what form the answers are required. Questions must be limited to the most relevant topics and capture the answers in a format that is easy to manage and make into a repeatable process. A clear and transparent process must be in place for validation and sign-off to identify who completed the assessment and who is responsible for review and sign-off, including the due date.

The NFPA 1600 [14] proposes a specific method of applying a self-assessment which can include defining the elements of each concept and providing the guidelines and minimum requirements for each element. It also suggests defining a method for the entity to conduct a scoring process to record its compliance with the model [14]. Finally, it suggests implementing a method to distribute the model, train the participants, gather results, and prepare a summary for all interested parties.

The Self-Assessment System should provide an overall BC state in organizations of all sizes. Nonetheless, it is suitable for small businesses who wish to assess their BC preparedness and readiness, even if they do not intend to use the Self-Assessment System.

We believe that the Self-Assessment System can boost the initiation of the BC program and simplify its use if questions are easily interpreted and a summary of the purpose to achieve is given using a score and semaphore color. Presenting a small but adequate amount of questions in each component can reduce the perception of complexity and allow adoption in organizations of lower capacity. It is justified by the incrementally decreasing value of each question as they have less coverage.

Quantifying BC information is challenging, yet it enhances accessibility compared to lengthy textual reports. The authors agree that organizations need a scoring system that allows benchmarking between organizations to obtain recognition for compliance and trigger the adoption of frameworks, Standards, or solutions to implement BC in the organization. Therefore, when answering the questions, the topic areas can be inferred, guidelines can emerge, and a more precise vision of what the organization should do can be discerned.

Therefore, to narrow the identified gap in BC self-assessment, we gather a set of contributions from academia and the latest Standards and incorporate all this knowledge in the proposed Self-Assessment System. Success factors, guidelines, or best practices may be used to benchmark and streamline BCP design, adequately supported by a set of metrics with defined goals. The guidelines are carefully selected in the Self-Assessment System, capturing the essence of the underlying activities metrics. By addressing the challenges and incorporating them into the proposed artifact, organizational processes were effectively supported, streamlining the establishment of the BCP.

Our approach bridges the gap between academic proposals and practical applicability, offering a method that is not only grounded in the literature and standards but also tailored for organizations with varying levels of resources and BCM maturity.

3. Methodology

This study follows the problem-centered initiation approach [65] of the Design Science Research (DSR) methodology. DSR is one of the research methods used in the Information Systems (IS) field to solve organizational issues and contribute to the resolution of complex problems [66,67]. DSR is particularly suited for this study because it emphasizes the creation and evaluation of innovative artifacts that address practical organizational problems, aligning perfectly with the goal of developing a Self-Assessment System for BCM that is both rigorously designed and pragmatically useful.

One of the aspects of the research question defined is the possibility of supporting an organization and streamlining its organizational processes, with the definition of strategic guidelines for implementing a BCP [45]. To succeed with the BC endeavor, it is necessary to break down the task into smaller, more manageable parts and tackle them gradually [68]. Implementing a BCP and developing a self-assessment can be daunting, but it can be accomplished by breaking it down into smaller, more manageable tasks. A self-assessment can help an organization identify and prioritize these tasks, making it easier to implement a BCP over time.

The ability to solve the problem and the utility, efficacy, and quality of utilizing the artifact was demonstrated and evaluated through Focus Groups with experts in business continuity and semi-structured interviews with ICT and BC professionals and managers [44].

The activities in each stage of the DSR are illustrated in Figure 1, with particular relevance to steps 4 and 5, where the Self-Assessment Methodology was demonstrated and evaluated.

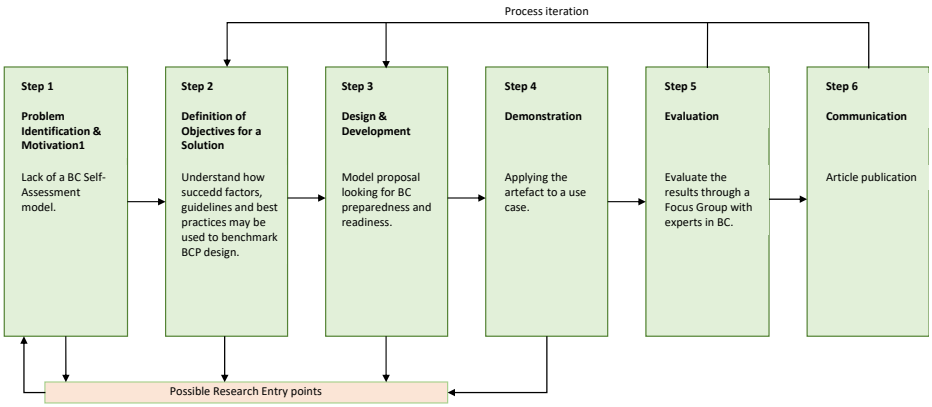

Figure 1. DSR methodology applied to the research (adapted from Hevner et al. [66]).

Figure 1 illustrates the six-step DSR methodology applied in this study to develop and validate the Self-Assessment System for BCM. The details for each step are as follows:

- Step 1—Identification of the problem and motivation: The relevance of the research problem to be tackled was identified, defined, and presented [17]. The research problem was identified as the lack of a standardized and comprehensive self-assessment methodology for BCM. Organizations face challenges in implementing BCM, such as high costs, lack of expertise, and insufficient top management awareness. There is a need for a structured self-assessment tool to evaluate BCM readiness, identify gaps, and improve organizational resilience. The problem was contextualized within the broader scope of BCM frameworks, standards, and best practices, as discussed in the background research.
- Step 2—Definition of the objectives of a solution: We defined what an improved artifact could accomplish and inferred the objectives of a solution from the definition of the problem and the knowledge of what is achievable and feasible [45]. The primary objective was to develop a Self-Assessment System that could help organizations evaluate their BCM readiness, identify gaps, and improve strategic alignment. The solution aimed to provide a structured and adaptable evaluation tool that could be used by organizations of all sizes, regardless of their current BCM adoption level. The Self-Assessment System was designed to integrate with any framework in the BCM scope. During the design phase, careful consideration was given to balancing comprehensiveness with usability to ensure that the Self-Assessment System could be adopted by organizations with varying levels of BCM maturity and resource availability. This balance was a key design decision grounded in DSR's emphasis on artifact relevance and applicability.
- Step 3—Design and development: Artefact development to solve the identified problem following the defined objectives. It comprises stating the artifact's desired functionality [69], its architecture, and the design of the prototype. The Self-Assessment System was designed to align with the BCM Model, which includes eight components and 118 activities. The eight components of the BCM Model were derived from a systematic literature review (SLR) of 167 publications, which identified recurring themes in BCM across sectors such as healthcare, finance, and energy. Key components—including Risk Assessment (RA), Business Impact Analysis (BIA), and ICT Strategy—were prioritized based on their frequency in the literature (e.g., RA appeared in 39 publications, BIA in 58) and their alignment with established standards like ISO 22301. Components such as 'Emergency Response' and 'Crisis Management' were added due to emerging trends in disaster resilience (e.g., 11 publications addressed natural disaster strategies). A structured set of questions was developed for each activity within the BCM Model components. Questions for each activity were formulated using evidence from the SLR, where specific gaps or best practices were highlighted (e.g., 23 publications emphasized cybersecurity measures in ICT Strategy, prompting dedicated questions on incident recovery). To ensure validity, questions were iteratively reviewed by a panel of five experts with >15 years of BCM experience, covering domains like risk management (16 years), ICT governance (21 years), and cybersecurity (22 years). Discrepancies were resolved through Delphi rounds until consensus was reached on clarity and relevance. These questions were designed to assess the organization's alignment with BCM best practices and standards. The questions were weighted based on their relevance and importance to the overall BCM process. Weightings were empirically determined through two methods: (1) a frequency analysis of SLR findings (e.g., 'ICT Strategy' received higher weights due to representation in 129 publications, versus 11 for supply chain risks), and (2) expert scale scoring (1–5) during the Focus Group session. For instance, metrics tied to data recovery (RTO/RPO) were weighted 30% higher than generic policy checks,

reflecting their critical role in 70% of disruption scenarios analyzed in the literature. The Self-Assessment System was formalized as a rapid assessment tool, enabling organizations to quickly evaluate their BCM readiness and identify critical issues. The system was designed to be user-friendly, with clear instructions and visual indicators (e.g., scorecards with color-coded results) to help users interpret their scores and identify areas for improvement. The artifact design followed an iterative development approach, allowing for continuous refinement based on expert feedback and empirical evaluation. This iterative process ensured that the Self-Assessment System was not only theoretically sound but also practically viable and responsive to real organizational contexts. The system underwent an iteration based on feedback from the Focus Group. For example, initial questions about 'cloud-computing redundancy' (from 11 SLR publications) were simplified after users noted technical complexity, while 'crisis communication' metrics were expanded following participant reports of ambiguity during simulated cyberattacks.

- Step 4—Demonstration: The feasibility of the artifact was demonstrated, allowing for an accurate assessment of its suitability for its purpose. With proof of concept, we demonstrated use of the artifact to address case scenarios through simulation. The resources required for the demonstration include adequate knowledge of how to use the artifact to solve the problem [65]. The Self-Assessment System was demonstrated through a Focus Group session with experts in business continuity, ICT governance, risk management, and cybersecurity. Participants were given a hands-on opportunity to interact with the system and simulate its application within their own organizations.
- Step 5—Evaluation: A design artifact's utility, quality, and effectiveness must be rigorously demonstrated through well-performed evaluation methods [66]. The business context defines the criteria for artifact evaluation. The assessment involves integrating the artifact into the business's technical infrastructure. How well the artifact supports a solution to the problem was observed and measured [44]. It included objective quantitative performance measures, using questionnaires to evaluate the artifact's characteristics. This quantitative evaluation employed validated scales (1–5) according to the domain of the problem. Participants rated each attribute on, for example, clarity, relevance, and usability. Open-ended responses were thematically grouped to contextualize scores. BC experts and professionals in the ICT and BC area were selected from various activity sectors. We evaluated the artifact's completeness and the quality of the changes resulting from the iterations [44]. The artifact evaluation enabled the development of a valid artifact aimed at reducing the identified problem. The evaluation strategy incorporated both qualitative and quantitative measures to rigorously assess the artifact's utility, quality, and effectiveness. Participant responses were analyzed using a thematic analysis approach [70], combining deductive coding based on the 16 predefined attributes (e.g., clarity, adaptability) and inductive coding for emergent themes. The authors coded the Focus Group transcripts, with discrepancies resolved through consensus. To ensure validity, coded data were cross-validated against questionnaire responses for usability, relevance, and clarity metrics.
  By involving diverse stakeholders from different sectors, the study ensured comprehensive validation of the Self-Assessment System's capability to identify BCM gaps and support continuous improvement.
- Step 6—Communication: Communicate the problem and its relevance, the Self-Assessment methodology artifact, its usefulness and novelty, the rigor of its design, and its effectiveness for researchers and professionals in the area. The importance and usefulness of the research and the various step results of the research were communicated to the scientific community, professionals, and interested organizations [44,45,64].

Our objective is to submit further scientific articles to journals to disseminate our findings and contributions widely. This research contributes to the DSR body of knowledge by providing a validated artifact that addresses a recognized gap in BCM assessment, demonstrating how design science principles can be effectively applied to develop tools that enhance organizational resilience and strategic management of BC.

4. Problem Identification and Motivation

In the previous section, the methodology was described. In this section, the research problem is stated, corresponding to step 1 of the DSR, considering what was discussed in theoretical background, in Section 2.

Due to feasibility concerns and associated costs, there are constraints and limitations throughout the BCMS implementation [43]. There are multiple efforts in the scientific and professional communities to systematize and reduce the complexity of BCMS implementation. The literature also reports various challenges to launching a BCM program, like the qualified expertise necessary to design and implement a BCP [71,72]. These constraints may be partly justified because the organization's top managers must be more aware of the benefits of continuity planning [73]. Furthermore, personnel may require additional resilience or recovery skills and assistance in understanding the importance of implementing a BCMS [74].

