Working Papers

ISSN 2219-780X

3
MARCH
2024

Business Continuity Plan: Increasing Importance for Tax Administrations

CENTRO INTERAMERICANO DE ADMINISTRACIONES TRIBUTARIAS
CIAT
FUNDADO 1967

Antonio Seco
Wolney Martins
Gilberto Netto

Business Continuity Plan: Increasing Importance for Tax Administrations

Antonio Seco
Wolney Martins
Gilberto Netto

Serie: *Working Papers*
ISSN 2219-780X

Business Continuity Plan:
Increasing Importance for Tax Administrations

WP-03-2024

Antonio Seco

Wolney Martins

Gilberto Netto

Diagramming: CIAT Communication and Publications Coordination

Content

List of Acronyms

BCM	Business Continuity Management
BCMS	Business Continuity Management System
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BPP	Business Priority Processes (IRS)
CIAT	Centro Interamericano de Administraciones Tributarias
COBIT	Control Objectives for Information and Related Technology
CRA	Canada Revenue Agency
ESA	Essential Supporting Activities (IRS)
IOTA	Intra-European Organisation of Tax Administrations
IRS	Internal Revenue Service (USA)
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
MEF	Mission Essential Functions (IRS)
OCP	Operational Continuity Plan
OECD	Organization for Economic Collaboration and Development
PwC	Price, Waterhouse & Coopers (Consulting and Audit)
RTO	Recovery Time Objective
SEFAZ-MA	Secretaria de Estado de Fazenda do Estado do Maranhão (Brazil)
SUNAT	Superintendencia Nacional de Administración Tributaria (Peru)
TADAT	Tax Administration Diagnostic Assessment Tool

Executive Summary

Business continuity helps organizations maintain resilience and respond quickly to disruptions, allowing them to continue working at a minimal level during disruptive events.

The recent crisis caused by the COVID-19 pandemic has highlighted the importance of having a continuity plan and has reminded us of the need for a long-term approach to this strategic element. Crises can affect the continuity of administrative processes, both manual and computerized, and can range from climate events/natural phenomena to cyber-attacks, geopolitical conflicts, regulatory changes, and social crises.

Tax administrations are vital organizations for a country and are not exempt from these types of disturbances; therefore, they must improve their resilience and aim to safeguard their activities as a strategic need. However, to date, of the 92 assessments conducted by the Tax Administration Diagnostic Assessment Tool (TADAT), most low- and middle-income countries did not have a robust business continuity plan (BCP).

Thus, there arises an imperative need to have a BCP specifically designed for tax administrations and their inherent complexities.

A BCP describes the procedures and instructions that the organization must follow during disruptive events to minimize downtime; this includes organizational processes, assets, human resources, and stakeholders that are external to the institution.

To develop a BCP, it is not necessary to reinvent the wheel. There are documented experiences and a set of international standards and good practices that can guide the process.

Usually, it is recommended to follow the Plan-Do-Check-Act (PDCA) cycle in four stages to implement a BCP: understanding the organization, determining strategies, developing and implementing responses, and testing, maintaining, and reviewing. Each of these stages has its own activities that are essential for the success of the plan, framed by including the culture of business continuity in the organization. Some examples of topics covered in these stages are risk analysis, business impact analysis, and recovery time objectives.

This general context must be adapted to each tax administration, since they rely on different conditions, such as the degree of digitalization of services, availability of remote work, outsourcing agreements, and the scope of action.

Senior management involvement and internal audits are also key elements to the success of a BCP.

1 Introduction

On the threshold of the 21st century, the world finds itself at technological and administrative crossroads. This is especially true in the field of tax administrations, considering that these entities not only manage a large amount of critical and sensitive data for governments and taxpayers, but also play a pivotal role in the economy and functioning of societies.

The unprecedented advances in information technology (IT) have transformed the way these organizations operate. Their key processes are heavily dependent on information, and so the methods and techniques to continuously access, process, and distribute this information have become a top priority. We can also highlight growing internal and external threats that affect the continuity of manual and computerized administrative processes – ranging from climatic events/natural phenomena to cyber-attacks, geopolitical conflicts, regulatory changes, and social crises.

Paraphrasing Harari[1], in general, organizations can be considered products of collective inventions created by humanity. To not fall into this category, an organization must be completely automated, including its external relations. Such invention can be examined from different perspectives. Most of the major approaches can be conducted through collaborative efforts among the various organizational stakeholders.

The business continuity of a conventional organization, after an event that alters its normal operations, has everything to do with the collaboration between stakeholders. The very idea of normal operations depends on the aforementioned collaboration. There are very few activities that work regardless of collaboration among people; in these extreme cases, it is not necessary to speak of "organization." There is no organization that is functional without collaboration among people.

[1] Yuval Noah Harari, History professor and author of books

The discussion on continuity is an opportunity to equalize knowledge and understanding fundamental to collaboration. Regardless of the conclusions and results that emerge from such discussions, these activities allow everyone to share and update knowledge about the organization in terms of the situation, challenges, risks, strategies, priorities, etc. Collective discussion can help in selecting and implementing preventive measures, which precede take place before planning continuity actions.

