BLACK CELL
Protecting critical infrastructures

Business continuity management projects case study

TLP:CLEAR

Table of Contents

TLP:CLEAR

1. Introduction

This case study illustrates the lessons learned from reviewing and designing business continuity management systems in recent times. The projects have been conducted or are currently underway in various organizations across different sectors and sizes, including Critical Infrastructure, Defence, Manufacturing, Service, and Product Reseller sectors. Experiences are not attributed to specific organizations and mentioning them does not enable identification of the organizations involved. The case study highlights the challenges and difficulties in this domain, thereby assisting organizations facing similar issues in managing their business continuity functions.

2. Target group

The target audience of this case study includes all organizations required by law or standards to establish and maintain a business continuity system, as well as those organizations that recognize the importance of safeguarding their operations against the impact of adverse events.

3. Facts and background information

Any organization, whether operating for the betterment of society or for profit, recognizes the significance of business continuity. Many organizations are legally obligated comply with regulations such as The Network and Information Systems Directive-2 (NIS2), while compliance with various standards such as ISO/IEC 27001:2022 and ISO 22301:2019 necessitates ensuring business or service continuity. Consequently, different methodologies are available for constructing or auditing a business continuity system.

Irrespective of the methodology chosen, there exists a general process for establishing business continuity systems. It is imperative to understand the activities of the organization and the processes that underpin them for each business continuity system. Having this information readily available is a critical success factor for conducting business impact analysis (BIA), which involves identifying operational limitations, known vulnerabilities, and risks associated with each process. Once the Business Impact Analysis is completed, it becomes feasible to pinpoint which impacts or risks necessitate the development of Business Continuity Plans (BCPs), as well as to recognize the risks to the IT and other infrastructure supporting those processes, enabling the formulation of Disaster Recovery Plans (DRPs). Following the establishment of these plans, they must undergo education and testing, with subsequent adjustments made to address any deficiencies or inefficiencies. In essence, this process forms the foundation of standards and recommendations in this field.

4. Analysis and Methodology

The case study is crafted to analyse the experiences acquired during the construction or evaluation of business continuity systems. The methodology aligns with this objective by outlining the challenges and pitfalls encountered, aiming to equip other organizations with insights into the potential obstacles they might encounter when undertaking similar projects.

5. Experiences

5.1. Incorrect process definition

In some cases, organizations lack process descriptions or documentation outlining their operational procedures and responsibilities, making it challenging to conduct an accurate business impact analysis. Organizations with an Organizational and Operational Charter (OOR) find it easier to identify processes, as this document delineates departmental roles and responsibilities in detail. However, in the absence of such documentation, organizations struggle to precisely define the processes constituting their business and supporting activities.

Consequently, identifying processes becomes a complex and difficult task. Managers may not be able to provide a comprehensive list of activities during interviews, leading to incomplete information. Some departments or managers may focus too much on detail, resulting in a mixture of main and sub-processes. Discrepancies in process identification can lead to varying numbers of processes identified across departments, with some departments listing core processes while others list numerous supporting activities. In such scenarios, it becomes necessary to define the main processes, albeit at the expense of project duration.

It is crucial to identify recurring or key business activities, such as production, sales, and customer service processes, to ensure project success. While challenging, having a clear understanding of processes is essential for facilitating subsequent project activities. Without it, project progress becomes significantly hindered.

5.2. Incident-generated need for business continuity in the absence of preconditions

In many organizations, incidents prompt the necessity of establishing a business continuity system, yet essential prerequisites are often lacking. Following an incident, senior management may demand the implementation of business continuity measures, but many critical components are absent in such cases. For instance, there might be no Information Security Policy in place to address various business continuity concerns. Procedures such as backups, Information Security Awareness training, or the identification, analysis, assessment, and mitigation of risks might be lacking.

Additionally, there may be no designated Business Continuity Manager to oversee the necessary tasks, and there could be a deficiency in the requisite knowledge to operate a business continuity system effectively.