Medium-sized and small enterprises are more vulnerable to disasters due to limited financial and human resources and inadequate technological capabilities to recover from disasters [16]. Specific organizations delay BCP implementation for various reasons, such as design restrictions driven by technical or financial challenges or different interpretations of requirements [72]. Additionally, restrictive company policies or time constraints to finish the project might justify postponement [28].

Apart from these hurdles, some organizations may need more proactiveness in BC planning and Disaster Recovery [75]. This lack can lead to severe consequences, including damage to reputation and market share, impaired customer service and business processes, regulatory responsibility, and extended downtime and system recovery times. Thus, more organizations, particularly in the public sector, must implement and be certified in BCM Standards [76].

In his research, Stourac [63] proposes implementing an annual scorecard to ensure program realization to develop a measurable and successful BC program. Similarly, the author of [77] argued that only a limited number of methods are available to assess and measure how an organization allocates its time and resources to address the essential areas within BCM components. Zeng & Zio [61] propose their Framework for BC quantitative evaluation, highlighting the need for more clearly defined business metrics in the studied models.

Based on these models, BC quantitative analysis is therefore unfeasible, restricting its practical use [61]. The framework proposes four BC quantitative metrics based on the potential loss caused by disruptive events.

Although these studies confirm the relevance of measuring under the BC scope, they primarily focus on measuring an established BCM program or one of its components, such as metrics for ICT systems, disaster recovery plans, risk management, and financial loss or justification. We identified the need for a self-assessment system that covers all phases of a BCMS, including awareness and commitment of top management, understanding the organization and its information flows, and business processes. By integrating these components, the organization can identify risks and prepare measures and solutions to avoid or mitigate them. Assessing the BC planning and implementation phases, as well as conducting training, tests, and exercises under the PDCA life cycle, is essential.

5. Proposal

In the previous section, the research problem was defined, highlighting the challenges in BCMS implementation, such as cost, expertise, and management awareness, and emphasizing the need for a comprehensive self-assessment system covering all BCMS phases. In this section, the objectives and requirements of the Self-Assessment System are presented, detailing its integration with a BCM Model to help organizations evaluate their BCM readiness, transition to self-assessment, and establish a solid foundation for BCMS implementation.

5.1. Objectives and Requirements

Self-assessment tools are more likely to be effective when they are appropriate in conceptual scope and assessment content, provide diagnostic guidance, and have high validity [78]. Thus, to inform the developed Self-Assessment Methodology, we integrated it with the Framework for the Multidisciplinary Assessment of Organizational Maturity on Business Continuity Management (FAMMO^{CN}) [44]. FAMMO^{CN} defines a Model with components and activities organized to manage business continuity. Each component is organized into domains of action to make it easier to identify the activities' context. Each domain describes the activities that detail, among other things, the projects, actions, tasks, intents, initiatives, strategies, or policies that may be addressed, measured, or assessed.

It also provides an Implementation Guide with FAMMO^{CN} elements and implementation aspects.

The Self-Assessment System, integrated within FAMMO^{CN}, was designed to assist organizations in assessing their current state of BCM and identifying potential solutions for significant BC concerns. By utilizing the Self-Assessment System, organizations can better understand their BCM's strengths and weaknesses and develop strategies to improve their overall readiness for business continuity.

A structured set of questions was developed for each activity within the components of the BCM Model. Developing and integrating an assessment system with a model that supports it can be challenging, particularly when preparing an organization to plan a continuity response. This preparation must fulfill the organization's requirements to make the self-assessment system easy to apply while ensuring a robust and reliable continuity response.

The Self-Assessment System formalizes the rapid assessment process based on the BCM Model and the reviewed literature. The system defines and systematizes questions for each BCM activity, enabling organizations to identify critical issues that must be addressed in their BC activities and determine the appropriate course of action.

The Self-Assessment System was developed by selecting the most relevant questions inferred through analysis of the BCM frameworks, Standards, and reviewed literature to assess multidisciplinary BC preparedness. Therefore, its purpose is to provide a quick overview of the organization's state of BC readiness. The Self-Assessment System can be used by organizations of all sizes to assess their preparedness and readiness for BC, regardless of whether they plan to adopt a BCM Framework or are currently evaluating it for adoption.

5.2. From Self-Assessment to Measurement

Considering the structure of the BCM Model [44], we outlined a strategy to address the identified constraints across the various stages of organizational business continuity progress. The Implementation Guide supports using the Self-Assessment System in the initial stages of developing a BC response. Once the organization is sufficiently prepared, conscious, and disciplined in BC, it can use a measurement system to measure its BC preparedness and response systematically.

As BC awareness increases, it becomes relevant to strengthen organizational discipline and improve underlying BC processes, such as through the PDCA cycle or BCMS implementation.

The Self-Assessment System can set a starting point for the BCMS establishment. Prompt self-assessment enables internal and external benchmarking and visualization of the organization's present state. Ultimately, the objective is to support raising the commitment and awareness of Top Management to secure the required investment to develop a suitable BCMS for the organization.

However, as organizations adapt and their BC awareness grows, it is relevant to increase discipline in the processes that ensure the management of the organization's BCMS. In this context, if an organization decides to establish measurement as a management practice, it may undertake periodic and systematic assessments of its organizational maturity in the BC area, which correspond to advanced assessment, as depicted in Figure 2.

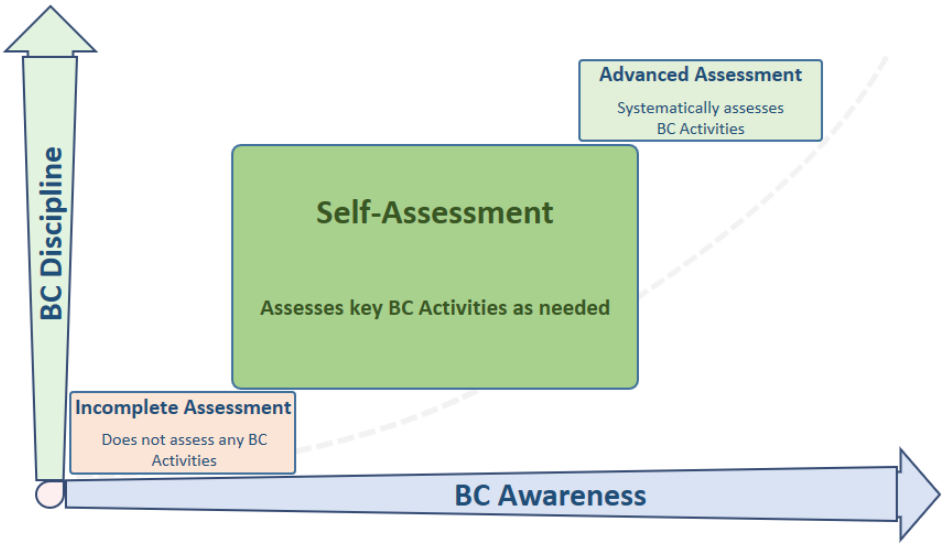

Figure 2. Stages of BC assessment in the organization.

Figure 2 is inspired by the stages of the CMMI process discipline, emphasizing that the foundation of process improvement lies in instilling discipline in the organization's culture [46]. Therefore, it is recommended that the organization self-assess its BC preparedness during a preparatory stage to quickly obtain an overall perspective. At this stage, the Self-Assessment System is used, considering essential activities within components, with compliance reported by quantitative answers to written questions in a simplified and straightforward manner.

Figure 2 illustrates that as BC awareness grows, there is a need to enhance organizational discipline and improve the underlying BC processes, for example through the PDCA cycle or a BCM System. To support organizations in various stages of BC, valuable assistance is required in initiating, planning, implementing, maintaining, reviewing, and improving the response, recovery, resumption, and restoration of business processes, focusing on ICT.

The Self-Assessment System provides a BC overall view of the organization, which may be a starting point for the BCMS implementation. The quick self-assessment enables the organization to visualize its present state and establish internal and external benchmarking. Thus, the objective is to support increasing the top management's commitment and awareness to attract the necessary investment to start and establish an appropriate BCMS.

Nonetheless, it is crucial to adapt and monitor the progress of BC awareness and the need for enhanced discipline in the processes that guarantee effective management of the

organization's BCMS. As a result, systematic assessment can transition into systematic measurement, entailing the definition of a scalable array of metrics for each activity. Each metric should evaluate an initiative that aids in achieving a certain level of activity readiness, preparedness, or compliance. Each metric's purpose is to guide the organization to understand what must be considered to achieve the activity's objective.

5.3. Self-Assessment System

The organization can self-assess its preparedness for BC in a preparatory phase for continuity and to capture a brief overview. The organization can establish a starting point for implementing a BCP through the Self-Assessment System support application, agilely measuring its current state of multidisciplinary preparedness in the BC area. At this stage, essential activities in each component are considered, reporting their compliance through written questions in a simplified and straightforward manner.

In selected activities for each BCM Model component, the organization directly answers self-assessment questions. A single activity may have several questions. The total score will be the sum of the weighted scores for each component, reporting model compliance.

The Self-Assessment System tool provides instructions to assist the evaluator in understanding and interpreting the questions available, as depicted in Figure 3.

Self-Assessment System

Instructions

You can fill in the information on the "Organizational Profile" sheet, to characterize the organization and identify the moment of the self-assessment.
In order to obtain a score for the various components of the BCM Model, you must fill in each sheet of this book. **Answer all questions.**
Read the self-assessment question and assess the achievement of the intention referred to in the question, according to the instructions below.
Fill in a value from 0 to 100 in the Scorecard 0 to 100 column (column G).
The value assigned to the question depends on the level of achievement that the organization considers to have achieved. The **colour of the semaphore** depends on the achievement value entered.
The total achievement value must be interpreted by each self-evaluator, taking into account the intentions defined in the question. Some questions suggest several intentions to be implemented, so the implementation of each one must be evaluated, in order to compose the evaluation of the question. For example: in the question "Has the organization defined and communicated policies within the scope of Business Continuity?" there are two underlying intentions, on the one hand the definition that is most relevant to the issue and on the other hand the communication of policies, which is relevant but may not have started for some reason. Thus, if the organization has defined policies but not communicated them, the score should be between 60 and 80.
Red: [0.60[-> **Value 0** indicates that the intent of the question has not yet been considered. At the upper bound value, the intent of the question has been planned or prepared and is waiting for implementation to begin.
Yellow: [60.90[-> **Value ≥60** indicates that the question intent has been initiated. At the upper limit value, the intent of the question is in the final stage of realization.
Green: [90,100] -> No relevant intervention is required, however adjustments may still exist.

Evaluation

The weighted value of the self-assessment question on the activity and component is shown in the **Weighted Score** column.
The **Component Score** is the sum of the **Weighted Score** column and indicates the component's current rating.
There are 4 sheets in this Excel workbook with the 8 components of the BCM Model that can be evaluated.
The Excel sheet "Total Score" presents the total evaluation, weighted according to the result of each component.

Legend

Domain: Each component is organized into domains of action, in order to speed up the identification of the context of the activities. Note: It has no influence on the measurement.
Activity weighting: Weight that indicates the relevance that each activity has in the component.
Activity: Details, among others, projects, actions, tasks, intentions, initiatives, strategies or policies that can be addressed and measured through metrics/questions.
Question ID: The question identification number.
Question weighting: Weight that indicates the relevance that the question has in the activity.
Assessment question: The question for self-assessment about what should be accomplished.
Scorecard 0 to 100: A value from 0 to 100 that indicates the level of achievement that the organization believes it has achieved.
Weighted score: The product of the weight of the activity in the component, the weight of the question in the activity, and the assessment value. (Activity Weighting X Question Weighting X Scorecard 0 to 100)
Component score: The sum of the weighted scores for each assessment question.

