ENHANCING AUDITING OF PUBLIC SERVICE CONTINUITY PLANS IN POLAND

Best practices for internal audit functions

Funded by the European Union

OECD
BETTER POLICIES FOR BETTER LIVES

Ministry of Finance
Republic of Poland

This document was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

The project was funded by the European Union via the Technical Support Instrument, and implemented by the OECD, in cooperation with the European Commission.

This paper was approved and declassified by the Public Governance Committee on 14 November 2024.

Cover design by Meral Gedik using image from © Lukasz Pawel Szczepanski/Shutterstock.com.

About This Paper

The COVID-19 pandemic crisis highlighted several areas where governments must improve in how they manage crises and extraordinary events, including the challenges affecting the delivery of critical public services. Part of those challenges included those related to digitalisation.

This paper is designed to inform and support all public sector internal audit practitioners working within internal audit functions and all other functions performing audit or assurance related activities, either directly or indirectly, within Poland. It will describe the context surrounding the auditing of public service continuity plans along with the implications and experiences related to digitalisation in the public service. It is vital that all aspects of digitalisation are considered to ensure continuity plans remain relevant and up to date.

This guidance discusses the elements of a business continuity plan and details the aspects of performance auditing and digitalisation in relation to the following topics: selecting audit type, resources, objectives, scope, risk assessment, criteria, involvement of stakeholders, checklist recommendation and necessary competencies to support auditors. It will contribute to the preparedness of internal audit functions across all levels of government in Poland. It guides practitioners in providing assurance that an organisation's governance of the continuity processes and related risks are effective and in line with the organisation's objectives. This will further help organisations be better prepared in the event of an emergency or extraordinary event.

This guidance describes international regulations related to continuity and the elements of the standards required. These elements include the context of the organisation, leadership, planning, support, operation, performance evaluation and improvement. It further describes the business continuity management policy in Poland's Ministry of Finance and the related responsibility.

The guidance includes international good practice examples, including topics related to business continuity such as, toolkits, strategies and steps for an appropriate emergency plan. It also includes relevant examples of auditing of continuity planning including examples of objectives, scope, criteria and relevant recommendations. These examples provide guidance on structure and language which may be used when developing a similar type of audit on continuity planning.

The OECD would like to express its appreciation to the Poland Ministry of Finance in the development of this guidance, within the framework of the Technical Support Instrument.

Table of contents

About This Paper 3

1 Introduction 6
Audit Universe 6

2 Regulations and Standards 15
Continuity Regulation 15
Continuity Regulation in Poland 18
Notes 19

3 Audit Attributes 20
Selecting Audit Type 20
Timing and Resources 20
Objectives 20
Scope 21
Risk Assessment 23
Criteria 23
Involvement of Stakeholders 26
BCP Audit Checklist 26
Recommendations 29
Reporting 30
Competencies Supporting Auditors in Digitalisation 31
Notes 32

References 33

Glossary 36

FIGURES

Figure 1.1. Continuity Planning Framework in the U.S. federal government 7
Figure 1.2. Illustration of business continuity being effective for sudden disruption 8
Figure 2.1. ISO 22301 Business Continuity Management Systems – Elements of standards 15
Figure 3.1. Differences among Emergency response, Crisis Management and Business Continuity 22

INFOGRAPHICS

Infographic 1.1. Digital Technology Ecosystem 9
Infographic 1.2. OECD Going Digital Indicators – Poland vs OECD Countries 10

BOXES

Box 1.1. OECD Public Integrity Handbook (Chapter 13 – Participation) 14
Box 2.1. The UK's Business Continuity Management Toolkit 16
Box 2.2. Business Continuity Management Strategies in the UK's Toolkit 17
Box 2.3. Business Development Canada's steps for planning an emergency and disaster plan 18
Box 2.4. Business Continuity Management Policy in Poland's Ministry of Finance 19
Box 3.1. Example of Relevant Audit Objective 21
Box 3.2. Examples of Relevant Scope 22
Box 3.3. Examples of Relevant Audit Criteria 25
Box 3.4. Checklist for BCP Audit 27
Box 3.5. Example of Relevant Recommendations 30