In such circumstances, it becomes exceedingly challenging to focus on the task at hand due to constant barriers faced by the individual tasked with implementing the project. Additional resources are often necessary because of the lack of prerequisites, and work cannot commence until these conditions are fulfilled. In such a scenario, it is advisable to commence with an audit to identify gaps in the existing infrastructure, followed by efforts to address these gaps and prioritize the establishment of business continuity measures.

Moreover, it is recommended to provide training courses for personnel assigned to the task, enabling them to acquire the knowledge essential for operating the business continuity system effectively. By addressing these prerequisites and investing in training, organizations can better prepare themselves to navigate and mitigate the impacts of future incidents.

5.3. Business impact analysis carried out by IT

In certain organizations, the business impact analysis is conducted not by the business area but by individuals responsible for project implementation or by IT operations. This approach is flawed as it tends to prioritize the IT perspective in task execution, despite numerous instances demonstrating that the business area often holds a distinct viewpoint on the significance of certain information systems. Consequently, delegating the project solely to IT represents a misguided decision. This can lead to conflicts, as the business area must make decisions on substitute or alternative solutions based on information provided by IT and adapt to Recovery Point Objective (RPO) values set by IT. Such an approach does not align with supporting the business; rather, it places IT in a dominant position when, ideally, IT should serve the business.

This misalignment has indirect implications for maximizing profits in for-profit organizations and for the efficient performance of activities mandated by governmental or public bodies. It is imperative to recognize that different departments must collaborate to achieve project objectives. Therefore, it is advisable to prepare the organization before project implementation, ensuring that all stakeholders are involved and providing training to delineate responsibilities for each activity and how they should be carried out. This approach fosters a more cohesive and effective execution of business continuity initiatives, ultimately benefiting the organization as a whole.

5.4. MTD, RTO, RPO value determination problem

Defining MTDs (Maximum Tolerable Downtime), RTOs (Recovery Time Objectives), and RPOs (Recovery Point Objectives) often poses a common challenge. Even with prior

training aimed at ensuring that the business and/or IT area comprehends the significance of these values, they may still struggle to define them accurately. Merely providing examples to illustrate the importance of these values and their concepts is often insufficient for a complete understanding.

In some cases, the responsible individuals for the process may avoid taking ownership of defining these values, citing an inability to do so. However, what's crucial is for the department to grasp the potential consequences of process failure. Collaboration with other departments, such as finance, can also be beneficial. For instance, the finance department may be able to quantify the loss associated with a failed process, aiding in the determination of MTDs, RTOs, and RPOs.

This challenge underscores the importance of interdepartmental cooperation in resolving such issues. Additionally, it's not uncommon for the relative importance of these values to be inconsistent with reality. For example, having an MTD value higher than the RTO value presents a contradiction. Therefore, it is advisable to educate individuals involved in the development of the BCMS (Business Continuity Management System) before the project commences, allowing them the opportunity to ask questions and gain a clear understanding of the values' significance and interpretation. This proactive approach can help to alleviate misunderstandings and ensure a more effective implementation of the business continuity plan.

5.5. Missing information asset inventory

Unfortunately, many organizations often lack awareness of their informational assets, creating challenges in accurately identifying what the organization requires for its operations within a given process. This deficiency is widespread, and even when an inventory of informational assets exists, it is frequently outdated and incomplete, lacking all the elements necessary for establishing business continuity.

In numerous cases, contracts play a crucial role for organizations, especially due to Service Level Agreements (SLAs) aimed at ensuring that a process meets its Recovery Time Objective (RTO). However, certain elements may be overlooked in planning due to the absence of support tools. For instance, internet connectivity is frequently omitted from the list of assets, potentially compromising redundancy for activities heavily reliant on the internet.

Another issue lies in determining informational assets, as many organizations typically only include hardware and software elements, despite the broader scope of informational assets. Human resources, documents, equipment, applications, software, hardware, backups, base configurations and any other elements essential for a process to function can be considered informational assets. By conducting a comprehensive assessment of what is necessary for a process to function, these assets become visible.