Over the years, organizations have acquired facilities and resources to minimize disruption, adjusting overhead, and increasing the proportion of fixed costs. This approach can be classified as technical or technological, generally associated with the use of redundant and fault-tolerant solutions, in addition to the search for economies of scale. However, it is also necessary to consider the social aspects, i.e., behaviors and procedures. Continuity challenges require a combination of both types of solutions.

Though it may seem obvious, it is important to highlight that the decision and execution of expenses to satisfy the operational and continuity needs of the organization must be aimed at resources directly related to adding value and generating results.

As shown in this text, the development of continuity plans can – and should – use widely tested and validated methods and models. Risk analysis is a step that occurs in all references, usually by assessing the probability of occurrence and prioritizing based on the effects that each type of downtime can cause.

Risk analysis must avoid short-term biases. Risk analyses carried out in recent years may have overestimated the risk of pandemics and other health incidents. In other words, risks can be strongly influenced by recent events.

For example, there are many situations in which access to the organization’s physical facilities may be disrupted: health incidents, force majeure events (floods, property damage, etc.), transportation and public service outages, etc. Some possible causes can be mitigated with preventive actions, e.g., installing an electrical generator to deal with power outages. For other types of disturbances, it is recommended to group them according to their effects and then deal with continuity, e.g., taking measures to address circumstances that make it impossible to access the organization’s facilities, regardless of the events that made it so. It should be noted that the growing automation of tax processes and experiences with the expansion of remote work, also driven by the recent COVID-19 outbreak, can facilitate contingency decisions in cases of inability to access workplaces.

According to PwC's 2023 Global Crisis and Resilience Survey[2], 96% of 1,812 business leaders said their organizations had experienced disruption in the past two years, and 76% said the most severe disruption had a medium to high impact on their business operations. Because of the negative impacts, 89% of executives include resilience as one of their top strategic priorities. However, only 70% of respondents expressed confidence in their organizations' current ability to address disruptions.

Tax administrations are not exempt from these possible disturbances and, therefore, must increase their resilience, addressing threats to the continuity of their activities as a strategic need.

Potential Threats to the Operational Continuity of Tax Administrations – Overview and Examples:

1. Cyberattacks and Data Security: Protecting tax information systems against cyberattacks (malware, ransomware, phishing, online activism, etc.) and ensuring the integrity and confidentiality of tax data.

2. Hardware and Software Downtime: Preparing for downtime in critical equipment and tax management software, including backup and recovery plans.

3. Network and Connectivity Downtime: Guaranteeing continuity of services in case of connectivity downtime, whether internal or with internet providers.

4. Recovery from Natural Disasters/Climate Events: Planning responses to and recovery from natural disasters that may affect physical computing infrastructure.

5. System Overload During Critical Periods: Managing high demand during key periods, such as tax filing deadlines.

6. Regulatory Compliance and Legislative Changes: Quickly adapting to changes in tax legislation and ensuring regulatory compliance in computer systems.

7. Personnel Continuity Management: Ensuring availability of trained personnel during emergencies and developing succession and training plans.

8. Protection against Data Loss: Implementing robust data backup and recovery solutions to prevent loss of critical information.

[2] See **https://www.pwc.com/gx/en/issues/crisis-solutions/global-crisis-survey.html**

Potential Threats to the Operational Continuity of Tax Administrations – Overview and Examples:

9. Power Outages: Preparing for power outages and having backup solutions, such as generators or UPS systems.

10. Human Mistakes: Minimizing the risk of human mistakes that may cause downtime or data loss and offering proper training.

11. Systems Scalability and Upgrade Issues: Maintaining the systems' ability to adapt to growing workloads and managing upgrades without interrupting services.

12. Internal Threats: Preventing and detecting malicious actions by employees that may compromise the security or operation of the systems.

13. Social Crises: Planning how to mitigate service outages derived from strikes that are internal and external to the tax administration.

14. Poor Management of Suppliers and Third Parties: ensuring continuity and reliability of services provided by third parties, – including administrative services, software, hardware, and cloud services.

This highlights the imperative need for a business continuity plan (BCP) specifically designed for tax administrations and their inherent complexities. A BCP is a strategic manual created to help an organization maintain or quickly resume business functionality in the face of downtime. This plan is the main component of a business continuity management system (BCMS).

A BCP describes the procedures and instructions that the organization must follow during disruptive events in order to minimize downtime, and covers organizational processes, assets, human resources, and stakeholders external to the institution.

