DOI: 10.2507/35th.daaam.proceedings.xxx

BUSINESS CONTINUITY PLANNING (BCP) AND DISASTER RECOVERY PLANNING (DRP)

Katja Mikulic Premuzic, Vedran Dakic*, Robert Petrunic

This Publication has to be referred as: Mikulic Premuzic, K[atja]; Dakic, V[edran] & Petrunic, R[obert] (2024). Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP), Proceedings of the 35th DAAAM International Symposium, pp.xxxx-xxxx, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-xx-x, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/35th.daaam.proceedings.xxx

Abstract

This paper explores the critical aspects of Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP), highlighting their essential role in ensuring organisational resilience. It defines Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP), emphasising their importance in addressing various operational risks. The paper then systematically explores the processes of risk assessments and business impact analyses, showing how these tools are essential in identifying and avoiding potential disruptions. The paper examines real-world case studies, which provide practical insights into successful and failed implementations of BCP and DRP strategies. These case studies are essential in drawing lessons on proactive measures and typical disaster planning and recovery challenges. The paper also discusses testing methodologies vital for the effectiveness of BCP and DRP, emphasising the need for regular plan updates and exercises. The final part brings together these discoveries, proposing possible paths for further study and progress in BCP and DRP, especially as technology keeps changing and risks evolve.

Keywords: Business Continuity Planning; Disaster Recovery Planning; Risk Assessment; Business Impact Analysis; Organizational Resilience.

1. Introduction

In today's volatile environment, Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) are essential for maintaining operations and ensuring rapid recovery in the face of disruptions. This paper investigates the strategic planning, risk assessments, impact analyses, and testing methodologies that underpin BCP and DRP. A review of the literature and case studies assesses the effectiveness of these frameworks in actual disaster scenarios, identifies prevalent shortcomings in their implementation, such as outdated systems and insufficient testing, and explores innovative solutions.

The insights gained reveal the factors crucial for the success or failure of BCP and DRP initiatives and suggest that ongoing innovation in these strategies is necessary due to the rapid changes in technology and global business conditions.

This paper aims to provide a comprehensive understanding of BCP and DRP as vital tools for navigating the complexities of modern business environments, emphasising the need for continuous adaptation and improvement.

2. Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) Strategies

Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) are essential for organisational resilience and sustainability in today's business environment. As natural disasters, technological errors, and other disruptions become more frequent and unpredictable, these frameworks have transitioned from optional to critical corporate governance and risk management components. BCP ensures the continuation or quick resumption of crucial business functions, encompassing operational aspects, employee safety, data management, and customer relations. Its goal is to maintain smooth operational continuity during and after crises. Meanwhile, DRP focuses on restoring IT systems and data, which is crucial for operational functionality post-disaster. The importance of BCP and DRP in maintaining organisational resilience and mitigating financial losses during disruptions cannot be overstated. Security Information and Event Management (SIEM) systems are crucial in the realm of Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP), ensuring robust cybersecurity. These systems are central to collecting, normalising, and analysing extensive security data from various network components [6]. The primary function of SIEM systems is to enhance organisational capacity to promptly detect and address potential security threats, thereby bolstering the overall strategy for cybersecurity. Integrating both security information management (SIM) and security event management (SEM), SIEM systems not only manage security data but also facilitate real-time analysis and threat detection [6].

This integration is vital in BCP and DRP, as it ensures that organisations can maintain continuous oversight and quick response capabilities, which is crucial for minimising downtime and protecting critical infrastructure during and after an incident. Critical infrastructure encompasses various technological systems essential for meeting societal needs. These systems are composed of both control systems and systems that are controlled and integral to company processes, social systems (including humans, organisational structures, assets, values, and knowledge), and technological systems (comprising tools, equipment, procedures, and technologies) [7]. As multistage systems, they facilitate bidirectional flows of materials, finances, information, and decisions. Consequently, it is crucial to analyse these systems from the perspective of interactions and interdependencies among their technical, human, social, and organisational components [7]. This analysis includes the consideration of human survival, which can be either active or passive. Passive survival capacity is embedded within the system properties, based on knowledge of environmental defects, depicted through causal chains. On the other hand, active survival is demonstrated by the system's behaviour, considering the uncertainty in forecasting future defects and failures [7].