Figure 3. Self-Assessment System instructions.

The instructions assist the evaluator in understanding the range of values to use, what they mean, and how the Self-Assessment System is presented in the application tool.

Figure 4 depicts the organization's profile information and all the evaluators participating in the assessment.

Organizational Profile		
Self-Assessment date:		
Organization name:		
Activity sector:	<< Select >>	
Number of employees:	<< Select >>	
Turnover:	<< Select >>	
Comments:		

Contributors to the Self-Assessment			
Evaluator name 1:	**Profile:**	<< Select >>	**Date:**
Evaluator name 2:	**Profile:**	<< Select >>	**Date:**
Evaluator name 3:	**Profile:**	<< Select >>	**Date:**
Evaluator name 4:	**Profile:**	<< Select >>	**Date:**
Evaluator name 5:	**Profile:**	<< Select >>	**Date:**
Evaluator name 6:	**Profile:**	<< Select >>	**Date:**

Organizational Profile legend
Self-Assessment Date: Fill in the self-assessment completion date
Organization Name: Enter the organization name.
Activity sector: Select the activity sector, according to the Portuguese Classification of Economic Activities Rev. 3, of the National Institute of Statistics, I.P., 2007 Edition
Number of Employees: Fill in the number of employees (This covers full-time, part-time and seasonal employees. Apprentices or students in training are not counted)
Turnover: Select the annual turnover (calculation of the company's revenue during the year in question, resulting from its sales and provision of services, after paying any discounts and excluding VAT or other indirect taxes).
Comments: If you consider it relevant, you can register some notes or observations in this field.

Legend for Contributors to the Self-Assessment
Evaluator name: In this field you can register who collaborated in answering the self-assessment questions
Profile: In this field, you can register the profile or the functions that the evaluator performs in the organization.
Date: In this field you can record the date on which the collaboration was carried out.

Figure 4. Self-Assessment System profile.

This information is relevant for describing the organization and maintaining a benchmarking dataset. This benchmark is internal for comparing previous assessments but can be used for external benchmarking with other organizations.

The total score will be the sum of each component's weighted score, demonstrating compliance with the BCM Model. Figure 5 depicts the Self-assessment Methodology.

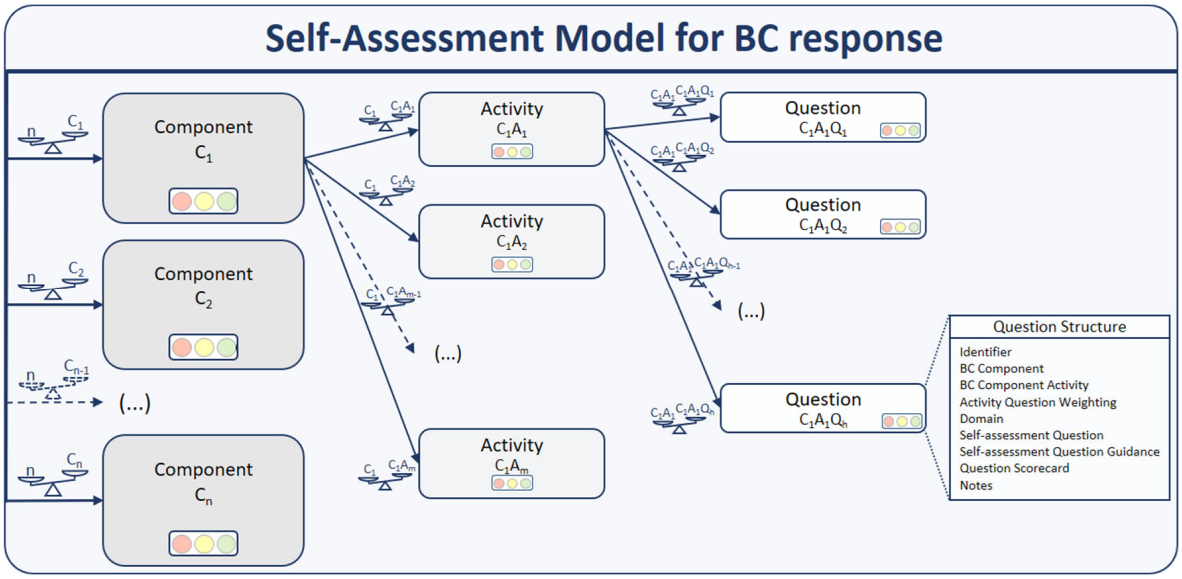

Figure 5. The Self-Assessment Model for BC response.

Figure 5 depicts the question's structure with nine attributes. In an activity, each question has a weight. The activities are weighted for each component, which in turn is weighted, providing their contribution to the assessment of the total score of the organiza-

tion. Components, activities and questions can be added according to the evolution of the model, this configuration being represented by (. . .) in the dashed arrows in Figure 5.

Thus, the metrics structure concepts apply to the Self-Assessment Methodology. However, only a subset of attributes are required for the self-assessment. The considered attributes in the Self-Assessment Methodology are presented in Table 1.

Table 1. Question structure attributes used in the Self-Assessment Methodology.

Attribute	Description	Classification
Identifier	Question identification number	Identification
BC Component	BC component identification	
BC Component Activity	Activity identification in the BC component	
Activity Question Weighting	Weight of the question to achieve the intention of the activity	
Domain	The field of action	
Self-assessment Question	The question for self-assessment about what should be accomplished	Self-assessment
Self-assessment Question Guidance	Guidelines for direct measurement in self-assessment, suggesting what should be achieved in each color of the scorecard	
Question Scorecard	The percentage range of accumulated measurements according to the goal of defining the color of the scorecard	Achievement
Notes	Relevant comments on any parameter	Evidence

The "Self-assessment Question Guidance" attribute in Table 1 indicates what is expected to be accomplished by the system user. Thus, this system assists the organization in understanding what has to be done within the BC scope, which is one of the research objectives.

Table 1 presents the protocol for assessing a component using the Self-assessment Methodology.

Table 2 shows the explanatory notes for each attribute:

1 *— The domain of the activity. It does not influence measurement.
2 *— The weighting (p) of activity A is referenced by pA. The sum of the weightings of all the essential activities in the component is 100.
3 *—Essential activities for the BCM Model component in the Self-assessment Methodology.
4 *—The question identification number.
5 *—The weighting (p) of question A1 in activity A. The sum of the question weightings for each activity is 100.
6 *—The self-assessment question no. 1 of activity A (A1), defined for domain X1. There may be multiple questions for a single activity.
7 *—The scorecard of the self-assessment question A1 (sA1). A value between 0 and 100 is accepted, represented by the semaphore. Red (<60), yellow ($\geq$60 and <90), or green ($\geq$90).
The Self-Assessment System adopts the FAMMO^{CN} maturity model, and the resulting score can be interpreted as an indicator of the organization's relative maturity in BCM preparedness. The scoring scale uses visual semaphores: red, yellow, and green, which offer an intuitive view of performance:

Table 2. Protocol for a BC component self-assessment.

Domain	Activity Weighting	Activity	Question ID	Question Weighting	Self-Assessment Question	Scorecard 0 to 100	Weighted Score
Domain X_1 (1 *)	pA (2 *)	Activity A (3 *)	# (4 *)	pA_1 (5 *)	Question A_1 (6 *)	sA_1 (7 *)	$pA \times pA_1 \times sA_1 = spA_1$ (8 *)
			#	pA_2	Question A_2	sA_2	$pA \times pA_2 \times sA_2 = spA_2$
Domain X_2	pB	Activity B	#	pB_1	Question B_1	sB_1	$pB \times pB_1 \times sB_1 = spB_1$
			#	pB_2	Question B_2	sB_2	$pB \times pB_2 \times sB_2 = spB_2$
	pC	Activity C	#	pC_1	Question C_1	sC_1	$pC \times pC_1 \times sC_1 = spC_1$
Domain X_3	pD	Activity D	#	pD_1	Question D_1	sD_1	$pD \times pD_1 \times sD_1 = spD_1$
					Component Score		$spA_1 + spA_2 + spB_1 + spB_2 + spC_2 + spD_1$ (9 *)

Red (0–59) suggests the organization has significant gaps and should prioritize foundational actions such as raising awareness, allocating roles, and defining policies.

Yellow (60–89) indicates that key activities have been initiated but are not yet systematically integrated; organizations in this range should focus on standardizing processes, formalizing documentation, and increasing training and testing frequency.

Green (90–100) reflects a well-established and integrated BCMS; however, continuous improvement should still be pursued, with efforts toward optimization, performance tracking, and external validation.

These ranges are not rigid levels of maturity but serve as diagnostic indicators to help organizations tailor their next steps according to their current preparedness stage.

8 *—The result of the self-assessment question is the product of the weighting in the activity (pA) by the metric weighting (pA1) and the entered value that defines the achievement of the intention defined in the self-assessment question (sA1). The weighted score of the question is referenced by spA1.
9 *—The component score is the sum of the weighted results of each self-assessment question. This value assumes values between 0 and 100.

The self-assessment of multidisciplinary preparedness in the BC area follows a defined protocol. The total score achieved will be the sum of the weighted score values of each component, which reflects compliance with the BCM Model, as shown in Table 3.

Table 3 provides explanatory notes on what is considered in order to obtain the total score:

1 *—The BCM Model component;
2 *—The number of questions answered out of the total of 61 questions defined. It is considered answered if the value is between 0 and 100;
3 *—The weighting (p) of the CA component is referenced by pCA. The sum of the weightings of all components is 100;
4 *—The score of the component resulting from its assessment (score) (see Table 2). A value between 0 and 100 is accepted, which is represented by the semaphore: red (≥ 0 and < 60), yellow (≥ 60 and < 90), or green (≥ 90 and ≤ 100);
5 *—The result of the component of the self-assessment is the product of the component weighting (pCA) by the value of the component score (score). The weighted score of the component is referenced by spCA;
6 *—The total score is the sum of the weighted results of each component. This value assumes values between 0 and 100.

Table 3. Protocol for self-assessment of all components.

BCM Model component	Answered Questions	Component Weighting	Component Score	Weighted Score
Top Management commitment (1 *)	# of 5 (2 *)	*p*CA (3 *)	*score*CA (4 *)	*p*CA × *score*CA = ***sp*CA** (5 *)
Understand the organization	# of 5	*p*CB	*score*CB	*p*CB × *score*CB = ***sp*CB**
Manage Risk	# of 8	*p*CC	*score*CC	*p*CC × *score*CC = ***sp*CC**
Consolidate the strategy for continuity	# of 11	*p*CD	*score*CD	*p*CD × *score*CD = ***sp*CD**
Plan and structure the continuity response	# of 11	*p*CE	*score*CE	*p*CE × *score*CE = ***sp*CE**
Implement and maintain continuity plans	# of 8	*p*CF	*score*CF	*p*CF × *score*CF = ***sp*CF**
Check the continuity management system	# of 8	*p*CG	*score*CG	*p*CG × *score*CG = ***sp*CG**
Improve the continuity management system	# of 5	*p*CH	*score*CH	*p*CH × *score*CH = ***sp*CH**
	# of 61		***Total Score***	*sp*CA + *sp*CB + *sp*CC + + *sp*CD + *sp*CE + *sp*CF + + *sp*CG + *sp*CH (6 *)

5.4. Components

The BCM components of the Self-Assessment System were derived from an extensive Systematic Literature Review (SLR) of existing BCM frameworks and models. This comprehensive analysis identified key areas essential for effective BC planning and response. The SLR encompassed various studies, including those that explored trends in BC planning and the development of BCM maturity models [45]. For instance, recent research [79] analyzed the existing literature to identify BCM processes and maturity models, providing valuable insights into the structuring of BCM components.