Having an up-to-date list of informational assets enables the efficient execution of business continuity management tasks. Therefore, organizations should prioritize maintaining such a list to ensure effective continuity planning and management.

5.6. Strong IT dependency, no alternative process

When the criticality of a process is established and the risk values are deemed high, as determined in the business impact analysis, it's common for the business area to struggle in finding alternative solutions to cope with system outages. The level of dependency on IT in organizational processes often leads to a scenario where IT is expected to solve all problems. Consequently, when IT systems fail, the business area may come to a standstill because it cannot operate without them.

However, with a more thorough examination of the process, it's possible to identify alternative solutions that can function even when IT systems are down, presuming that IT can restore the information systems. To illustrate, for tasks involving data that is not live but stored within the system (at rest), accessing backups or utilizing offline data can enable the completion of tasks.

In today's rapidly evolving technological landscape, this principle extends beyond business continuity and permeates almost every field. Taking the time to analyse processes and explore available opportunities is crucial. Many information systems possess capabilities that are underutilized, and often organizations are unaware of their full potential. It's beneficial to map out these capabilities and maintain an updated list of available system functionalities. This proactive approach increases the likelihood of finding solutions to system failures by leveraging the functionalities of other systems in the organization.

5.7. The consulting firm cannot write the plans

In some projects, organizations may mistakenly believe that consulting firms will handle every aspect, creating and overseeing every plan from start to finish. However, this is a misconception. While consulting firms' experts can certainly assist in building business continuity systems, they cannot execute all tasks independently. Active involvement from the organization is essential because they possess the most intimate knowledge of the organization and its unique processes.

During such projects, consulting experts provide valuable insights, but they may not necessarily offer alternative solutions or technical steps required for restoring individually built architectures and systems during Disaster Recovery Plan (DRP) construction. Every network and system operate differently, making it unrealistic to expect a one-size-fits-all approach.

While consulting experts can and should be utilized in these projects, organizations must understand that their engagement requires adequate allocation of resources for

task execution. Collaboration between the consulting firm and the organization is vital for the success of the project, with each party bringing its unique expertise to the table.

5.8. There is no one to manage BCMS

The lack of dedicated management for business continuity is a common issue once a business continuity framework has been successfully established. Organizations often struggle with the absence of a designated person responsible for overseeing tasks such as implementation of training, testing, review, and development of the Business Continuity Management System (BCMS). The role of a Business Continuity Manager is frequently compromised or left unfilled, especially in larger organizations where the position may be linked with other responsibilities.

This problem is even more pronounced in smaller organizations, where there may be insufficient human and other resources to address business continuity effectively. Unfortunately, since the performance of these tasks doesn't yield immediate, tangible results on a day-to-day basis, they often receive inadequate attention from senior managers.

However, it's crucial to recognize that in addition to handling specific periodic tasks, ongoing improvement, and development of the business continuity system is vital for timely preparation against new threats and negative events. While business continuity is indeed a part of information security, it constitutes a separate discipline with its own set of requirements and considerations.

Effecting change in this area requires effective communication to management regarding the importance and distinctiveness of business continuity. Often, in the business world, other priorities may take precedence over business continuity, making it challenging to secure proper management attention and resources for this area. Nevertheless, it's imperative to advocate for the recognition and prioritization of business continuity within organizations to ensure resilience and readiness in the face of unforeseen events.

5.9. Business impact analysis is not an audit

When an organization engages with a consultancy service for assistance in building a business continuity system, it is sometimes perceived as an audit by the organization's staff. This perception can hinder efficient collaboration, as staff may withhold important information necessary for ensuring completeness. Unfortunately, staff members often view the consultancy's involvement in the process as akin to an audit, leading them to withhold information or provide responses they believe the "auditor" wants to hear.

Dispelling this belief can be challenging, but it's essential to make staff aware that the purpose of consulting and participating in work processes is to help the organization identify and address non-compliances. Before embarking on any such project, it is

advisable to educate all parties involved and clarify that they are not participating in an audit. In the long run, this approach will enable organizations to better handle both expected and unexpected events by fostering a culture of transparency and collaboration.