To develop a BCP, it is not necessary to reinvent the wheel. There are documented experiences and a set of international standards and good practices that can guide the process, such as:

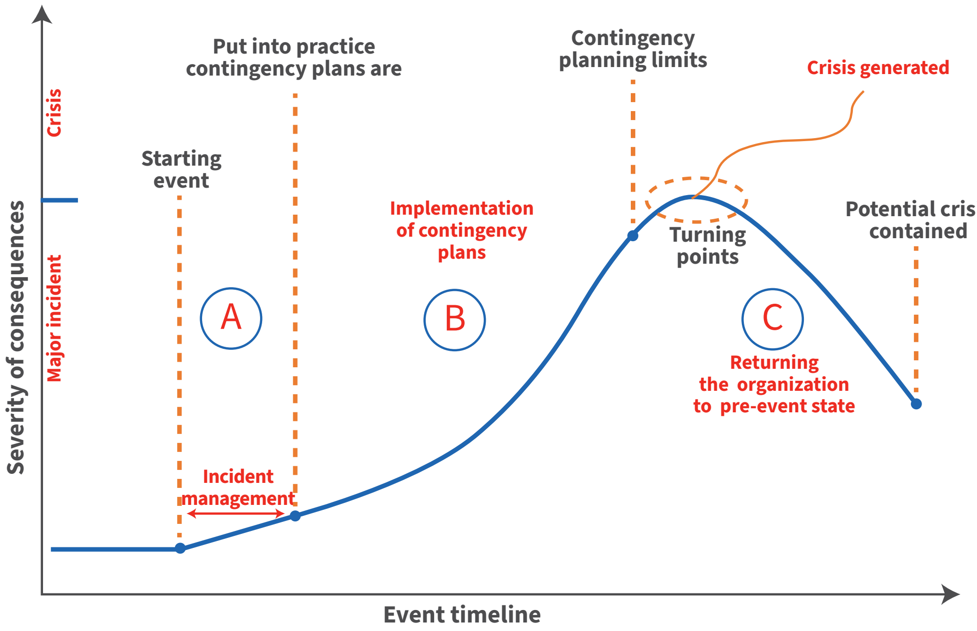
- ISO 22301:2019 (Security and Resilience - Business Continuity Management System – Requirements.
- ISO 22313:2020 – Security and Resilience – Business Continuity Management System – Guidance on the Use of ISO 22301.
- Technical Specification ISO/TS 22317:2021 – Security and Resilience – Business Continuity Management System – Guidelines for Business Impact Analysis (BIA).
- IT service management frameworks, such as ITIL and COBIT (risk and continuity segments).

2 Genesis of a Crisis

Figure 1 below describes the chronology of transformation from a normal situation to an incident, which, if not contained, can reach a serious level, and requires the application of contingency plans to avoid a crisis.

An incident is an unexpected episode or accidental circumstance that changes the normal course of action. This is a common occurrence in the day-to-day business of institutions, and they have their own processes to correct it ("A"). However, if such processes are inadequate, it would be necessary to implement contingency plans ("B"). Normally, contingency plans are sufficient to halt serious incidents, returning the organization to its state prior to the initial event ("C").

FIGURE 1: Chronology and Criticality of the Consequences of an Incident.



Source: Adapted from Smith and Elliot (2006).

Major disruptions arise when an event escalates, generating circumstances that have not been considered by those responsible for assessing the risks. If a crisis occurs at this point, external resources will probably be required to recover from the damage caused and avoid further escalation. Since contingency plans cover previously assessed risk situations, we can see the importance of a more complete and detailed risk study.

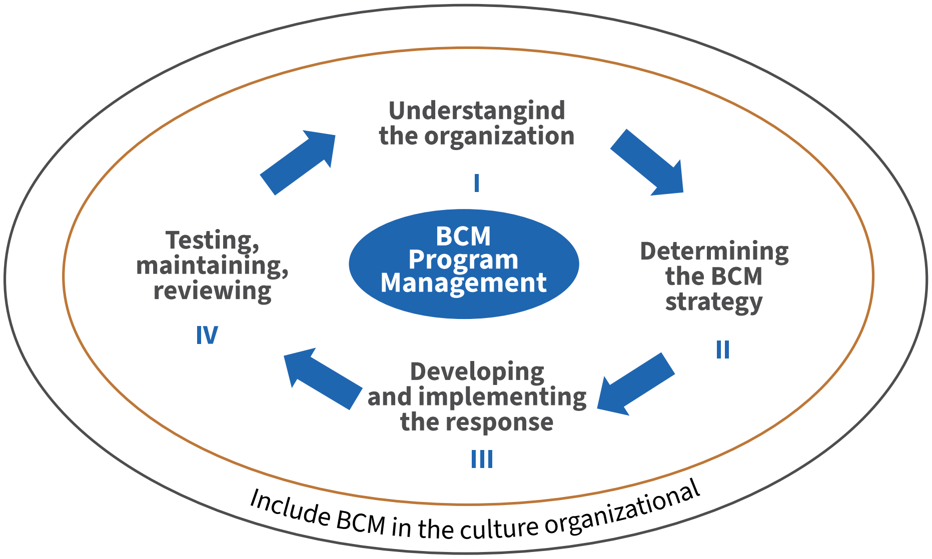
3 Business Continuity Management System

A business continuity management system (BCMS) identifies the effects that activity downtime may have and establishes response measures. Note that early assessment of the potential for disruption may lead to the adoption of preventive measures. It is necessary to take into account all the different factors and agents that must act in a risk situation. If it is rigid, it will surely leave aside some of the threats that can negatively affect its functioning (Estruga, 2023).