These strategies help sustain operations and protect the company's reputation by maintaining customer trust during crises. Additionally, they are vital for complying with industry regulations, especially in the finance and healthcare sectors, where data protection and service availability are heavily regulated. An example of a Business Continuity Management plan can be seen in the following figure:

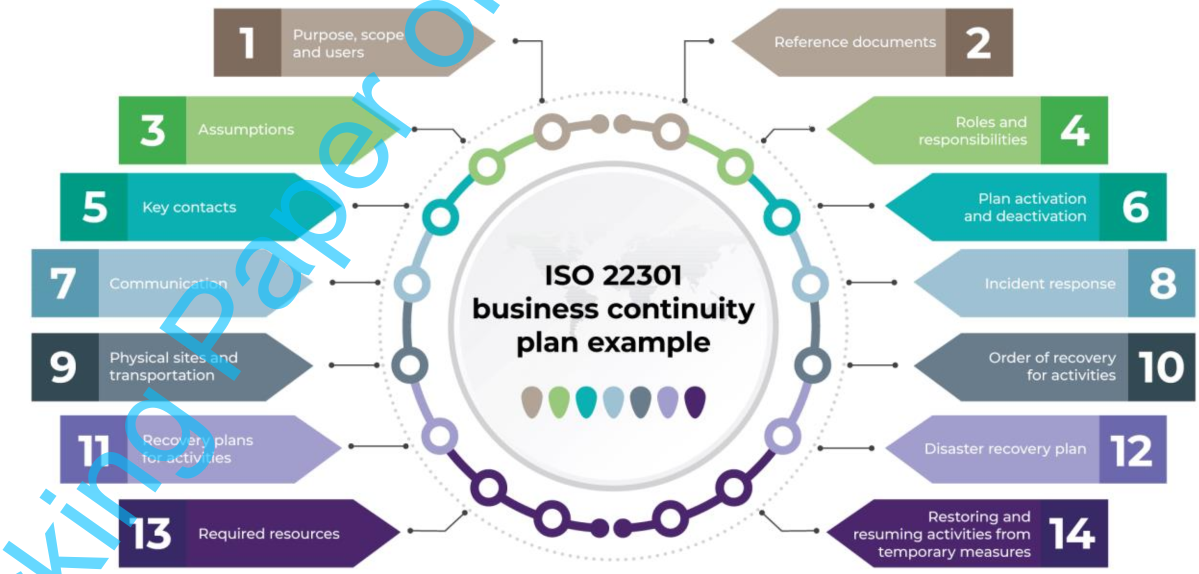
1 Purpose, scope and users
2 Reference documents
3 Assumptions
4 Roles and responsibilities
5 Key contacts
6 Plan activation and deactivation
7 Communication
8 Incident response
9 Physical sites and transportation
10 Order of recovery for activities
11 Recovery plans for activities
12 Disaster recovery plan
13 Required resources
14 Restoring and resuming activities from temporary measures
ISO 22301 business continuity plan example

Fig. 1. ISO 22301 business continuity management plan, https://advisera.com/27001academy/knowledgebase/business-continuity-plan-how-to-structure-it-according-to-iso-22301/, accessed on 2024-05-05.

The ongoing complexity of IT infrastructures, including the rise of cloud computing and big data, has made DRP even more significant. It must evolve to address new technological challenges and opportunities. Real-world case studies demonstrate the consequences of inadequate disaster planning and the benefits of robust BCP and DRP. These examples provide crucial lessons in risk assessment and proactive strategy formulation, emphasising the need for continuous adaptation to the dynamic business and technological landscape.

3. Risk Assessments in Business Continuity Planning

Risk assessments are crucial in Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP), serving as the foundation for developing robust strategies to enhance business resilience against disruptions. This process entails qualitative and quantitative methods to identify, evaluate, and prioritise potential risks, thereby shaping effective continuity and recovery strategies.

3.1. Iidentifying Potential Risks

The process starts by identifying risks that could affect business operations, which include natural disasters, technological failures, cybersecurity threats, and human errors. Risk identification involves analysing potential hazards from various sources, such as historical data, industry reports, and expert opinions. For example, a business in a hurricane-prone area would prioritise this as a significant risk, while a tech-heavy company might focus on cybersecurity threats. Small and medium-sized enterprises (SMEs) must incorporate resilience into their strategic frameworks to address the complexities associated with disaster recovery and business continuity. The implementation of resilience, as explored in [8], entails a strategic management approach to risk factors, enhancing SMEs' capabilities to manage and mitigate risks effectively. This approach includes applying the Delphi technique for iterative feedback and consensus in risk prioritisation, essential for maintaining operational continuity and minimising disruptions in dynamic market conditions [8].