1 Introduction

The Institute of Internal Auditors (IIA) defines internal audit as an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. Throughout the global public sector, there are various types of audits that are conducted with varying objectives. (IIA, 2024[1])

The COVID-19 pandemic crisis raised the importance of how governments manage crises. The situation created uncertainty across all sectors globally, especially in the public sector. This was particularly complex, as the delivery of critical public services needed to be ensured, while the majority of public servants were forced to transition their work remotely and virtually, in a matter of weeks. This required appropriate continuity planning from all public entities. Moreover, the massive increase in digitalisation and remote work, while maintaining public services, created a large set of new risks. The internal audit units were utilised in an array of ways throughout the various governments of the world. Some played a key factor in many roles related to the crisis while others continued their usual operations.

Audit Universe

What is a Business Continuity Plan?

Business continuity refers to an organisation's ability to continue delivering products or services at a predefined capacity within an acceptable timeframe during a disruption. A business continuity plan (BCP) is a documented guide that helps an organisation respond to disruption and resume, recover, and restore service delivery.

From a broader perspective, a BCP can be seen as the process of building a business continuity management system (BCMS) and its results. BCMS is designed to manage an organisation's ability to continue operations during disruptions. It supports strategic objectives, boosts reputation, and enhances resilience. The BCMS builds confidence among business partners and reduces both legal and financial risks, as well as costs associated with disruptions. It also considers the expectations of relevant parties, safeguards life and property, protects the environment, and bolsters the organisation's effectiveness during disruptions by proactively managing risks (ISO, 2019[2]). A BCMS should include the following components:

- a policy
- competent people with defined responsibilities
- management processes relating to:
  - policy
  - planning
  - implementation and operation
  - performance assessment
  - management review

- continual improvement.
- documented information supporting operational control and enabling performance evaluation.

Figure 1.1 shows an example of the overall process of the BCP model in the U.S. federal government. Organisations must first identify their essential functions. They then determine the planning factors necessary to carry out these functions, conduct risk assessments for each planning factor, and finally identify and implement continuity strategies to address the areas of greatest vulnerability.

Figure 1.1. Continuity Planning Framework in the U.S. federal government

Source: (FEMA, 2023[3]).

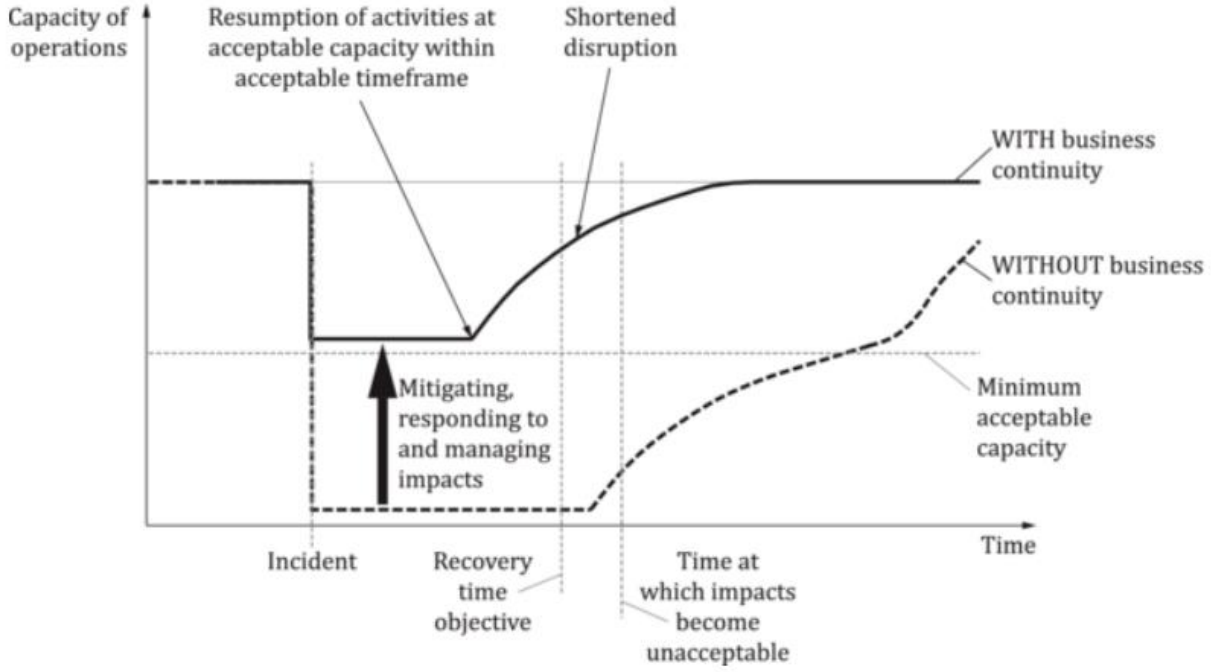
Importance of Business Continuity Plan in the Public Sector