Additionally, studies such as [80] discussed the need for a BCP framework to handle threats or disasters, highlighting the importance of structured components within BCM. These insights, among others, informed the selection and definition of the eight components and 118 activities within the BCM Model, ensuring a comprehensive approach to organizational preparedness and resilience.

The recent literature continues to emphasize the significance of structured BCM frameworks. A study by Ostadi et al. [81] conducted an SLR to analyze organizational resilience, business continuity, and risk, contributing to the understanding of process resilience and continuity. These ongoing studies reinforce the relevance of the components identified in the BCM Model and support their application in current organizational contexts.

Therefore, the BCM Model encompasses relevant areas in BCM and defines eight components and 118 activities [44]. The strategic guidelines within the model are organized into components that must be addressed in the event of an interruption or disaster.

The demonstration and evaluation of the Self-Assessment Methodology revealed that a quick and efficient assessment that results in a score and allows for benchmarking with other organizations is crucial to justify BC. It was determined that the initiation of the BC program and ease of use of a BCM framework could be improved if each component included self-assessment questions. The questions should be of clear and

concise interpretation (self-assessment) and use a visual indicator to describe the purpose of the activity. Furthermore, it was considered that a self-assessment was necessary for overall recognition of compliance and could increase the adoption of a BCM framework and implementation of BC within an organization.

Each component is structured into operational domains to facilitate identifying the context of activities. Thus, each domain outlines the activities that detail the projects, actions, tasks, intentions, initiatives, strategies, or policies that can be addressed and assessed.

Hence, the activities with the highest relevance and added value were selected to represent the essential strategic guidelines defined in the model and emphasized by the Standards. This emphasis is reflected in the weight given to each activity for the BC component. Some activities may contain multiple self-assessment questions. In these cases, the relevance of each question is quantitatively distributed through the weighting attribute.

Figures 6–13 list the components of the Self-Assessment System and their related activities. Each component has a set of questions that were filled with random values in the presented cases.

Top Management commitment

Domain	Activity weighting	Activity	Question ID	Question weighting	Assessment question	Scorecard 0 to 100	Weighted score
Leadership	0.2	Define the strategy, objectives and how they align and achieve.	1	1	Has the organization defined the overall strategy and objectives for Business Continuity?	50	10.00
	0.2	Define and communicate policies.	2	1	Has the organization defined and communicated policies within the scope of Business Continuity?	75	15.00
Support	0.25	Appoint people and teams, define their roles, responsibilities and authority.	3	0.6	Has the organization appointed people or teams within the scope of Business Continuity?	90	13.50
			4	0.4	Has the organization defined the roles, responsibilities and authority of people or teams within the scope of Business Continuity?	50	5.00
Commitment	0.35	Demonstrate commitment and active involvement in business continuity management.	5	1	Does the organization demonstrate commitment and active involvement in the management of Business Continuity?	90	31.50
						Component score	75.00

Figure 6. Self-assessment questions for the Top Management Commitment component.

Figure 6 focuses on the "Top Management Commitment" component and continuous management activities that support the BCM program. Top management must demonstrate leadership and commitment and support BCMS activities.

Figure 6 summarizes Top Management's responsibilities: define the strategy and objectives, define policies, appoint BC teams, ensure adequate resources, and demonstrate active involvement in the BCM.

The component "Understanding the organization" in Figure 7 aims to determine which factors are relevant to the organization's mission, which involves delivering products or services and impacting the expected BCMS results.

Understand the organization

Domain	Activity weighting	Activity	Question ID	Question weighting	Assessment question	Scorecard 0 to 100	Weighted score
Organization	0.1	Understand the organization's structure and management, roles, responsibilities, requirements, and authority and communication systems	6	1	Does the organization understand how is defined the management structure, operating model and assigned roles and responsibilities?	90	9.00
Processes and technology	0.3	Identify ICT services, infrastructure and assets, technology and applications.	7	1	Has the organization identified and understood the services, infrastructure, assets, technologies and applications that enable ICT processing?	60	18.00
	0.3	Identify products, services and their processes, activities, flows and resources.	8	1	Has the organization identified and understood the value streams and processes, namely the activities, workflows, controls, procedures and resources needed to achieve agreed objectives?	75	22.50
	0.1	Understand the needs, capabilities, relationships and information flows of interested parties, identifying internal and external issues and their requirements and formalities.	9	1	Has the organization identified internal and external issues and their requirements and formalities in order to understand the needs, capabilities, relationships and information flows with stakeholders?	80	8.00
People	0.2	Identify and describe the necessary skills of human resources and their training.	10	1	Has the organization identified and described the necessary skills, training and certification of human resources within the scope of Business Continuity?	90	18.00
						Component score	75.50

Figure 7. Self-assessment questions for the Understand the Organization component.

As a summary of Figure 7, the organization must understand its organizational structure and culture, the products and services delivered and the related business processes, the information flows, and necessary technologies.

Figure 8 depicts the "Manage Risk" component, which aims to determine risks based on the outcomes of Understanding the Organization, assess the impact of risks and opportunities identified, and plan risk management according to the defined strategy.

Manage Risk							
Domain	**Activity weighting**	**Activity**	**Question ID**	**Question weighting**	**Assessment question**	**Scorecard0 to 100**	**Weighted score**
Governance	0.1	Develop a risk or opportunity management strategy.	11	1	Has the organization developed risk or opportunity management strategies?	78	7.80
	0.1	Develop risk or opportunity management plans.	12	1	Has the organization developed risk or opportunity management plans?	45	4.50
Risk management	0.2	Identify and document risks and opportunities.	13	0.6	Does the organization identify and document risks and opportunities?	98	11.76
			14	0.4	Does the organization monitor and communicate risks and opportunities?	23	1.84
	0.1	Analyse risks and opportunities.	15	1	Does the organization analyse risks and opportunities?	99	9.90
	0.2	Address risk by planning appropriate risk responses.	16	1	Does the organization plan appropriate responses to address risks and opportunities?	34	6.80
Business Impact Analysis	0.2	Conduct Business Impact Analysis (BIA) and assess and estimate the probability, impact and proximity of risks, prioritize risks and understand risk exposure.	17	1	Does the organization perform the Business Impact Analysis?	56	11.20
	0.1	Monitor the probability and severity of risks occurring.	18	1	Does the organization monitor the probability and severity of risks occurring?	98	9.80
						Component score	63.60

Figure 8. Self-assessment questions for Manage Risk component.

As a summary of Figure 8, the organization must develop risk management strategies and plan its activity to cope with risks. Risks must be analyzed, evaluated for their business impact, and treated with the appropriate response that ensures continuity and predefined readiness.

Figure 9 depicts the component "Consolidate the Strategy for Continuity", which strives to establish strategies that allow the BC objectives to be met, following the continuity requirements and available resources.

Consolidate the strategy for continuity							
Domain	**Activity weighting**	**Activity**	**Question ID**	**Question weighting**	**Assessment question**	**Scorecard0 to 100**	**Weighted score**
Governance	0.2	Consider developing backup policies.	19	1	Does the organization have backup policies?	56	11.20
	0.1	Consider implementing alternative solutions, including manuals, while ICT systems are re-established.	20	1	Has the organization considered implementing workarounds to be activated while ICT systems are re-established?	87	8.70
Communication and reporting	0.05	Consider developing communication and reporting strategies in the event of an incident or disaster.	21	1	Does the organization have communication and reporting strategies in the event of an incident or disaster?	67	3.35
Resources	0.05	Support strategies and plans by ensuring that financial resources and investments are effective and available.	22	1	Does the organization ensure the necessary financial resources and investments for continuity plans?	9	0.45
	0.05	Consider the management of contracted ICT services.	23	1	Does the organization ensure that contracted ICT services are managed?	89	4.45
	0.05	Consider implementing contingency solutions in information systems and ICT.	24	1	Does the organization ensure that contingency solutions are implemented in information systems and ICT?	78	3.90
Security	0.2	Consider developing information security policies.	25	1	Does the organization have information security policies?	98	19.60
	0.05	Consider implementing and maintaining preventive, detection and corrective measures to protect information systems and ICT from software and malicious attacks.	26	1	Has the organization implemented and maintain preventive, detection and corrective measures to protect information systems and ICT from software and malicious attacks?	56	2.80
Monitoring	0.05	Consider monitoring and managing the events that may cause an incident or disaster in accordance with the event monitoring policy.	27	1	Does the organization have policies for monitoring known events that could cause an incident or disaster?	78	3.90
Training	0.1	Consider developing strategies for periodic training of staff with responsibilities in the plans.	28	1	Does the organization have periodic training strategies for staff with responsibilities in the plans?	56	5.60
Exercises and tests	0.1	Consider developing strategies for exercises and testing plans.	29	1	Does the organization have strategies for exercising and testing the plans?	87	8.70
						Component score	72.65

Figure 9. Self-assessment questions for the Consolidate the Strategy for Continuity component.

Figure 9 highlights how the organization should consider the strategy for its BCMS, the communication in case of an incident or disaster, and contingency strategies regarding the delivery of products and services. Staff assistance is relevant, as is facilities safety and maintenance. The ICT strategy and security must be established following the defined recovery times. This set of activities should integrate the development of strategies for training on continuity and plans. The organization should also consider strategies for exercises and tests to ensure the effectiveness and efficiency of preparedness, readiness, and responsiveness to disruptive events impacting the activity.

The "Planning and Structure the Continuity Response" component in Figure 10 aims to develop and document the plans and capacity required to execute the stated strategy and the BCM program.

Plan and structure the continuity response							
Domain	**Activity weighting**	**Activity**	**Question ID**	**Question weighting**	**Assessment question**	***Scorecard0 to 100***	***Weighted score***
Governance	0.05	Engage and validate the organization's plans with identified stakeholders.	30	*1*	Has the organization engaged and validated plans with stakeholders?	**67**	*3.35*
Scope	0.2	Development of business continuity plans that focus on sustaining the organization's prioritized business activities and processes.	31	*1*	Has the organization developed business continuity plans that focus on sustaining business activities and processes?	**67**	*13.40*
	0.05	Development of operation continuity plans that focus on restoring the organization's mission-critical functions to an alternate location.	32	*1*	Has the organization developed operation continuity plans that focus on restoring the organization's mission-critical functions to an alternate	**56**	*2.80*
	0.2	Development of disaster recovery plans that focus on information systems and ICT and that may require relocation.	33	*1*	Has the organization developed disaster recovery plans that focus on information systems and ICT?	**56**	*11.20*
	0.1	Development of information systems contingency plans that establish procedures for the assessment and recovery of a system or operation.	34	*1*	Has the organization developed information systems contingency plans that establish procedures for their assessment and recovery?	**67**	*6.70*
	0.15	Development of security and cybersecurity incident response plans that establish the procedures that deal with the detection, response and recovery of a computer security event or incident.	35	*1*	Has the organization developed security and cybersecurity incident response plans that establish procedures that deal with detection, response and recovery?	**78**	*11.70*
	0.05	Development of communication plans that document standard procedures for internal and external communication in the event of a disruptive event.	36	*1*	Has the organization developed communication plans that document standard procedures for internal and external communication?	**98**	*4.90*
Documentation	0.05	Document the phases of activation, notification and recovery of an incident or disaster and reconstitution and cessation after its	37	*1*	Has the organization documented the activation, notification, recovery, reconstitution and cessation phases of an incident or disaster in the plans?	**34**	*1.70*
	0.05	Define and document the conditions, dependencies and procedures for recovery and restoration of processes, technology, information, services, resources, facilities, programs and infrastructure.	38	*1*	Has the organization documented, in the plans, the conditions, dependencies and procedures for the recovery and restoration of processes, technologies, information, services, resources, facilities, programs and infrastructures?	**76**	*3.80*
	0.05	Document in the plans the procedures to be followed that allow the continuous operation and delivery of products and services and the details for managing the immediate consequences of the interruption.	39	*1*	Has the organization documented, in the plans, the procedures to be followed that allow for the continuous operation and delivery of products and services and the details to manage the immediate consequences of the interruption?	**34**	*1.70*
	0.05	Document and section in each plan, the roles, responsibilities and competencies of each team that will implement the plan, including the task lists with assigned people.	40	*1*	Has the organization documented, in the plans, the roles, responsibilities, competencies and task list of each team that will apply the plan?	**34**	*1.70*
						Component score	**62.95**

Figure 10. Self-assessment questions for the Plan and Structure the Continuity Response component.