3.2. Qualitative and Quantitative Risk Assessments

Qualitative assessments involve a subjective risk probability and impact analysis, utilising tools like risk matrices and registers to categorise and prioritise risks. This approach is suited for risks that are challenging to measure numerically, such as reputational damage or employee morale [10]. Conversely, quantitative risk assessments use numerical data to estimate risk probability and impact, providing a more objective basis for decision-making. This method is precious for financial risk assessments, where potential losses can be estimated in monetary terms, aiding financial planning and regulatory compliance [10]. Both types of risk assessments are vital for BCP. They allow organisations to understand the risk landscape thoroughly and allocate resources effectively to safeguard critical business functions. Qualitative assessments contribute to a broad understanding of risks and help engage stakeholders and prepare for less quantifiable events [10]. Quantitative assessments provide the precision for developing detailed recovery strategies and financial preparations, such as determining investments in backup systems or insurance. Together, these assessments form the bedrock of a proactive and resilient BCP and DRP strategy [10].

4. Impact Analyses in Business Continuity Planning

The Business Impact Analysis (BIA) identifies, quantifies, and qualitatively assesses the impacts of a loss, interruption, or disruption of business processes on an organisation. It furnishes the necessary data to determine suitable continuity strategies [13]. The most crucial steps in the BIA process are as follows: (1) Identify the management owners and business activities; (2) Select the right personnel to obtain information as efficiently as possible; (3) Identify scenarios that could seriously harm the company's assets, reputation, or financial situation; and (4) Determine the window of time during which interruptions to business operations are unacceptable [13]. Various information-gathering methods, including workshops, questionnaires, and interviews, may be used, depending on the company under analysis. The maximum tolerable period of disruption (MTPD) and the recovery point objectives (RPO) are the two primary deliverables of the BIA for every business activity. This analysis extends beyond simple risk assessment by projecting the potential real-world impacts on organisational functionality. The BIA process is initiated by cataloguing key business processes and assessing their vulnerability to disruptions across various dimensions, such as financial damage, regulatory issues, customer relations, and potential long-term strategic challenges.

4.1. Conducting a Business Impact Analysis

The BIA involves detailed steps, from thoroughly reviewing organisational operations to identifying critical functions and understanding the interdependencies among business units and external entities. It evaluates the potential immediate, intermediate, and long-term impacts of various disruption scenarios like natural disasters, technological failures, or cyberattacks. In cloud computing, assessing and mitigating risks necessitate a structured approach, as illustrated in [12]. Their model incorporates a multi-level grading system that evaluates business continuity risks across several dimensions, including business operations, security levels, system lifecycle, and economic factors. This method ensures that the disaster recovery capabilities are appropriately aligned with the specific needs and vulnerabilities of the cloud environment, thereby enhancing the resilience and responsiveness of the business systems involved [12]. This evaluation guides the prioritisation of recovery efforts to restore essential operations rapidly.

Resource identification for recovery and establishing Recovery Time Objectives (RTO) for each business function is also integral to the BIA. RTOs dictate the maximum tolerable downtime, which is crucial for developing targeted recovery strategies and managing recovery expectations.

4.2. *Significance of Business Impact Analysis*

BIA offers multiple benefits by enabling efficient resource allocation and enhancing the precision of recovery strategies, thereby minimising downtime and accelerating recovery. It provides critical information that improves transparency with stakeholders, employees, customers, investors, and regulators, helping manage expectations and sustain trust during disruptions. Moreover, BIA ensures adherence to regulatory standards and informs decision-making processes in BCP, grounding them in a detailed understanding of potential impacts rather than mere speculation.

In conclusion, BIA is essential for crafting effective Business Continuity Plans. It provides a detailed overview of how disruptions affect business operations, allowing organisations to make informed recovery priorities and resource distribution decisions. This process supports the continuity of operations and facilitates strategic planning and stakeholder management. Regular updates to BIA are necessary to keep pace with changing business landscapes and risk profiles, ensuring that continuity plans remain relevant and robust.

5. Testing Methodologies in Business Continuity and Disaster Recovery Planning

Testing methodologies ensure that Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) are theoretically sound and practically practical during actual disasters. Regular updates and consistent practice of these plans are critical to adapt to the changing risk environment. Testing in BCP and DRP involves a detailed evaluation of recovery plans to confirm their effectiveness and pinpoint areas needing enhancement. This process often includes various exercises and simulations that check each part of the plan, from communication protocols to technical recovery solutions, aiming to meet Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). In formulating and testing Business Continuity and Disaster Recovery Plans, it is essential to integrate cybersecurity measures comprehensively. As highlighted in [9], ensuring the security and continuity of business operations, especially in environments with high criticality and availability, is highly important. Integrating cybersecurity throughout the business continuity planning and disaster recovery process helps manage cyber threats and ensures a resilient infrastructure capable of smooth transition and recovery from cyber incidents [9].