Critical risks can develop quickly and spread unpredictably across borders. These risks can have nationally significant impacts, disrupt essential infrastructure, harm key environmental assets, strain public finances, and diminish public trust in the government. Effective risk governance can help maintain or enhance a nation's competitive advantage. This is crucial in the face of uncertainties surrounding geopolitics, the environment, society, and the economy (OECD, 2014[4]). Ensuring the continuity of essential public services during crisis times is crucial to the well-being and safety of citizens, and it significantly influences the recovery process.

In the face of disruptions to routine operations, organisations need to ensure the continuity of vital functions. These disruptions often lead to constraints on resources, assets, and capabilities. In such scenarios, the focus is on maintaining operations with little to no margin for downtime, while activities that can be delayed are put on hold. It is crucial for organisations to analyse their operations to determine which tasks must continue without interruption and which can be minimised, delayed, or set aside. Prioritising resources in potentially limited scenarios involves understanding the needs of the organisation's staff, equipment, systems, information, data, and sites to fulfil its mission. By examining the susceptibilities of each planning factor to a wide array of threats and hazards, organisations can gain a better comprehension of the overall risk each essential function faces. The allocation of staff, equipment, data, and sites is among the many strategies that can help reduce risk and ensure organisations continue performing their essential functions with minimal to zero downtime (FEMA Office of National Continuity Programs, 2023[5]).

Figure 1.2 shows how business continuity can be effective in mitigating impacts in certain situations.

Figure 1.2. Illustration of business continuity being effective for sudden disruption



Source: (ISO, 2019[2]).

Modern business continuity management strategies are closely tied to the digitalisation of administration. As administrative tasks become more digital, the safety and adaptability of these systems significantly impact business continuity. Digitalisation also presents opportunities to bolster business continuity in crises. For instance, during the COVID-19 pandemic, the adoption of remote work and digital administration tasks in sectors like tax, architecture, and public procurement bidding helped maintain essential administrative functions. It implies that it is crucial to ask, "Can the administration's digital functions be adequately performed in a crisis?" and "Are management and staff prepared for these changes?" when auditing the BCP.