Business continuity management (BCM) is a recurring process, with its own life cycle.

Figure 2 below summarizes the BCM life cycle.

FIGURE 2: BCM Life Cycle


Understangind the organization
I
Determining the BCM strategy
II
Developing and implementing the response
III
Testing, maintaining, reviewing
IV
BCM Program Management
Include BCM in the culture organizational

Source: Adapted from BSI 25999 and ISO 15999–1.

The main goal of a BCMS is to make it possible to manage, plan, monitor, control, and permanently improve an organization's business continuity strategy in order to guarantee its critical operation in case of a contingency.

4 The Four Stages of a BCMS

The cycle begins with **understanding the organization**, its business processes, its resources, and its priorities (**I**). The BCMS must be aligned with the organization's strategies. Additionally, one of the best practices for leadership teams is to understand the outlook for threats, especially those that are most likely in the social and natural context in which the tax administration operates and identify potential problems. To the extent that strategies are dynamic, the execution of the BCMS must also reflect changes. Therefore, the BCMS cannot be unalterable or independent of the organization's management. Techniques such as SWOT analysis[3], risk analysis, and strategic planning can also be useful to provide knowledge.

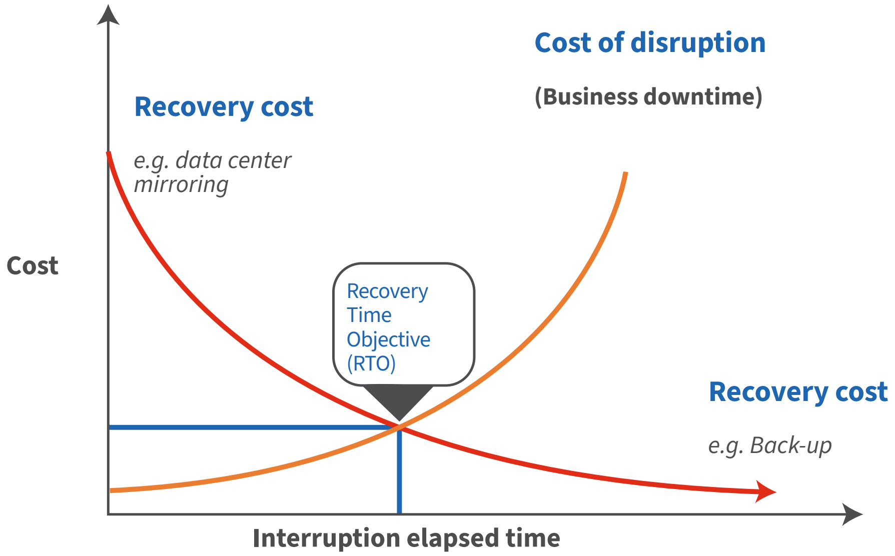
ISO 22301 requires the organization to determine what will be covered by business continuity, as well as what will be excluded. On the other hand, the organization is required to communicate to parties - both internal and external - the scope of the BCMS.

From this understanding, we can work on determining the **BCM strategy** (**II**). To do so, it is essential to evaluate how disruptions and deviations can affect the business, given the strategic management of the organization. This is done through business impact analysis (*BIA*). This analysis should examine the impact of the disruption in terms of criticality and importance, the consequences on other business areas, and the data that will be lost. Put another way, the first step in building a BCP is to evaluate business processes to determine which are the most critical, which are the most vulnerable and to what type of events, and what are the potential losses corresponding to periods of inactivity (hours, days, or weeks).

[3] Acronym for *Strengths*, *Weaknesses*, *Opportunities*, and *Threats*.

While the ideal is to have very low disruption and not lose any operations or data, this type of capability requires a large number of resources, and costs need to be accurately assessed. Figure 3 below shows the cost variation of a strategy, from one that assumes near-zero, but high-cost, disruption to one that allows for long, but low-cost, disruption.

FIGURE 3: **Recovery Cost vs. Downtime**



Source: Adapted from Smith and Elliot (2006).

Recovery Time Objective (RTO) is the maximum acceptable time that an application, computer, network, or system can be disabled after an unexpected disaster, outage, or comparable event occurs.

The availability of financial and/or human resources is a critical factor in determining an ideal strategy for business continuity management, indicated by risk assessment. Likewise, not making decisions due to lack of resources for an ideal solution should not be considered a possibility. It is possible to create scenarios with simple and low-cost strategies (considering the most probable situations detected and expanding the RTO), which advance to more complete levels as resources are made available. For example, starting with full backups found outside the main data center, leading up to – possibly – a duplication of the data center. Along the same lines is the hiring of cloud services, which may be another strategy.

Continuity of information systems is of utmost importance in the business continuity of a tax administration. The criticality of each system depends on the strategic importance of the area it serves, and the assessment criteria usually vary over time: there may be seasonality in taxes (such as posting and collecting Vehicle Tax) or concentration of an activity on certain days of the month (deadlines for collecting certain taxes, for instance). The criteria may also vary depending on other factors, such as making the taxpayer registration functionality available during a stimulus period for regularizing the tax status of companies.