Due to the evolving nature of threats and technology, updating and testing BCP and DRP regularly is necessary. Changes in technology, business processes, or regulations could make older plans ineffective. Regular testing helps spot these inefficiencies and allows staff to be trained and familiarised with their roles in disaster scenarios, reducing response times and potential confusion during actual events. In addition to traditional testing methodologies, implementing simulation games has proven effective in enhancing the cybersecurity training aspect of business continuity and disaster recovery plans. As noted in [11], simulation games provide a dynamic platform for personnel to develop critical decision-making and crisis management skills in a controlled yet realistic environment [11]. This method prepares individuals to handle real-world cybersecurity threats and incidents efficiently, ensuring they can maintain operational integrity under adverse conditions [11]. Some key testing processes in BCP and DRP involve:

- Tabletop exercises are discussion-based sessions where team members work through the plan in a simulated disaster scenario. They are critical for assessing the plan’s comprehensiveness and training staff on their responsibilities.
- Technical recovery tests: These involve recovering systems and data from backups to check that they can be restored quickly and efficiently, ensuring the integrity and functionality of backup systems.
- Full-scale drills: These extensive exercises mimic a natural disaster as closely as possible, testing the organisation's ability to implement the recovery plan under realistic conditions, often including mobilising resources and personnel.
- Communication tests evaluate the effectiveness of communication channels and protocols, which are crucial during a disaster for maintaining timely and accurate information flow.
- Business process tests assess the ability to sustain or swiftly resume essential business processes during and after a disruption.

Let’s now see what these processes will bring to our company and why they are essential to reducing risk.

5.1. *TThe Impact of Simulations and Drills*

Simulations and drills play a pivotal role in validating the efficacy of BCP and DRP. They provide numerous benefits:

- Simulations offer a realistic environment to assess the plan's performance, clearly indicating its functionality in a disaster.
- Drills act as practical training sessions for staff, ensuring they understand and can effectively execute their roles under pressure.
- These exercises are essential for identifying weaknesses in the plan related to resources, procedures, or technical capabilities.
- Conducting regular drills can significantly enhance response times, which is crucial for reducing the impact of a disaster.
- Successful simulations and drills boost confidence among all stakeholders—employees, customers, and investors—about the organisation's resilience capabilities.

Testing methodologies form an integral part of the success of BCP and DRP, ensuring that the plans are viable on paper and effective in real scenarios. Regularly updating and practising these plans through tabletop exercises, recovery tests, full-scale drills, communication tests, and business process assessments are vital for maintaining their effectiveness. Such activities are crucial for staff training, spotting plan deficiencies, and enhancing the organisation's resilience in the face of potential disasters.

6. Integration of Case Studies in Business Continuity Planning and Disaster Recovery Planning

The integration of real-life scenarios in Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) is essential for understanding and enhancing the efficacy of these strategies. Learning from case studies provides invaluable insights into the practical application, challenges, and outcomes of BCP and DRP in real-world situations. These studies serve as a compass, guiding organisations in crafting theoretically sound plans and pragmatically viable plans that are tested against the nuances of real-life disasters and disruptions.

The examination of case studies, such as those presented in [1], [2], [3], [4], and [5], highlights the many aspects of disaster recovery and business continuity. These studies show how organisations have succeeded and failed when faced with unexpected problems, such as natural disasters, technology breakdowns, and cyberattacks.

- FAA System Failure [1]: This case study highlights the repercussions of relying on outdated systems, emphasising the need for modernisation and regular updates in BCP and DRP. The incident underscores the importance of having contingency plans for legacy systems and ensuring high availability in critical infrastructure.
- Microsoft Azure/Office Outage [1]: This global disruption showcases the vulnerabilities in cloud-based systems and the need for robust, multi-regional strategies. It stresses the significance of having diversified disaster recovery options, especially for organisations relying heavily on cloud services.
- OVHcloud Data Centre Fire [1]: This event illustrates the catastrophic impact of physical disasters on data centres. It reinforces the 3-2-1 rule of data backup and the importance of off-site backups in safeguarding data against natural calamities.
- NHS Ransomware Attack [1]: This case study demonstrates the devastating effects of cyberattacks on public health infrastructure. It highlights the need for rigorous cybersecurity measures and the importance of quick response mechanisms in BCP and DRP to mitigate the impact of such attacks.
- Houston Wire and Cable's BCDR Success [5]: This example shows the efficacy of a well-implemented BCDR solution, enabling the organisation to maintain operations during extreme weather. The success story emphasises the value of cloud technology and proactive planning in ensuring business continuity amidst natural disasters.