To summarize Figure 10, the organization should develop and document the plans in the BC scope that it considers appropriate, according to the strategies defined and the BIA. The following procedures must be included in the documentation according to the incident or disaster stages.

Figure 11 depicts the "Implement and Maintain Continuity Plans" component, aiming to implement the directives, actions, solutions, and processes required to accomplish the continuity objectives as planned.

Implement and maintain continuity plans							
Domain	**Activity weighting**	**Activity**	**Question ID**	**Question weighting**	**Assessment question**	***Scorecard0 to 100***	***Weighted score***
Documentation	0.05	Securely store and distribute each plan and supporting documentation to duly authorized stakeholders ensuring accessibility and usability in all disruption scenarios and whenever and wherever needed.	41	*1*	Does the organization ensure that plans and supporting documentation are distributed, stored and accessible to interested parties?	**23**	*1.15*
Measures, processes and solutions	0.1	Implement and maintain preventive, detective and corrective security measures, including the protection of information systems and ICT against malicious attacks.	42	*1*	Does the organization ensure that preventive, detective and corrective security measures are implemented and maintained to protect information systems and ICT against malicious attacks?	**56**	*5.60*
	0.2	Implement and maintain selected business continuity solutions so they can be activated when needed.	43	*1*	Does the organization ensure that business continuity solutions are implemented, maintained and activated when necessary that allow implementing what has been defined in the plans?	**87**	*17.40*
Backups	0.1	Implement, test and periodically update procedures and back up systems, applications, data and documentation to continue the organization's operations on-site or off-site, according to a defined schedule.	44	*0.6*	Does the organization ensure that procedures for backing up systems, applications, data and documentation are implemented in accordance with backup policies?	**98**	*5.88*
			45	*0.4*	Does the organization ensure that procedures for backing up systems, applications, data and documentation are tested and updated, according to a defined schedule?	**9**	*0.36*
Incident	0.15	Develop, keep up to date and follow an approach to incident prevention and resolution that includes recording, tracking and reporting status.	46	*1*	Does the organization have and ensure that an information system is maintained to manage and support incident resolution?	**78**	*11.70*
Training	0.2	Implement awareness and regular training on the plans as planned.	47	*1*	Does the organization ensure that awareness and training on the plans is performed regularly as planned?	**67**	*13.40*
Exercises and tests	0.2	Develop and document periodic exercises and tests to validate plans and the effectiveness of your business continuity strategies and solutions over time.	48	*1*	Does the organization ensure that periodic exercises and tests are performed and documented to validate implemented plans?	**65**	*13.00*
						Component score	**68.49**

Figure 11. Self-assessment questions for the Implement and Maintain Continuity Plans component.

Summarizing Figure 11, the organization must implement continuity solutions that provide security, continuity, and compliance with the defined requirements, implement and maintain training within the BC scope, and perform exercises and tests as planned. Having the required resources available before, during, and after a disruption is essential.

Figure 12 depicts the "Check the Continuity Management System" component that advises the organization to check the BCMS's adequacy, effectiveness, and requirements.

Check the continuity management system							
Domain	**Activity weighting**	**Activity**	**Question ID**	**Question weighting**	**Assessment question**	***Scorecard0 to 100***	***Weighted score***
Change management	0.2	Review and approve continuity plans by the responsible teams to identify necessary changes and actions to be addressed.	49	1	Does the organization review plans to identify necessary changes and actions to address?	**13**	*2.60*
	0.1	Regularly assess and document the implementation of changes resulting from preventive and corrective actions to assess their success.	50	1	Does the organization regularly assess the success of implementing changes resulting from preventive and corrective actions?	**15**	*1.50*
Compliance and Audit	0.15	Regularly assess policies, programs, plans, procedures and capabilities using performance objectives reflected in the BCMS.	51	1	Does the organization regularly assess plans against defined performance objectives?	**56**	*8.40*
	0.1	Conduct internal or external audits at planned intervals to provide information on the compliance and effectiveness of the BCMS, as defined in the audit programs.	52	1	Does the organization ensure that an audit is performed on the compliance and effectiveness of the Business Continuity Management System?	**45**	*4.50*
Suppliers	0.1	Review contracts and service levels to ensure that vendors provide adequate support to meet system availability requirements.	53	1	Does the organization periodically review contracts and service levels with suppliers to verify that they meet defined requirements?	**78**	*7.80*
Training	0.1	Assess continuity training according to plan.	54	1	Does the organization assess the compliance of the performed training with the plan?	**90**	*9.00*
Exercises and tests	0.2	Assess the exercises and tests of each plan regarding procedures, training, capabilities and achievements to identify opportunities for improvement.	55	1	Does the organization assess the exercises and tests of each plan to identify opportunities for improvement?	**76**	*15.20*
Monitoring	0.05	Use methodologies to continuously monitor, measure, analyse and assess the performance and effectiveness of the BCMS.	56	1	Does the organization monitor the Business Continuity Management System implemented?	**95**	*4.75*
						Component score	**53.75**

Figure 12. Self-assessment questions for Check the Continuity Management System component.

As a summary of Figure 12, the organization should review the continuity plans to check compliance with the requirements. The changes, the training and its materials, the exercises, and the tests performed should be evaluated to check the adequacy and identify opportunities for improvement.

The component "Improve the Continuity Management System" in Figure 13 aims to ensure that the organization discovers opportunities for improvement, according to the checks performed, and implements the necessary actions to achieve the continuity and the BCMS objectives.

Improve the continuity management system							
Domain	**Activity weighting**	**Activity**	**Question ID**	**Question weighting**	**Assessment question**	***Scorecard0 to 100***	***Weighted score***
Change management	0.1	Consider evaluating the implementation of changes resulting from preventive and corrective actions to improve the effectiveness of plans through the proposal or reformulation of preventive or corrective actions.	57	1	Does the organization propose and reformulate preventive and corrective actions, resulting from the evaluation of its implementation, in order to improve the effectiveness of the plans?	34	3.40
Corrective process	0.3	Establish a documented process of preventive and corrective actions and implement the necessary actions to achieve the intended results of the BCMS.	58	1	Has the organization implemented the necessary preventive and corrective actions to achieve the intended results of the Business Continuity Management System?	56	16.80
Training, exercises and tests	0.25	Revise the training and its materials as needed to reflect changes in plans and feedback on the effectiveness of the training.	59	1	Does the organization review and propose improvements to the training and its materials to reflect changes in plans and feedback on the effectiveness of the training?	78	19.50
	0.25	Review exercise results and test plans to support problem resolution and improve responsiveness to significant disruptions.	60	1	Does the organization review the results and propose redesigning the exercises and testing the plans to improve the plans?	34	8.50
Continuous improvement	0.1	Maintain and regularly communicate the overall quality plan that promotes continuous improvement.	61	1	Does the organization have an overall quality plan that promotes continuous improvement?	89	8.90
						Component score	57.10

Figure 13. Self-assessment questions for Improve the Continuity Management System component.

To summarize Figure 13, the organization must establish a process of preventive and corrective actions and perform the required actions to accomplish the BCMS's intended results, training, exercises, and tests.

The application tool automatically calculates the BC component scores when the user completes the self-assessment questions shown in Figures 6–13. Figure 14 depicts the overall score of an example assessment following the protocol described in Table 3.

Components	**Questions answered**	**Component weight**	**Component score**	***Weighted score***
Top Management commitment	5 of 5	0.15	***75.00***	11.25
Understand the organization	5 of 5	0.10	***75.50***	7.55
Manage Risk	8 of 8	0.15	***63.60***	9.54
Consolidate the strategy for continuity	11 of 11	0.10	***72.65***	7.27
Plan and structure the continuity response	11 of 11	0.15	***62.95***	9.44
Implement and maintain continuity plans	8 of 8	0.20	***68.49***	13.70
Check the continuity management system	8 of 8	0.07	***53.75***	3.76
Improve the continuity management system	5 of 5	0.08	***57.10***	4.57
	61 of 61		***Total Score***	**67.08**

Evaluation:	The semaphore colour of **Total Score** and **Component score** has the following interpretation: **Red:** [0.60[-> Implies the need for intervention. Value 0 indicates that the components' intentions have not yet been considered. At a value of <60, generally, the components' intentions have been planned and are waiting for the implementation to start. **Yellow:** [60,90[-> Indicates that it is important to understand evolution. Value ≥60 indicates that component intents have been initiated. At a value of <90, the components' intentions are in the final stage of realization. **Green:** [90,100] -> Targets have been achieved and no relevant intervention is required, however adjustments may still exist.

Legend:	**Components:** They represent the major areas of Business Continuity. **Questions answered**: Indicates the questions that have a value inserted, even though the value is 0. **Component weight**: Weight that the component has. **Component score**: The sum of the weighted scores of each assessment question, which represent the components presented in the Excel sheets. **Weighted score**: The product of the component's weighting and the component's score obtained in the Excel sheets. **Total Score**: The sum of the weighted scores of each component that indicates compliance with BCM Model.

Figure 14. Total score in the Self-assessment application tool.

The data in Figure 14 allow the user to quickly assess the overall score of the multidisciplinary preparedness of the BC response. The interpretation of the semaphore color of the Total score and the Component score is as follows:

- Red: [0–60[Implies the need for intervention. Value 0 indicates that the intents of the components must still be considered. At a score of <60, the components' intents have been planned and are awaiting implementation.
- Yellow: [60–90[Indicates the importance of understanding evolution. Value ≥ 60 indicates that component intents have begun. At a value of <90, the components' intents are nearing completion.

- Green: [90–100[Targets have been met, and no relevant intervention is required; nevertheless, adjustments may be necessary.

6. Demonstration

In the previous section, the objectives and requirements of the Self-Assessment System were outlined, emphasizing its role in assessing BCM readiness and supporting BCMS implementation. This section focuses on demonstrating the system through semi-structured interviews with ten organizations. These interviews provided insights that refined the system's clarity and applicability, reinforcing its role in guiding resource allocation, enhancing top management commitment, and optimizing BC strategies.

6.1. Focus Group Session

The Self-Assessment System was first demonstrated through a Focus Group session, which was part of the iterative DSR process [66]. The primary goal of the demonstration was to showcase the artifact's functionality, gather initial feedback, and refine its clarity and applicability. The session was planned to allow participants to interact with the system, providing them with a hands-on opportunity to evaluate its effectiveness in real-world scenarios. The proof of concept developed utilizes adequate knowledge of how to use the artifact [65].

To ground the demonstration in practical application, participants were presented with a simulated organizational scenario involving a mid-sized financial institution facing a cyberattack. The scenario required the use of the Self-Assessment System to evaluate BCM readiness, prioritize recovery actions, and align responses with organizational priorities. This hands-on exercise allowed participants to test the artifact's functionality in a controlled yet realistic environment.

The planning of the session followed the methodology outlined by Tremblay et al. [82], ensuring a balance between exploratory and confirmatory approaches. Due to constraints in assembling a specialized group of experts and scheduling availability, the session was designed to gather incremental improvements while simultaneously demonstrating the artifact's utility. The session was recorded and transcribed to ensure a systematic qualitative analysis, facilitating structured extraction of insights for continuous improvement. Informed consent was obtained from all participants in the study. All participants were assured confidentiality and anonymity, and ethical guidelines consistent with institutional research standards were strictly followed throughout the study.