The criteria may also vary depending on other factors, such as making the taxpayer registration functionality available during a stimulus period for regularizing the tax status of companies.

The increasing use of electronic invoices (e-invoices) generates new risks. Important cases are related to e-invoice issuance/validation systems: sometimes, the tax administration itself issues invoices for small/medium taxpayers, and discontinuation of this system would cause a lot of damage to the economy, while at other times, these operations are outsourced, and the companies involved must be covered by the contingency plan.

As can be seen, there must be common sense and collaboration in these assessments of criticality and importance to stakeholders, so that the study is based on broad interests and goals, and not just individualized perspectives.

Interdependence between systems is an important issue to consider. It is possible to make direct use of a system that depends on another system, which, in turn, is not considered critical or important. Dependency chains must be clearly known and respected, with the support of the IT department.

The **development and implementation of the business continuity management strategy (III) makes it possible** to choose and implement a suitable response for each scenario, system, or service, considering parameters defined as acceptable, such as level of operation and time limits. Options will consider resilience and existing countermeasure choices, with particular emphasis on implementation and maintenance costs.

Also, along these lines, it is possible to create a management structure that covers incident management, business continuity, and recovery plans, among others. These plans detail the actions to be taken during and after an incident, with the aim of continuing and restoring operations according to established parameters.

Testing, maintaining, and reviewing the business continuity management plan (IV) allows the organization to prove the extent to which its strategies and plans are complete, up-to-date, and accurate. It is a time to identify opportunities for improvement.

Periodic tests should be planned with the types and methods proposed in ISO 22301 (simple, medium, complex). Each type of plan must have a defined maintenance/reviewing schedule (e.g., once or twice a year). Testing a BCP is the only way to verify its effectiveness before an unforeseen event occurs.

The plan should be a living document that is reviewed periodically to stay updated on system improvements and organizational changes

5 Organizational Culture

Another critical aspect is the inclusion of business continuity management in the organizational culture, allowing it to be configured as part of the organization's values, providing confidence to interested parties about its ability to survive disruptive events. Awareness-raising and training actions cover this aspect. The human factor is an important part in this context, which must be considered in structuring, developing, and carrying out the project, including establishing an institutional consensus on its strategic importance for the organization.

6 BCP, COVID-19, and other Wide-Ranging Crises

The crisis caused by COVID-19 not only affected the lives of people around the world, but also brought challenges for tax administrations on how to ensure the continuity of their critical activities and the safety of officials and taxpayers during the pandemic.

Along these lines, international organizations proposed guidelines for tax administrations to face these challenges, such as CIAT/IOTA/OECD (2020) and Brondolo, Aslett and Komso (2020). It is noteworthy that these guidelines follow, structurally, the model proposed by the ISO standards on security and resilience, mentioned at the beginning of this document.

Although written in the context of COVID-19, these guidelines can serve as a basis for evaluating measures to address other types of wide-ranging crises, especially those caused by natural events, e.g., other pandemics, earthquakes, floods, volcanic eruptions.

There is consensus among international organizations that there is no single solution to this problem, since tax administrations start from different positions, such as level of digitalization of services, deployment of remote work, outsourcing agreements, and scope of action.

It can be noted that the support of information technology is of utmost importance for a contingency plan designed to mitigate a disease outbreak. The plan must ensure at least uninterrupted availability of: (1) central processing units, (2) electronic taxpayer services, and (3) computing support for essential and mission-critical support functions. This includes allowing managers and officials to work remotely by providing them with the necessary equipment, training, and secure electronic access to systems.

CONTENT

It is thus considered that tax administrations can face these disasters more quickly if they have managed to develop the two attributes below:

- Maximizing automation (computerization) of internal tax processes – used by officials and external – used by taxpayers –.

- Providing administrative and technological capabilities for implementing large-scale remote work.

Brondolo, Aslett and Komso (2020) propose a set of actions, similar to those pointed out by the ISO standards, but geared towards the pandemic under discussion:

a) **Action plan for mission-critical systems**
Guarantees that the tax administration can continue to perform its most important operations during the crisis.

b) **Action plan to support health and safety**
Actions aimed at protecting employees and visitors from infectious diseases.

c) **Workforce deployment support plan**
Ensuring that the tax administration has adequate workforce to perform its critical functions.

d) **Computing support plan**
Computing is very important for pandemic mitigation actions. Several guidelines are proposed in this document.

e) **Facility support plan**
Intended to ensure the safety and integrity of the physical premises of the tax administration during the outbreak.

f) **Communication support plan**
Effective communication is an important part of the response to a crisis, both internal communication (with managers and employees of the tax administration) and external communication (with all interested parties inside and outside the government, including taxpayers).

7 The Practice of BCPs in Tax Administrations

Below is an outline of business continuity/operational continuity practices available for select tax administrations.

7.1 National Superintendency of Customs and Tax Administration (SUNAT) – Peru

The SUNAT is a specialized technical organization linked to the Ministry of Economy and Finance. Its primary purpose is to manage the taxes of the national government.