These are just some of the studies we should consider when doing our BCP and DRP, as they're valuable learning resources.

6.1. Successful Recoveries

Examining instances where organisations effectively navigated crises using their Business Continuity and Disaster Recovery Plans (BCP and DRP) provides invaluable insights into the essence of resilient planning. Case studies like those in [2], [4], and [5] exemplify successful recoveries. Houston Wire and Cable's Approach [5]: In the face of an unexpected snowstorm, Houston Wire and Cable demonstrated the robustness of their BCDR solution. They maintained operations despite widespread power outages using Azure cloud technology and proactive planning. The key to their success was the swift transition to a reliable backup system and their readiness for natural disasters, showcasing the importance of cloud-based solutions and the necessity of agility in response strategies.

Total Tool's Data Centre Crisis [4]: This case study highlights the importance of having an off-site data centre. When Total Tool faced a robbery that jeopardised their primary data centre, their disaster recovery plan involving an off-site data centre allowed for seamless business operations, illustrating the significance of having a robust, multi-location data storage and recovery strategy.

6.2. *Lessons from Failed Plans*

In contrast, analysing where BCP and DRP have failed offers critical lessons in the pitfalls of disaster recovery planning. Case studies like [1] and [3] reveal common shortcomings. FAA System Failure [1]: This instance underscores the perils of depending on outdated systems. The failure of the FAA's NOTAM system due to a simple error like a deleted file highlights the need for modern, resilient systems and the importance of regular system updates and backups. NHS Ransomware Attack [3]: This case illustrates the devastating impact of cyberattacks. The NHS's vulnerability to ransomware exposed the lack of adequate cybersecurity measures and swift response mechanisms. This case emphasises the importance of robust security protocols and contingency planning for cyber threats.

6.3. *Synthesis of Learnings*

These case studies offer important lessons. Success in disaster recovery depends on taking proactive steps, like using modern technology and storing data off-site. On the other hand, failures often result from old systems, weak security, and slow response plans. These lessons highlight the need for organisations to stay flexible, regularly update their BCP and DRP with the latest technology, and focus on strong security. Testing and updating these plans periodically are crucial to ensure they remain effective. Analysing these case studies gives us a clear picture of what makes a good BCP and DRP. Preparing for potential issues and adapting to unexpected situations are keys to successful disaster recovery. Failures remind us of the dangers of not planning well. These findings are essential for organisations creating or improving their BCP and DRP. Plans should consider successful and unsuccessful recoveries to build resilience and maintain business continuity in various disruptions.

7. Future Works

Further research could focus on integrating emerging technologies such as artificial intelligence, machine learning, and blockchain in BCP and DRP systems. Investigating their potential to automate risk assessments, predict potential disruptions, and optimise recovery processes could yield significant advancements in this field. Additionally, studies could explore the ethical and practical implications of automating decision-making processes in disaster recovery scenarios, ensuring that these technological solutions do not inadvertently increase organisational risk or create new vulnerabilities.

8. Conclusion

This paper has thoroughly explored Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP), emphasising their indispensable roles in maintaining organisational resilience. The findings reveal that BCP and DRP are dynamic processes requiring ongoing updates and refinements to address evolving risks effectively. Integrating comprehensive risk assessments and detailed business impact analyses is vital for detecting vulnerabilities and formulating effective mitigation strategies. The real-world case studies presented here illustrate both successful implementations and notable failures, underlining the importance of proactive and adaptable strategies for disaster management. These narratives demonstrate the critical need for preparedness and the ability to respond flexibly to unexpected challenges, providing essential lessons for enhancing future strategy. Moreover, this paper underscores that BCP and DRP extend beyond mere disaster survival; they leverage insights from past experiences to thrive in a post-disaster environment. With risks ranging from cyber threats to natural disasters, a forward-thinking approach that anticipates and adapts to change is crucial.