A thematic analysis approach was employed to analyze the qualitative data collected during the session, enabling the identification of recurring themes, patterns, and participant sentiments regarding the artifact's usability and applicability.

The Focus Group included professionals from various sectors, such as ICT governance, risk management, cybersecurity, and business continuity planning, comprising one ICT Governance Director (27 years of experience), one Cybersecurity Lead Researcher (22 years), one Risk Manager from the banking sector (16 years), one Public Sector IT Manager (21 years) and one Security Solutions Managing Partner (24 years). The session involved a total of five participants [82] selected based on their extensive professional experience (minimum 5 years) in BCM-related fields, ensuring a diverse representation of expertise. Participants were invited through a purposive sampling method targeting recognized experts and practitioners in their respective domains. Care was taken to ensure the independence of participants by including professionals from different organizations and industries, minimizing potential bias. The selection deliberately included two strategic decision-makers (ICT Governance Director, Managing Partner) responsible for BCM budget approvals, and three operational practitioners (Risk Manager, IT Manager, Security Re-

searcher) directly implementing continuity plans. This balance enabled evaluation of both the artifact's tactical usability and its alignment with organizational leadership priorities.

The session's small group size (n = 5) followed Tremblay et al.'s [82] recommendations for in-depth discussion, while the 90 min duration allowed each participant 18–22 min of active engagement time. Participants' average 22 years of BCM experience (range: 16–27) ensured high-credibility feedback.

The participants were encouraged to simulate the application of the Self-Assessment System within their own organizations. The session followed a structured format, starting with an introduction to the selected BCM model and a presentation of the artifact. Participants then engaged with the system, followed by a concluding discussion to gather insights on its usability, effectiveness, and alignment with BC strategies.

For instance, one participant walked through the system's scoring mechanism to assess their organization's incident response capabilities. The tool flagged gaps in crisis communication protocols, prompting a discussion on how to integrate predefined communication templates into the artifact. This interaction demonstrated the system's ability to surface actionable insights during a disruption.

Consequently, the Focus Group communications were collected and analyzed to improve and optimize the proposed artifact [44]. The demonstration revealed the artifact's potential to guide organizations in prioritizing resources and selecting appropriate BC strategies. Participants noted that the tool's structured metrics helped them identify overlooked dependencies, such as third-party vendor risks, which were not previously included in their BC plans. One participant remarked, 'The scoring system forced us to confront weaknesses in our supply chain continuity planning—this alone justified the exercise. However, feedback indicated a need for greater clarity in scoring interpretations and crisis communication mechanisms. These aspects were subsequently refined in the artifact's next iteration. The session also highlighted the interest of professionals in understanding how the system could be integrated into their existing BCMS, further supporting its relevance in addressing BC challenges.

6.2. Results of the Demonstration

The DSR design is inherently an iterative and incremental activity [66]. The artifact is deemed complete when it meets the defined requirements and effectively addresses the identified constraints. Hence, the Self-Assessment Methodology, as demonstrated, copes with instances of the problem.

The demonstration revealed both incomplete and complete aspects of the Self-Assessment System. While the artifact demonstrated significant promise, several refinements were needed to improve its clarity and usability. The participants found that while the system addressed key aspects of BC planning, certain areas, such as score interpretation and subjectivity in scoring values, required further clarification. The improvements were made and used in the evaluation phase.

For example, the artifact's 'crisis communication' module was revised to include customizable templates for stakeholder notifications, addressing feedback that generic prompts were insufficient. Another participant highlighted how the tool's benchmarking feature revealed their organization's lag in IT recovery preparedness compared to industry peers, leading to a reallocation of training budgets. This real-world impact demonstrates how the tool transitions from theoretical assessment to actionable business decisions, directly addressing the practitioner need for measurable ROI in continuity planning investments.

In addition to qualitative feedback, structured questionnaires were administered to quantitatively assess participant perceptions of the artifact's effectiveness and usability. Descriptive statistics summarized the responses, while inferential analyses, such as mean

comparisons and variance assessments, were performed to evaluate the consistency and significance of user feedback across different expert groups.

Session surveys showed that 80% of participants agreed the tool would reduce BC planning time, while 70% confirmed it clarified resource allocation priorities.

Despite the need for refinements, the Focus Group feedback indicated that the Self-Assessment System was comprehensive in its approach to guiding organizations in resource allocation and BC strategy selection. The professionals in the Focus Group expressed strong interest in the artifact's potential application within their own organizations, signaling a positive reception toward its future use.

7. Evaluation

In the previous section, the demonstration of the Self-Assessment System was presented, focusing on its validation through an iterative DSR process and expert feedback. This section shifts towards evaluating its effectiveness and applicability within real-world organizational contexts. The evaluation process involved a structured methodology based on semi-structured interviews with professionals from various industries, combined with Focus Group-type discussions.

The objective of this evaluation was to assess the artifact's usability, accuracy, and alignment with BC strategies. Participants provided qualitative insights that informed refinements, ensuring the system's clarity and practical utility. This chapter details the methodologies employed, the key findings derived from participant interactions, and the iterative improvements implemented as a result.

7.1. Evaluation Process

The evaluation phase aimed to assess the effectiveness and applicability of the Self-Assessment System in a real-world context. This was achieved through a structured methodology combining semi-structured interviews with Focus Group-type discussion. Participants engaged with the artifact, providing qualitative feedback that informed refinements in its design and functionality.

To substantiate claims of increased top management awareness, interview surveys were administered to participants, measuring changes in perceived leadership engagement (e.g., 'How often does your leadership team discuss BCM priorities?'). Results showed an increase in reported "frequent discussions" post-using the Self-Assessment System.

7.2. Semi-Structured Interviews

A series of semi-structured interviews were conducted with professionals from ten medium-sized and large organizations. The semi-structured interview aimed to gather information and concrete evidence to assess the artifact's usefulness, quality, and effectiveness in addressing the defined problem.

The participating organizations spanned medium (30%) and large enterprises (70%) across high-risk sectors including finance, insurance, and critical infrastructure, with organizational cultures ranging from hierarchical public institutions to agile tech firms, reflecting diverse risk profiles from operational disruptions to cyber threats.

Invitations for the planned semi-structured interviews were sent at least one week in advance, along with access to the Self-Assessment System. These individuals, holding senior positions such as managers, senior managers, and top executives, had extensive experience in ICT and BC Planning. Their direct involvement in executing and managing BCP, developing BC solutions and in managing BC strategies provided valuable perspectives on the Self-Assessment System's applicability.

Interview participants were invited to complete the Self-Assessment System prior to their scheduled sessions, ensuring their responses were as precise as possible and reflective of their organizational context. This was achieved by simulating the use of the artifact and examining the professionals' insights, views, and understanding, which were elicited through the semi-structured interview. For this reason, they were requested to fill it out in advance according to the instructions, providing data as accurate as possible regarding the organization's context [44].

During the interviews, participants reviewed their responses, addressed missing answers, and clarified specific questions. Explanatory texts were utilized to enhance understanding of scoring values, including score intervals and descriptive justifications. However, some professionals indicated that the subjectivity of certain scoring values required additional clarification, leading to the implementation of an option allowing participants to add notes to self-assessment questions.

7.3. Overview of a Use Case

A medium-sized organization in the delivery services sector used the Self-Assessment System to evaluate its BC readiness. The senior manager, after completing the system in advance, discussed the results with the interviewer, identifying gaps in their current BCMS. Through the collaborative review, the manager was able to refine their resource allocation strategy and increase awareness of the importance of top management commitment to the BC planning process. The insights gained from the self-assessment enabled the organization to prioritize areas requiring improvement and secure necessary investments for future resilience. Post-assessment, the organization expects a 50% reduction in time-to-recovery during a simulated outage, directly attributed to revised resource allocation. It was recommended that leadership meetings referencing BCM metrics be increased from quarterly to monthly, evidenced by the relevancy of the Self-Assessment System's description of activities.

Beyond this specific use case, broader insights from multiple participants helped refine the system further.

7.4. Key Findings and Refinements

Findings from the evaluation process underscored the Self-Assessment System's role in increasing top management commitment and awareness. By providing structured insights into BC readiness, the system supports organizations in justifying necessary investments to establish and enhance BCMS. Moreover, participant feedback guided refinements aimed at enhancing usability, including clearer score interpretations and expanded documentation.

Participants within the organization in the delivery services sector reported that usability improved after refinements, particularly with "ease of score interpretation". Feedback highlighted the need for crisis communication templates, which were subsequently integrated into the Implementation Guide, resulting in a 100% validation rate for this feature during follow-up feedback. These measurable improvements in both usability and adoption rates demonstrate how the system translates theoretical BCM principles into practical tools that directly address common pain points in organizational continuity planning.

Overall, the evaluation process demonstrated that the Self-Assessment System effectively supports organizations in prioritizing resource allocation and selecting BC strategies that align with their operational capacities and strategic objectives. The iterative refinements driven by expert feedback further enhanced its reliability and applicability within various organizational contexts.

Improvements and refinements can be triangulated across three data sources: (1) interview transcripts, (2) organizational BCMS audit reports (shared by the participants),

and (3) system-generated scorecards showing progression in maturity levels (e.g., 80% of organizations advanced in scoring of 'Risk Assessment' within six months).

During the interviews, the Self-Assessment System was used to review the previous answers, fill in blank answers, and explain some questions or elements in the support documentation. However, the organizations completed the Self-Assessment System and reviewed the filled scores based on their interpretation of the questions. Explanatory texts were used to clarify the scoring values of each question, namely the score intervals and description. However, some participants felt the need to clarify the subjectivity of the given values, which was addressed by registering notes to the self-assessment question in a specific field.

The Self-Assessment System supports the process of increasing top management commitment and awareness to secure the necessary investment to start up and establish a BCMS that is appropriate for the organization. The session introduced questions about the Self-Assessment System to evaluate these artifact components. Participants could have suggested significant improvements or flaws in the system. As a result, the Self-Assessment System provides the essential information to guide the organization in determining where resources will be required (prioritizing resource allocation) and in adopting strategies that best adapt to its organizational capacity.

Moreover, the session provided an opportunity to evaluate key components of the Self-Assessment System, allowing participants to identify areas for improvement and suggest potential refinements to enhance usability.

8. Conclusions

Organizations seek assistance in the design and/or implementation of a BCP and/or BCM, which conveys the assurance that they are prepared to respond effectively and efficiently to business interruption. The established BCP should enable the formulation of response, recovery, resumption, and restoration of business processes, supported by ICT, at a predefined level of operability, based on the organization's capacity.

While the FAMMO^{CN} framework demonstrably improves BCP readiness (evidenced by 100% validation in organizational interviews), its true innovation lies in bridging the gap between theoretical BCM standards and practical implementation. Unlike generic frameworks, FAMMO^{CN}'s tiered maturity metrics—validated across 10 diverse organizations—provide actionable thresholds for resource allocation, addressing a critical pain point identified in the literature: the lack of measurable progression pathways for SMEs [9].

The research project put forth and subsequently established a Self-assessment Methodology designed to aid in the preparation and implementation of a BCP in organizations, taking into account their respective size and capability [44]. This Self-assessment System proposes a relevant evaluation of organizational preparedness within the BC domain, serving as a strategic guide for developing and analyzing critical components and procedures needed for successful BCP design and implementation, with particular emphasis on ICT systems.

By utilizing the DSR methodology, the Self-assessment Methodology and system were developed and subsequently presented to BC experts and individuals responsible for ICT within organizations. This enabled its demonstration and evaluation [44].

The BCM Model determines the components and activities that underpin a BCMS. It suggested the path the organization can follow to establish or improve organizational processes that may result in an adequate response, recovery, resumption, and restoration of business processes. We developed self-assessment questions for each critical activity that

establish goals to achieve and are of additional value for increasing the multidisciplinary preparedness of the organization's continuity response.