Although the SUNAT has offices throughout the country, its main activities are carried out in Metropolitan Lima, this being the most geographically vulnerable location.

The development of the Operational Continuity Plan (OCP) meets what is determined by the ministerial resolution that guides the formulation of operational continuity plans for public entities. The enforcement of the PCO is planned in case of an adverse event whose magnitude specifically affects the SUNAT's operation, caused by a large earthquake, tsunami in Lima and Callao, fire, terrorist attack, social upheaval, computer attack, or pandemic, without, however, failing to consider other dangers that may arise.

The plan identifies and describes in detail the current risks and available resources, with an estimate of the associated impact levels and respective actions.

Among the SUNAT's main resources are its computer systems, classified as a National Critical Asset. The SUNAT maintains a general high-availability strategy between its data centers in Surco and San Isidro, which allows it to recover any service efficiently and effectively in case of a network, application server, or database server downtime. The Surco Data Center, especially, is a housing service with TIER III certification by the Uptime Institute[4]. This strategy is considered in the PCO's establishment of actions.

There are eight critical activities that must be maintained:

1. Control of entry of goods
2. Control of exit of goods
3. Tax collection management
4. Assistance to taxpayers and citizens
5. Procedure for exchanging information among countries
6. Human resource management
7. Administrative management
8. Financial management

The PCO identifies roles and responsibilities for the development of critical activities, alternate venues for different activities, considering their capabilities and construction characteristics (for example, energy dissipation elements in seismic events), responsibilities for damage assessment and disclosure processes, and announcement of officials.

The plan also consists of a schedule of drills and simulations.).

For more details, see SUNAT (2022a) and SUNAT (2022b).

7.2 Internal Revenue Service of the United States of America (IRS)

The following is an overview of the IRS' continuity plan, its guidelines, and its components.

[4] One of the requirements of TIER III certification is 99.98% availability.

Continuity planning establishes activities and efforts to document and ensure that the IRS can continue its Mission Essential Functions (MEFs) and Essential Supporting Activities (ESAs) during a wide range of potential emergencies.

The IRS' continuity planning is based on the assumption that there will be no warning of potential emergencies or incidents, using a worst-case scenario (inaccessibility or unavailability of an IRS facility and all its content). The main goal of the continuity plan is to ensure the recovery of the MEFs and the ESAs.

MEFs are directly related to fulfilling the organization's mission: to provide those goods and services to the Nation for whose production the agency was created in the first place. They are: (i) Processing Tax Remittances, (ii) Processing Tax Returns, and (iii) Processing Tax Refunds. These services must be operational within 12 hours.

ESAs are the essential functions that must be carried out to support the agency's performance in its MEFs. ESAs are common to most agencies (paying personnel, providing a safe workplace, ensuring computer systems are working, etc.), but they do not fulfill the agency's mission. These must be operational quickly to support the recovery of the MEF. A specific time will be determined for each process. The ESAs are the following: Physical Security; Facilities Management; Information Technology; General Legal Services/Chief Counsel; Financial Management; Procurement; Communications; Payroll; and Human Resources/Benefits.

There are also Business Priority Processes (BPPs), which are important and urgent to fulfill the mission of the business units in support of the MEFs; however, compliance with the BPPs does not complete the mission or deliver the services for which the agency was created. These functions are usually recovered through relocation.

The IRS has six BPPs: Taxpayer Assistance; Advocate Fair Taxpayer Treatment; Perform Compliance Activities; Perform Litigation; Provide Appeals Process; and Online Services.

The objectives of the Contingency Plan are established by Federal Directive and include: ensuring the safety of IRS personnel and visitors; ensuring the IRS can continue to perform its MEFs and ESAs, including conducting activities from an alternative location, if necessary; reducing the loss of life and minimizing property damage and loss; executing, as required, a successful succession to office with accompanying delegation of authorities in the event a disruption renders IRS leadership unable, unavailable, or incapable of assuming and performing its duties and responsibilities; reducing or mitigating disruptions to IRS operations; ensuring that IRS has facilities available where it can continue to perform its MEFs during a continuity event or emergency; protecting essential facilities, essential records, equipment, and other assets in the event of a disruption; achieving a timely and orderly recovery and reconstitution from a continuity event or emergency; ensuring and validating IRS continuity readiness through an integrated continuity test, training, and exercise program to support the implementation of the IRS continuity plans.

The following continuity requirements, among others, are part of the plan:

- The IRS must be able to continue carrying out its MEFs and ESAs during any emergency for a period of up to 30 days or until normal operations can resume.

- The IRS must have the ability to be fully operational at its continuity facilities as soon as possible after an emergency occurs, but no later than 12 hours after continuity operations begin.

The authorities and their responsibilities, succession orders (change of leadership), delegations of emergency authority, supervisory responsibilities, among others also make up the Contingency Plan. For more details, see IRS (2022).

7.3 Department of Finance of the State of Maranhão – Brazil (SEFAZ-MA)

Maranhão is a state in the northeast of Brazil and its Department of Finance (SEFAZ) has the mission of promoting and controlling compliance with tax obligations with equity and efficiency, with the aim of contributing to the development of the State[5].