In conclusion, the paper advocates for a proactive, iterative approach to BCP and DRP. Organisations should consider these plans as living documents, continually refined to align with the latest threats and technological changes. By fostering a culture of resilience and staying responsive to the changing world, organisations can prepare themselves to withstand future disruptions and emerge from them stronger and more resilient. This approach is not just about survival; it's about positioning for future success in an unpredictable world.

9. References

[1] https://www.techtarget.com/searchdisasterrecovery/tip/Real-life-business-continuity-failures-Examples-to-study, (2023). Real-life business continuity failures: 4 examples to study, Accessed on: 2024-01-15

[2] https://invenioit.com/continuity/4-real-life-business-continuity-examples/, (2022). 7 Real-Life Business Continuity Examples You'll Want to Read, Accessed on: 2024-01-15

[3] https://square3it.com/real-life-examples-of-business-continuity-plans-that-failed/, (2019). Real-Life Examples Of Business Continuity Plans That Failed, Accessed on: 2024-01-15

[4] https://www.loffler.com/blog/disaster-recovery-case-study-insights, (2022). Insights from Our Business Continuity & Disaster Recovery Case Study, Accessed on: 2024-01-15

[5] https://www.softwareone.com/en/case-studies/global/manufacturing/hwc-business-continuity-and-disaster-recovery-on-azure, (2024). Circuitry with the best shield, Accessed on: 2024-01-15

[6] Suskalo, D.; Moric, Z.; Redzepagic, J. & Regvart, D. (2023). Comparative Analysis of IBM Qradar and Wazuh for Security Information and Event Management, Proceedings of the 34th International DAAAM Symposium 2023 (pp.0096-0102), Published by DAAAM International, ISBN 978-3-902734-41-9, ISSN 1726-9679, Vienna, Austria. DOI: 10.2507/34th.daaam.proceedings.014, in press.

[7] Procházková, D.; Prochazka, J.; Rusko, M.; Mikulova, M. & Ilko, J. (2017). Model for Critical Infrastructure Safety Management, Proceedings of the 28th International DAAAM Symposium 2017 (pp.0602-0610), Published by DAAAM International, ISBN 978-3-902734-11-2, ISSN 1726-9679, Vienna, Austria. DOI: 10.2507/28th.daaam.proceedings.085, in press.

[8] Grujic, J. (2019). Concept of Resilience Implementation in Small and Medium Sized Enterprises (SMEs), Proceedings of the 30th DAAAM International Symposium, Published by DAAAM International, ISBN 978-3-902734-22-8, ISSN 1726-9679, Vienna, Austria. DOI: 10.2507/30th.daaam.proceedings.116, in press.

[9] Altaha, S. & Rahman, M. M. (2023). A Mini Literature Review on Integrating Cybersecurity for Business Continuity, Proceedings of the 2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Published by IEEE, ISBN 978-1-6654-5645-6, Al Hofuf, Al Hassa, Saudi Arabia. DOI: 10.1109/ICAIIC57133.2023.10067127, in press.

[10] Hewitt, J. & Pham, J. (2018). Qualitative Versus Quantitative Methods in Safety Risk Management, Proceedings of the 2018 Annual Reliability and Maintainability Symposium (RAMS), Published by IEEE, ISBN 978-1-5386-2870-6, Reno, USA. DOI: 10.1109/RAM.2018.8463052, in press.

[11] Lang-Muhr, C.; Tjoa, S.; Machherndl, S. & Haslinger, D. (2022). Business Continuity & Disaster Recovery A simulation game for holistic cyber security education, Proceedings of the 2022 IEEE Global Engineering Education Conference (EDUCON), Published by IEEE, ISBN 978-1-6654-4434-7, ISSN 2165-9567, Tunis, Tunisia. DOI: 10.1109/EDUCON52537.2022.9766714, in press.

[12] Zhang, L.; Fang, X.; Chen, Y.; Song, Y. & Qian, S. (2021). Research on business continuity rating model in cloud environment, Proceedings of the 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Published by IEEE, ISBN 978-1-7281-8028-1, ISSN 2689-6621, Chongqing, China. DOI: 10.1109/IAEAC50856.2021.9390871, in press.

[13] Tjoa, S.; Jakoubi, S. & Quirchmayr, G. (2008). Enhancing Business Impact Analysis and Risk Assessment Applying a Risk-Aware Business Process Modeling and Simulation Methodology, Proceedings of the 2008 Third International Conference on Availability, Reliability and Security, Published by IEEE, ISBN 978-0-7695-3102-1, Barcelona, Spain. DOI: 10.1109/ARES.2008.206