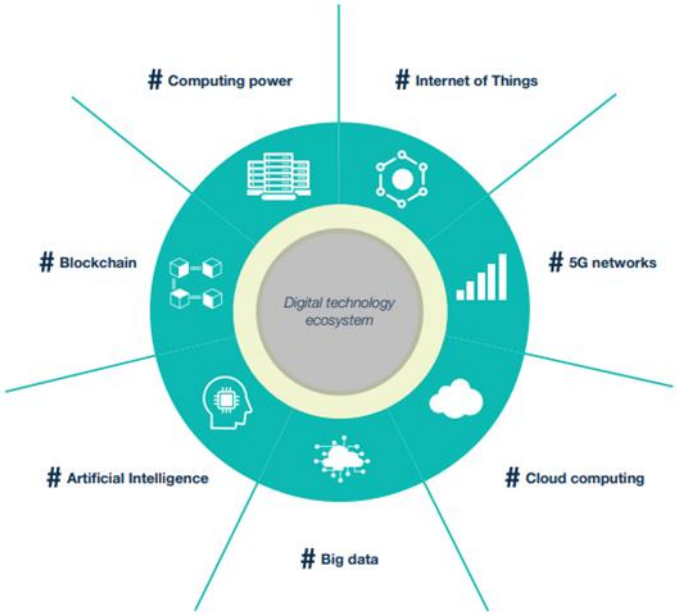
The experience of COVID-19 has shown that the responsiveness and quality of the continuity of public services in a crisis can greatly impact the lives of citizens. The COVID-19 pandemic posed a significant challenge to the continuity of public services. For instance, when educational institutions were abruptly closed due to lockdowns, educators promptly transitioned to remote teaching via online platforms and digital materials, wherever infrastructure permitted (UN, 2020[6]). Despite these responses, the education gap significantly widened during the disruption caused by COVID-19 and overall academic achievement fell in OECD countries from 2022 to 2018, as seen in the OECD's Programme for International Student Assessment (OECD, 2024[7]) (Kuhfeld et al., 2022[8]). This example shows how important it is to maintain the continuity and quality of public services as much as possible.

Digital Transformation

Digitisation is the adaptation of analogue data and processes into a machine-readable format. Digitalisation is the use of digital technologies that result in new or modifications to existing activities. Digital transformation commonly concerns the economic and societal effects of digitisation and digitalisation. To develop policies for the digital age, it is critical to be aware of the main elements of the evolving digital technology ecosystem and possible opportunities (and challenges) resulting from their application. Moreover, it is essential to understand the data revolution that is occurring and how data and data flows affect individuals, the economy and society more broadly. Finally, it is important to identify the key

properties of digital transformation, including how they are driving new and evolving business models, and what their implications may be for public policy (OECD, 2019[9]). See Infographic 1.1 for the aspects of the digital technology ecosystem.

Infographic 1.1. Digital Technology Ecosystem



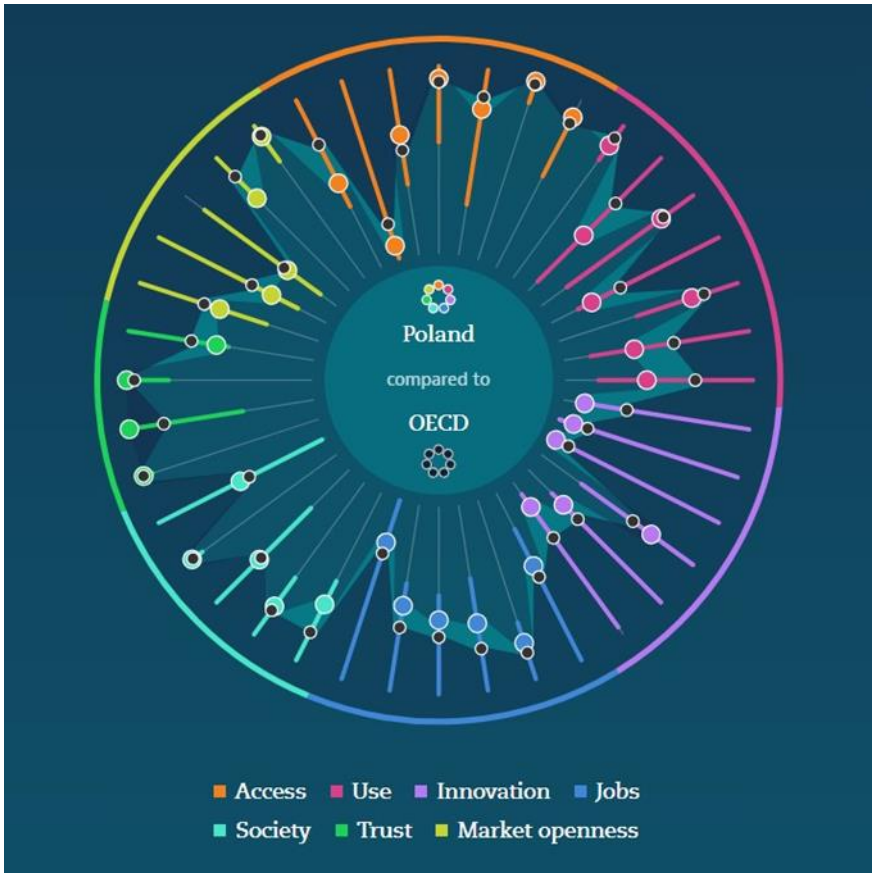
At the onset of the COVID-19 pandemic, policymakers and academics alike expected that the pandemic and subsequent containment policies would accelerate digitalisation, with potentially important implications for labour markets and productivity. Many workers had to switch from working in the office to working from home, and economic activities that are contact-intensive were restricted. As a result, many firms had to adjust to remote work and expand their activities online, which required changes in operations, logistics, and possibly a rapid investment in information and communication technology (ICT). During the COVID-19 pandemic, these forms of digitalisation that allowed businesses to operate remotely may have supported employment and labour productivity, and there were also hopes that they would boost firms' and workers' productivity in the longer term. In contrast, expectations regarding long-term impacts on the labour market were more mixed, with fears that digitalisation could displace swaths of low- and middle-skilled workers.