The intensive use of information technology has contributed strongly to the fulfillment of the SEFAZ's mission.

[5] In Brazil, the states are federative units with administrative/tax/financial autonomy, with competence to legislate and manage certain taxes.

In 2019, an analysis was performed using the Tax Administration Diagnostic Assessment Tool (TADAT). On that occasion, one of the highlighted weaknesses was the lack of a business continuity plan especially related to IT. THE 2020-2023 Strategic Plan addressed this need, determining the development of a business continuity plan for information technology, aligned with the other activities of the SEFAZ[6].

It should be noted that resilience of the central environment (Data Center) was already being used as a parameter for purchasing IT solutions, with redundant high-availability equipment, a safe room, independent cooling, supplementary electrical generators, and an advanced physical security system.

The continuity plan developed used the ISO and ABNT standards as a methodological basis, generating a set of operational plans for the identified downtime scenarios and strategies to improve continuity:

i) i) Short-term strategy, based on strengthening the central IT environment and finding a location for the future implementation of a secondary site. The Data Center of the Deputy Department of Information Technology, which needs to be expanded and adapted, will be used for this purpose. In this first phase, this location will house data backup tools.

ii) ii) Medium/long-term strategy, which will evaluate the feasibility of implementing a secondary site operating cold (receiving updates in a backup database and with the necessary computer equipment to operate priority systems in contingency mode; in the event of downtime that is critical at the primary site, the secondary site would assume the planned operation through previously defined actions/procedures; the scope of priority systems to operate depends on the size of the equipment involved) or operating hot (simultaneouslywiththeprimarysite,withadistributedloadofidenticalandsynchronizedapplicationsand databases;intheeventofdowntimeatoneofthesites,theotherwouldautomaticallytakeoveralloperations; depending on the size of the equipment, the service degradation could be minimal or acceptable).

The use of cloud computing will be assessed as an alternative.

The 2024-2027 Strategic Plan addresses complementing the medium/long-term continuity strategy with the allocation of the necessary resources.

[6] See SEFAZ-MA (2020).

8 Audits and Automation

Carrying out a business continuity audit is one of the ways to ensure that disruptive events will have the least possible effect on activity.

For this to be effective, auditors (both internal and external) must follow a series of guidelines and recommendations. Some issues that need to be addressed: confirming the scope of the BCMS; leadership and involvement of senior management (executives must agree on the principles and the balance between costs, complexity, and scope); documentation of business continuity objectives; awareness on the part of all parties involved; consulting if all the necessary components exist (BIA, strategies, continuity plans, etc.); proposing improvements and corrections (Estruga, 2023).

The Canada Revenue Agency (CRA) promotes periodic internal audits of its information systems, as part of a Business Continuity Management Program. At the time COVID-19 was declared a pandemic, it was carrying out one of these audits, the results of which were also used to improve the response to the calamity (CRA, 2021).

The key expected results of the audits driven by the CRA are adjustments to the following documents: **Business Continuity Plans**: enhancements of the plans, with the aim of outlining the minimum acceptable recovery configuration requirements, strategies, and all contact information necessary to maintain and recover critical services; **Critical Services Inventory**: review of the list of services whose compromise, in terms of availability or completeness, would result in a high or very high degree of harm to the health, safety, or economic well-being of Canadians or to the effective functioning of the Government of Canada; **Critical Business Applications and Services**: up-to-date list of applications that enable critical services; **After-Action Reports**: exploration of documents that capture experiences, gaps, and lessons learned after unplanned disruptions or testing exercises.

There are software packages on the market that automate the operational mechanics of a BCMS. For this purpose, these systems actually maintain a repository of BCMS documents and establish relationships among them, allowing integrated viewing and agility in their operation. It is not efficient or operational to rely on searches in paper manuals. Furthermore, in natural disasters, it is common for the responsible personnel not to arrive at their assigned work centers on time, due to being stuck in traffic jams, unavailability of transportation, etc. These software packages can enable remote interaction among those responsible, based on a suitable infrastructure. The packages themselves are continually improved, and the most recent alternatives can be searched on the web, such as the document drafted by the company Veritis[8].

It is very important to highlight that automation software does not perform continuity management: it simply automates many administrative and coordination tasks previously established in the plan.

[8] See https://www.veritis.com/blog/8-best-business-continuity-management-software-solutions/

9 BCP in the Cloud

Another important consideration is evaluating the use of cloud computing as a contingency strategy. Although we consider problem of using confidential data entrusted to the tax administration in external environments, it is possible to assess at least the contingency of subsystems and non-critical data in the cloud.

There are important aspects that must be considered in a cloud business continuity strategy, as proposed in Posey (2022):

- **Cost:** the savings obtained from public clouds can be difficult to achieve. The same for private clouds. It is important to evaluate the specific cost for a contingency plan.

- **Hardware and software compatibility:** some applications will not work in the cloud, while others will, but may be too expensive to run in that environment.