In the planning phase and to capture a broad vision, the organization can self-assess its preparation for BC. A self-assessment can help an organization identify gaps and weaknesses in its BCMS and provide an opportunity to improve its preparedness for business continuity events. By conducting a self-assessment, an organization can identify areas where it needs to focus its efforts to improve its BCM program. The organization can discover gaps in achieving each activity's objectives and raising awareness. The Self-assessment Methodology and System can track the progress of BC awareness and the requirement for enhanced discipline in processes that assure the organization's BCM system management. This information will be utilized to define strategic guidelines for implementing a BCP.

The iterative self-assessment process revealed an unanticipated insight: 60% of participating organizations underestimated their exposure to supply-chain risks until engaging with FAMMO^{CN}'s cross-functional metrics. This underscores the framework's unique capacity to surface latent vulnerabilities by enforcing multidisciplinary alignment—a finding that challenges assumptions in the prior literature about siloed risk awareness [83].

This enables the model to guide the organization to understand the path toward engaging in organizational process improvement, which may result in an acceptable response, recovery, resumption, and restoration of business processes in an incident or disaster. Essential activities are considered in each component at this stage, reporting their compliance through written questions in a simplified and straightforward manner.

The Self-assessment Methodology and System allow benchmarking and perception of the organization's current state of BC preparedness. Benchmarking between organizations is a way to obtain recognition for compliance, enhance the adoption of the framework, and implement BC solutions.

This paper overviews several frameworks, standards, and best practices related to business continuity, IT service management, and process improvement. It approaches how these frameworks and standards can help organizations assess their BCMS performance and continuously improve their processes and services. It also emphasizes the importance of self-assessment at all levels of the organization to achieve business results.

Three key lessons emerged from this research: (1) Framework adoption correlates more strongly with executive-level visualization tools (e.g., the FAMMO^{CN} scorecard) than with compliance mandates; (2) ICT teams served as unexpected change agents for BCM adoption, indicating untapped potential for bottom-up implementation strategies; and (3) the "priority" attribute reduced metric overload but required trade-offs in sector-specific customization—a tension needing further study.

While the proposed Self-Assessment System does not seek to claim superiority over existing BCM assessment methods, it introduces a distinct and complementary approach grounded in multidisciplinary integration, quantitative scoring, and broad adaptability. Developed in response to gaps identified through a prior systematic literature review, this methodology aims to unify fragmented practices by offering a universal tool that is both standards-aligned and scalable across organizational sizes and sectors. Its primary value lies in its practical applicability, ease of adoption, and potential to foster continuous improvement in BCM maturity through structured, repeatable evaluations.

As limitations to this work, the presented Self-Assessment System fits perfectly with the FAMMO^{CN} framework. However, in order to be used with other frameworks, further research may be needed. Other limitations, for example, methodological, may include the study's reliance on semi-structured interviews and Focus Groups; while providing rich qualitative insights, this may introduce subjectivity in interpreting self-assessment

scores. Future research could benefit from triangulating these findings with quantitative data or external audits to strengthen validity. A sampling limitation is that the evaluation primarily involved medium-sized and large organizations, with limited representation from micro-enterprises or highly regulated sectors (e.g., healthcare). That may affect the generalizability of findings across all organizational scales and industries. As an analytical limitation, the scoring mechanism weighting system, though empirically derived from SLR and expert input, may not equally suit all organizational contexts. For instance, SMEs with resource constraints might prioritize different BCM components than large enterprises.

While acknowledging these limitations, we plan in future work to address these issues since we developed the Self-Assessment Methodology with the aim of being universal and adaptable to any BC framework.

To broaden its applicability, future iterations of the methodology should aim to test its integration with alternative frameworks beyond FAMMO^{CN}, such as COBIT, CMMI or sector-specific standards in healthcare or finance. This would help validate its adaptability and reveal any constraints in aligning its scoring mechanism with different organizational logics.

These future directions could explore how the Self-Assessment System contributes to sustained improvements in BCM practices. Longitudinal studies may help evaluate whether improvements in BCM scores correlate with actual reductions in business disruptions or enhanced resilience during crises.

Moreover, while the Self-Assessment System was empirically validated through focus groups and interviews, further large-scale quantitative evaluations are necessary to generalize its effectiveness across diverse organizational contexts. Such studies could integrate external audits or independent assessments to triangulate the self-reported scores and mitigate subjectivity inherent in qualitative feedback.

Although full longitudinal case studies were not conducted in this initial research phase, early application in a real organizational context, as presented in Section 7.3, complemented by feedback from multiple participants, has already demonstrated the method's relevance, usability, and potential for impact. Future work will focus on supporting wider implementation across different sectors to further validate and refine the model in diverse real-world environments. For future work and to enhance interaction between participants in the Self-Assessment System, it is of the utmost relevance to developing a mobile/web application. Next, further development of the Measurement System will be a part of our plans.

Author Contributions: Conceptualization, N.R., H.S.M. and L.R.; methodology, N.R., H.S.M. and L.R.; software, N.R.; validation, N.R., H.S.M. and L.R.; formal analysis, N.R.; investigation, N.R.; resources, N.R., H.S.M. and L.R.; data curation, N.R.; writing—original draft preparation, N.R.; writing—review and editing, N.R., H.S.M. and L.R.; visualization, N.R.; supervision, H.S.M. and L.R.; project administration, N.R., H.S.M. and L.R.; funding acquisition, H.S.M. All authors have read and agreed to the published version of the manuscript.

Funding: This work is financed by National Funds through the Portuguese funding agency, FCT—Fundação para a Ciência e a Tecnologia, within project LA/P/0063/2020. https://doi.org/10.54499/LA/P/0063/2020.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

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

Abbreviations

The following abbreviations are used in this manuscript:

BC	Business Continuity
BCM	Business Continuity Management
BCMS	Business Continuity Management System
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CMMI	Capability Maturity Model Integration
COBIT	Control Objectives for Information and Related Technology
CR-SAT	Cyber Resilience Self-Assessment Tool
FAMMO^{CN}	Framework for the Multidisciplinary Assessment of Organizational Maturity on Business Continuity Management
DSR	Design Science Research
ICT	Information and Communication Technologies
IS	Information Systems
ITIL	Information Technology Infrastructure Library
KPI	Key Performance Indicators
PDCA	Plan-Do-Check-Act
SLR	Systematic Literature Review

References

1. BCI. The Role of ICT in Ensuring Business Continuity. 22 July 2024. Available online: https://www.thebci.org/news/the-role-of-ict-in-ensuring-business-continuity.html (accessed on 12 February 2025).
2. Katsaliaki, K.; Galetsi, P.; Kumar, S. Supply chain disruptions and resilience: A major review and future research agenda. *Ann. Oper. Res.* **2022**, *319*, 965–1002. [CrossRef] [PubMed]
3. Ramakrishnan, R.K.; Viswanathan, S. The importance of Business Strategy in Business Continuity Planing. In *The Definitive Handbook of Business Continuity Management*, 3rd ed.; John Wiley & Sons, Ltd.: West Sussex, UK, 2011.
4. Syed, A.; Syed, A. *Business Continuity Planning Methodology*; Sentryx: Austerlitz, The Netherlands, 2004.
5. Cerullo, V.; Cerullo, M.J. Business Continuity Planning: A Comprehensive Approach. *J. Inf. Syst. Manag.* **2004**, *21*, 70–78. [CrossRef]
6. Winkler, U.; Fritzsche, M.; Gilani, W.; Marshall, A. A Model-Driven Framework for Process-centric Business Continuity Management. In Proceedings of the 2010 Seventh International Conference on the Quality of Information and Communications Technology, Porto Portugal, 29 September–2 October 2010.
7. Järveläinen, J. IT incidents and business impacts: Validating a framework for continuity management in information systems. *Int. J. Inf. Manag.* **2013**, *33*, 583–590. [CrossRef]
8. Torabi, S.A.; Soufi, H.R.; Sahebjamnia, N. A new framework for business impact analysis in business continuity management (with a case study). *Saf. Sci.* **2014**, *68*, 309–323. [CrossRef]
9. Torabi, S.A.; Giahi, R.; Sahebjamnia, N. An enhanced risk assessment framework for business continuity management systems. *Saf. Sci.* **2016**, *89*, 201–218. [CrossRef]
10. Soufi, H.R.; Torabi, S.A.; Sahebjamnia, N. Developing a novel quantitative framework for business continuity planning. *Int. J. Prod. Res.* **2019**, *57*, 779–800. [CrossRef]
11. Gracey, A. Building an organisational resilience maturity framework. *J. Bus. Contin. Emerg. Plan.* **2019**, *13*, 313–327. [CrossRef]
12. Carías, J.F.; Arrizabalaga, S.; Labaka, L.; Hernantes, J. Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs. *IEEE Access* **2021**, *9*, 80741–80762. [CrossRef]
13. Monev, V. The "Self-Assessment Method" within a Mature Third-Party Risk Management Process in the Context of Information Security. In Proceedings of the 2021 International Conference on Information Technologies (InfoTech), Varna, Bulgaria, 16–17 September 2021; pp. 1–7.
14. *NFPA 1600*; NFPA 1600® Standard on Continuity, Emergency, and Crisis Management. National Fire Protection Association: Quincy, MA, USA, 2019.
15. FFIEC. *Business Continuity Management, USA: Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook*; FFIEC: Washington, DC, USA, 2019.
16. Kato, M.; Charoenrat, T. Business continuity management of small and medium sized enterprises: Evidence from Thailand. *Int. J. Disaster Risk Reduct.* **2018**, *27*, 577–587. [CrossRef]