5.10. Key employees who fear for their position

Especially in smaller organizations, and occasionally in larger ones as well, there may be individuals who possess crucial knowledge for ensuring business continuity. However, due to concerns about their position or other reasons, they may not provide the necessary quantity and quality of information during reviews or when building the business continuity system. These concerns can arise from various factors, which this case study does not delve into. Nevertheless, it's important to be aware in advance if such individuals are among the stakeholders, as deeper investigation may be required to obtain the required level of information.

In many cases, an audit may indeed be necessary to uncover the reality and gain clarity on all aspects of a situation. Therefore, it's worth considering this factor during project preparations. Additionally, there are key employees who juggle multiple tasks simultaneously, holding multiple roles as a single individual. Their roles are also crucial for business continuity, as they are usually a long-standing personnel within the organization. Therefore, it is essential to implement recommendations such as job rotation and other best practices to prevent such situations.

5.11. Undocumented incidents

The lack of documentation of past events, such as incidents or security events is a recurring issue, that often arises. The absence of historical documentation limits the possibility of conducting quantitative risk analysis while assessing business impacts, leaving only qualitative analysis as a methodological option. Consequently, the analysis of impacts becomes more subjective, and risk analysis based on estimation may not accurately reflect real scenarios, potentially distorting the assessment of actual impacts.

While there are situations where analysis based on historical data is not feasible due to the absence of prior incidents or similar situations, documenting past events can provide a more accurate understanding of the real impact of negative events. Therefore, it is crucial to collect incidents, document them with sufficient detail, and utilize this data and information during the analysis of business impacts.

By incorporating documented incidents into the analysis process, preparation becomes more straightforward, preparatory efforts will be simplified, uncertainty arising from estimation can be reduced, and organisations can obtain a more realistic assessment of potential impacts when developing and reviewing business continuity measures.

5.12. Inadequate testing efforts

Organizations either do not conduct testing of completed plans at all, or they partially or not at all execute them due to the time-consuming preparations involved. Testing a Business Continuity Plan (BCP) and/or a Disaster Recovery Plan (DRP) requires careful planning if an organization intends to carry it out comprehensively. It should not impede the execution of daily tasks or the core business.

The lack of a testing environment is also a common problem within this area. Even if all resources are available, the actual practical testing often falls short, and organizations only go through the plans within the framework of Tabletop Exercises (TTX), which can be useful but may not fully reveal the errors or inadequacies that need to be addressed.

It is advisable to consider planning for BCP and DRP testing during the development of annual work plans, with coordination preferably conducted by the Business Continuity Manager. Investing time and other resources into planned testing upfront is more likely to yield results than conducting a test that has not been properly prepared for.

6. Results and lessons learned

The outcome of this case study can be summarized in the difficulty of building a business continuity system under optimal conditions. Often, the prerequisites necessary for fully planning, executing, testing, and improving such a system are missing. Small and medium-sized organizations often face different challenges than large corporations, but common points can still be found. In the case of large corporations, resources are generally available, but they may encounter other problems such as determining MTD, RTO, RPO values or dealing with key employees who fear for their positions.

As a lesson learned, it is advisable to commence every business continuity construction project with an audit, where an examination is conducted to determine if the necessary conditions are in place. The audit will reveal any deficiencies such as missing policies, an inventory of informational assets, or other resources and conditions. Once these deficiencies are addressed and remediated, it would be timely to launch such a project.

Before starting the project, it is recommended to involve all relevant stakeholders in the project and provide them with training to ensure understanding of the various processes involved, what needs to be done, who needs to do it, whom to collaborate with, and to avoid confusion caused by unfamiliar terms.

It is essential to have a dedicated individual, preferably in an independent position, whose responsibility is managing business continuity, coordinating necessary tasks, possessing appropriate professional expertise, and ideally having experience in the

field of business continuity. With such a person in place, the implementation of testing and other tasks can proceed smoothly and in a planned manner.