- **Cloud provider reputation and assurances about continuity:** mission-critical systems should not be entrusted to a provider with a reputation for periodic downtime or one that could go out of business within the next week. A service level agreement must guarantee a minimum level of service.

- **Data ownership:** the provider must be transparent about where the data will be stored, and the terms of service must ensure security of access to this data.

- **Cost of moving data out of the cloud:** most cloud providers charge a data removal fee. This includes data that migrates to an organization's own data center or to another cloud. These fees can be quite high, so it is important to know how much a transfer would cost. There are even certain backup and recovery operations that may incur data output fees. It should be clear when such charges might be incurred.

- **Who is in charge of backing up data and what methods will be used?** most cloud providers have adopted a shared responsibility model, where the provider is in charge of maintaining the underlying infrastructure, and subscribers are responsible for backing up and protecting their own data.

- **Cost and availability of support within the cloud:** IT is important to verify that assistance will be available in times of crisis and how much that additional support might cost.

- **Security:** it is necessary to verify whether the cloud-based business continuity plan will undermine security. This is especially true in regulated institutions, such as tax administrations, where it is possible to apply penalties for breaches of security best practices.

As can be seen, many of these aspects must be considered in any strategy for using the cloud to host information systems. The tax administrations of Mexico, Peru, Guatemala, and Colombia have their own strategies for using the cloud.

10 Final Remarks

Despite the importance assumed by tax managers, and now reinforced by the COVID-19 pandemic, of the 92 assessments carried out using the Tax Administration Diagnostic Assessment Tool (TADAT) to date, the majority of low- and middle-income countries did not have a robust BCP (IMF-FA, 2020).

The development of a BCMS covers technological and management aspects, but the design and implementation of the strategic component is possibly the main factor to achieve success.

The main executives of the tax administration must be involved from the beginning, knowing and participating in the main aspects of the plan and in the definition of its limits.

The definition of the limits and conditions of downtime implies new financial and human resources: less service downtime means more costs (see Figure 3). Thus, a joint analysis of the strategic recovery options versus the respective costs and limits of action will avoid future surprises.

References

Brondolo, J., Aslett, J., Komso, A. (2020). Tax Administration: Designing a Business Continuity Plan for an Epidemic. IMF Technical Notes and Manuals. TNM 2020/001. IMF Fiscal Affairs Department. Washington, DC.

CIAT/IOTA/OECD (2020). Tax Administration Responses to COVID-19: Business Continuity Considerations. OECD. Paris. Disponible en: https://biblioteca.ciat.org/opac/book/5721

CRA (2021). Internal Audit – Information Technology Continuity Management. Disponible en: https://bit.ly/4b250gh

Estruga, N. (2023). ISO 22301: Cómo establecer un Sistema de Gestión de Continuidad del Negocio. Ealde Business School. Disponible en: https://www.ealde.es/iso-22301-continuidad-negocio/

FMI-FA (2020). Continuidad de las Operaciones de las Administraciones de Ingresos Públicos. Fondo Monetario Internacional – Fiscal Affairs. Disponible en: http://bit.ly/48F9at1

IRS (2022). Security, Privacy and Assurance: Overview of Continuity Planning (Manual). IRS. Disponible en: https://www.irs.gov/irm/part10/irm_10-006-001

Posey, B. (2022). Business continuity in the cloud: Benefits and planning tips. TechTarget Blog. Disponible en: https://www.techtarget.com/searchdisasterrecovery/tip/Business-continuity-in-the-cloud-Benefits-and-planning-tips

SEFAZ-MA. (2020). Plano Estratégico 2020-2023. Secretaria de Estado de Fazenda – SEFAZ. São Luís. Disponible en: https://sistemas1.sefaz.ma.gov.br/portalsefaz/files?codigo=20180

Smith, D. y D. Elliot (Editores) (2006). Key Readings in Crisis Management. Routledge, London y New York.

SUNAT (2022) a. Plan de Continuidad Operativa. Oficina de Seguridad y Defensa Nacional. Julio. Disponible en: https://www.sunat.gob.pe/legislacion/superin/2022/anexo-135-2022.pdf

SUNAT (2022) b. Plan de Prevención y Reducción de Riesgos de Desastres de la SUNAT. Oficina de Seguridad y Defensa Nacional. Disponible en: https://www.sunat.gob.pe/legislacion/superin/2023/anexo-000241-2023.pdf

APPENDIX:

Documents that Make Up a Business Continuity Plan (Non-Exhaustive List)

- Systemic Architecture
- Business Continuity Policy
- Business Impact Analysis (BIA) Report
- Risk Analysis Report (RAR) and Operational Risk Report (ORR)
- Business Continuity Strategy Report
- Crisis Management Plan
- Incident Management Plan
- Operational Continuity Plan
- Disaster Recovery Plan
- Testing and Validation Plan
- Business Continuity Plan

Working Papers *Serie*

CIAT Executive Secretary
P.O. Box: 0834-02129, Panama, Republic of Panama
Phone: (507) 307-2428
Fax: (507) 264-4926
E-mail: ciat@ciat.org
Web: www.ciat.org