17. Russo, N.; Reis, L.; Silveira, C.; Mamede, H.S. Framework for designing Business Continuity—Multidisciplinary Evaluation of Organizational Maturity. In Proceedings of the 6th Iberian Conference on Information Systems and Technologies (CISTI), Chaves, Portugal, 23–26 June 2021.
18. Botha, J.; von Solms, R. A cyclic approach to business continuity planning. *Inf. Manag. Comput. Secur.* **2004**, *12*, 328–337. [CrossRef]
19. Tjoa, S.; Jakoubi, S.; Quirchmayr, G. Enhancing Business Impact Analysis and Risk Assessment Applying a Risk-Aware Business Process Modeling and Simulation Methodology. In Proceedings of the 2008 Third International Conference on Availability, Reliability and Security, Barcelona, Spain, 4–7 March 2008.
20. Valackienė, A.; Žostautienė, D. Changes Management as the Presumption for Business Continuity. *Changes Soc. Bus. Environ.* **2013**, 207–212.
21. Iovan, S.; Ivanus, C. Disaster Recovery and Business Continuity. *Ann. Constantin Brancusi Univ. Targu-Jiu. Econ. Ser.* **2013**, *4*, 153–158.
22. Sterling, S. Encouraging resilience within SMEs: The Cabinet Office's proposed approach. *J. Bus. Contin. Emerg. Plan.* **2011**, *5*, 128–139. [CrossRef]
23. Arduini, F.; Morabito, V. Business continuity and the banking industry. *Commun. ACM* **2010**, *53*, 121–125. [CrossRef]
24. Benyoucef, M.; Forzley, S. Business Continuity Planning and Supply Chain Management. *Supply Chain Forum Int. J.* **2007**, *8*, 14–22. [CrossRef]
25. Shaw, G.; Harrald, J. The core competencies required of executive level business crisis and continuity managers—The results. *J. Homel. Secur. Emerg. Manag.* **2006**, *3*, 1–34. [CrossRef]
26. Brás, J.; Guerreiro, S. Designing Business Continuity Processes Using DEMO: An Insurance Company Case Study. In *Enterprise and Organizational Modeling and Simulation*; EOMAS 2016. Lecture Notes in Business Information Processing; Pergl, R., Molhanec, M., Babkin, E., Fosso Wamba, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2016; Volume 272.
27. Pramudya, G.; Fajar, A. Business continuity plan using ISO 22301:2012 in IT solution company (pt. ABC). *Int. J. Mech. Eng. Technol.* **2019**, *10*, 865–872.
28. Fani, S.V.; Subriadi, A.P. Business Continuity Plan: Examining of Multi-Usable Framework. *Procedia Comput. Sci.* **2019**, *161*, 275–282. [CrossRef]
29. Herbane, B.; Elliott, D.; Swartz, M. Business Continuity Management: Time for a strategic role? *Long Range Plan.* **2004**, *37*, 435–457. [CrossRef]
30. Putra, E.P.P.; Nazief, B.A.A. Analysis of Main Cause Factors and Improvement Recommendation of IT Disaster Recovery Problems: A Case Study of XYZ Organization. *AIP Conf. Proc.* **2018**, *1977*, 020024.
31. Burtles, J. Manager's Guide to Business Continuity Exercises: Testing Your Plan. In *Rothstein Publishing eBook Collection*; Rothstein Publishing: Brookfield, CT, USA, 2016.
32. Păunescu, C. How Prepared are Small and Medium Sized Companies for Business Continuity Management? *Qual.-Access Success* **2017**, *18*, 43–48.
33. Veerasamy, N.; Mashiane, T.; Pillay, K. Contextualising cybersecurity readiness in South Africa. In Proceedings of the 14th International Conference on Cyber Warfare and Security, Stellenbosch, South Africa, 28 February–1 March 2019.
34. Ohlhausen, P.E.; McGarvey, D. The use of metrics to manage enterprise security risks: Understanding, evaluation and persuasion. *J. Bus. Contin. Emerg. Plan.* **2018**, *12*, 6–16. [CrossRef]
35. Moody, G.D.; Siponen, M.; Pahnila, S. Toward a Unified Model of Information Security Policy Compliance. *MIS Q.* **2018**, *42*, 285–312. [CrossRef]
36. Hiles, A. *Business Continuity Management: Global Best Practices*; Rothstein Publishing: Brookfiel, CT, USA, 2014.
37. *ISO 22301*; Societal Security—Business Continuity Management Systems—Requirements. ISO: Geneve, Switzerland, 2019.
38. *ISO/IEC 27031*; Information Technology—Security Techniques—Guidelines for Information and Communication Technology Readiness for Business Continuity. ISO/IEC: Geneve, Switzerland, 2011.
39. *ISO 22300*; Security and Resilience—Vocabulary. ISO: Geneve, Switzerland, 2021.
40. Fernando, M.S. IT disaster recovery system to ensure the business continuity of an organization. In Proceedings of the 2017 National Information Technology Conference (NITC), Colombo, Sri Lanka, 14–15 September 2017.
41. Vasquez, E.J.; Ortega, J.C. Design of a business contingency plan. Case study: Municipality of Cantón Suscal. In Proceedings of the 2020 International Conference on Intelligent Systems and Computer Vision (ISCV), Fez, Morocco, 9–11 June 2020.
42. Brás, J. Bootstrapping Enterprise Models with Business Continuity Processes and DEMO. 2018. Available online: https://recil.ulusofona.pt/items/ca18f831-c912-45e8-9e3e-dcae13b1bb42 (accessed on 12 February 2025).
43. Aronis, S.; Stratopoulos, G. Implementing business continuity management systems and sharing best practices at a European bank. *J. Bus. Contin. Emerg. Plan.* **2016**, *9*, 203–217. [CrossRef]
44. Russo, N.; Mamede, H.S.; Reis, L.; Silveira, C. FAMMO^{CN}—Demonstration and evaluation of a framework for the multidisciplinary assessment of organisational maturity on business continuity. *Heliyon* **2022**, *8*, e10566. [CrossRef]

45. Russo, N.; Reis, L.; Silveira, C.; Mamede, H.S. Towards a Comprehensive Framework for the Multidisciplinary Evaluation of Organizational Maturity on Business Continuity Program Management: A Systematic Literature Review. *Inf. Secur. J. A Glob. Perspect.* **2023**, *33*, 54–72. [CrossRef]
46. CMMI Institute. *CMMI Model V2.0*; CMMI Institute: Pittsburgh, PA, USA, 2018.
47. ITIL. *ITIL Foundation ITIL 4 Edition*; AXELOS: London, UK, 2019.
48. ISACA. *COBIT 2019 Framework—Governance, Management Objectives*; ISACA: Schaumburg, IL, USA, 2018.
49. NIST. *NIST Special Publication 800-34 Rev. 1—Contingency Planning Guide for Federal Information Systems*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2010.
50. Marshall, M. How to develop a risk assessment programme for your vendor's BCP capabilities and their impact on your organisation. *J. Bus. Contin. Emerg. Plan.* **2007**, *1*, 340–347. [CrossRef]
51. Trousdale, L. Using self-assessments to enhance business continuity programmes. *J. Bus. Contin. Emerg. Plan.* **2015**, *9*, 6–9. [CrossRef]
52. Tomsic, H. Auditing emergency management programmes: Measuring leading indicators of programme performance. *J. Bus. Contin. Emerg. Plan.* **2016**, *10*, 57–75. [CrossRef]
53. Iqbal Widyawan, A.; Mustika, I.W. COBIT 5 domain delivery, service and support mapping for business continuity plan. *AIP Conf. Proc.* **2016**, *1746*, 020045.
54. Vaidyanathan, K. Post-event reviews: Using a quantitative approach for analysing incident response to demonstrate the value of business continuity programmes and increase planning efficiency. *J. Bus. Contin. Emerg. Plan.* **2017**, *11*, 107–116. [CrossRef]
55. Harding, M. Moving your business continuity management programme forward with recoverability measurement. *J. Bus. Contin. Emerg. Plan.* **2018**, *12*, 113–118. [CrossRef]
56. Ricks, M.; Boswell, L. Assessing the resilience of an IT portfolio. *J. Bus. Contin. Emerg. Plan.* **2019**, *13*, 22–31. [CrossRef]
57. Bajgorić, N.; Turulja, L.; Ibrahimović, S.; Alagić, A. *Enhancing Business Continuity and IT Capability: System Administration and Server Operating Platforms*; CRC Press: Boca Raton, FL, USA, 2020.
58. Gallagher, M. Business Continuity Management—Do you measure up? *Account. Irel.* **2003**, *35*, 15–16.
59. Gardner, B. An Exploratory Qualitative Inquiry of Key Indicators on IT Disaster Recovery Planning. Ph.D. Thesis, Capella University, Minneapolis, MN, USA, 2016.
60. Ream, S.; Mathew, S. A metrics framework to get and keep management engaged. *J. Bus. Contin. Emerg. Plan.* **2018**, *11*, 298–308. [CrossRef]
61. Zeng, Z.; Zio, E. An integrated modeling framework for quantitative business continuity assessment. *Process Saf. Environ. Prot. Trans. Inst. Chem. Eng. Part B* **2017**, *106*, 76–88. [CrossRef]
62. Olson, A.; Anderson, J. Resiliency scoring for business continuity plans. *J. Bus. Contin. Emerg. Plan.* **2016**, *10*, 31–43. [CrossRef]
63. Stourac, T. Wheels, hubs and spokes: Incorporating a scorecard into a business continuity programme. *J. Bus. Contin. Emerg. Plan.* **2014**, *7*, 260–269. [CrossRef]
64. Russo, N.; Mamede, H.S.; Reis, L.; Martins, J.; Branco, F. Exploring a Multidisciplinary Assessment of Organisational Maturity in Business Continuity: A Perspective and Future Research Outlook. *Appl. Sci.* **2023**, *13*, 11846. [CrossRef]
65. Peffers, K.; Tuunanen, T.; Rothenberger, M.A.; Chatterjee, S. A Design Science Research Methodology for Information Systems Research. *J. Manag. Inf. Syst.* **2007**, *24*, 45–77. [CrossRef]
66. Hevner, A.R.; March, S.T.; Park, J.; Ram, S. Design Science in Information Systems Research. *Manag. Inf. Syst. Q.* **2004**, *28*, 75–105. [CrossRef]
67. Ferreira, I.; Ferreira, S.; Silva, C.; Carvalho, J. Dilemas iniciais na investigação em TSI. In Proceedings of the Atas da Conferencia Ibérica de Sistemas y Tecnologias de Informacíon (7ª CISTI), Madrid, Spain, 20–23 June 2012.
68. Hiles, A. *Business Continuity: Best Practices: World-Class Business Continuity Management*; Rothstein Associates Inc.: Brookfield, CT, USA, 2004.
69. Russo, N.; Reis, L. Chapter 10—Methodological Approach to Systematization of Business Continuity in Organizations. In *Handbook of Research on Multidisciplinary Approaches to Entrepreneurship, Innovation, and ICTs*; IGI Global: Hershey, PA, USA, 2020; pp. 200–223.
70. Clarke, V.; Braun, V. Thematic analysis. *J. Posit. Psychol.* **2016**, *12*, 297–298. [CrossRef]
71. Wong, W.N.Z. The strategic skills of business continuity managers: Putting business continuity management into corporate long-term planning. *J. Bus. Contin. Emerg. Plan.* **2009**, *4*, 62–68. [CrossRef]
72. Russo, N.; Reis, L. Updated analysis of business continuity issues underlying the certification of invoicing software, considering a pandemic scenario. *Adv. Sci. Technol. Eng. Syst. J.* **2020**, *5*, 845–852. [CrossRef]
73. Bethany, M.P. *Business Continuity Planning: Identifying Gaps, Patterns and Justifications*; California State University: Long Beach, CA, USA, 2014.
74. Gallo, U.E. *Implementación de un Sistema Integrado de Gestión Basado en los Estándares ISO 27001, ISO 31000 e ISO 22301 en la Empresa Paris & Asociados, S.A.C*; Universidad Nacional Mayor de San Marcos: Lima, Perú, 2021.

75. Sahebjamnia, N.; Torabi, S.A.; Mansouri, S.A. Integrated business continuity and disaster recovery planning: Towards organizational resilience. *Eur. J. Oper. Res.* **2015**, *242*, 261–273. [CrossRef]
76. Hamid, A.H.A. Limitations and challenges towards an effective business continuity management in Nuklear Malaysia. In Proceedings of the IOP Conference Series: Materials Science and Engineering, Xi'an, China, 24–26 June 2018.
77. Green, C. Measuring business continuity programmes in large organisations. *J. Bus. Contin. Emerg. Plan.* **2014**, *8*, 71–82. [CrossRef]
78. Ford, M.W.; Evans, J.R. Models for organizational self-assessment. Business horizons. *Bus. Horiz.* **2002**, *45*, 25–32. [CrossRef]
79. Pinto, D.; Fernandes, A.; da Silva, M.; Pereira, R. Maturity models for business continuity–A systematic literature review. *Int. J. Saf. Secur. Eng.* **2022**, *12*, 123–136. [CrossRef]
80. Fani, S.V.; Subiadi, A.P. Trend of Business Continuity Plan: A Systematic Literature Review. In Proceedings of the 1st International Conference on Business, Law And Pedagogy, ICBLP 2019, Sidoarjo, Indonesia, 13–15 February 2019.
81. Ostadi, B.; Ebrahimi-Sadrabadi, M.; Sepehri, M.M.; Kashan, A.H. A Systematic Literature Review of Organization Resilience, Business Continuity, and Risk: Towards Process Resilience and Continuity. *Interdiscip. J. Manag. Studies* **2023**, *16*, 229–257.
82. Tremblay, M.C.; Hevner, A.R.; Berndt, D.J.; Chatterjee, S. The use of focus groups in design science research. *Des. Res. Inf. Syst.* **2010**, *22*, 121–143.
83. Revilla, E.; Saenz, M.J. The impact of risk management on the frequency of supply chain disruptions: A configurational approach. *Int. J. Oper. Prod. Manag.* **2017**, *37*, 557–576. [CrossRef]