While further natural pandemics are possible there are other potential future disruptions which may have an impact on the ecosystem. Possible disruptions may include:

- Engineered pandemics: the presence of genetic engineering and bioengineering create the risk of pandemics which may be the most devastating in the history of humanity. As their intention is to cause mortality they have a significant impact to society.
- Kessler syndrome: the extraordinary volume of satellites orbiting the earth continues to generate technological and economic opportunities. At the same time it increases the risk of collisions and a chain reaction of them (also known as Kessler Syndrome) has the potential to destroy the world's communication systems and disrupt years of progress.
- Unaligned artificial intelligence: the accelerated advancement of technology is pushing society to the development of superintelligence. As machine learning and artificial intelligence decrease the volume of human inputs for society to operate, machines will be responsible for conducting new tasks. If learning and self-improvement surpass what is acceptable, there is a risk that humanity may lose control of its own trajectory. (OECD, 2021[10])

OECD developed the Going Digital Toolkit, which is structured along the seven policy dimensions of the Going Digital Integrated Policy Framework, which cuts across policy areas to help ensure a whole-of-economy and society approach to realising the promises of digital transformation for all. Infographic 1.2 represents the current situation in Poland compared to other OECD countries.

Infographic 1.2. OECD Going Digital Indicators – Poland vs OECD Countries



Source: (OECD, 2024[11]).

Digitalisation in the Public Sector Post Pandemic

The topic of digitalisation and how governments continuously transition and manage it is integral within the context of continuity planning. Therefore, auditors must understand its significance, particularly how it stemmed and advanced in recent years.

Digitalisation and transformation move away from the *status quo*, demanding that governments innovate and allow them to become more responsive, accountable, agile and efficient. Governments must accept change and encourage a culture of innovation to facilitate employees and organisations to experiment, learn and develop. As the culture of the public sector will evolve with changing needs, increasing flexibility and productivity, all stakeholders must be aware of the constantly evolving risks.

As digitalisation is associated with being data driven, governments will work towards data optimisation by improving and developing approaches to data collection, collation, analysis and dissemination. The use and sharing of data include both the public and private sectors. Government plays a role in ensuring its accessibility, usability and being actionable across various levels of government. In that context, data

should be appropriately secured and protected. Auditors can play a role in that, ensuring as data becomes publicly available that appropriate controls are in place to safeguard it respectively.

The COVID-19 pandemic demonstrated that governments were not prepared to handle the crisis in a variety of ways. Since that time though, it was the catalyst in the commencement of a digital transformation to build a sustainable and digitally robust society. The pandemic provided governments the opportunity to play a central role in addressing societal obstacles. Digital technologies were used to respond to crises in the short term and ideally, reinvigorate policies and other tools in the long term.

The introduction of new technologies played an important role in government efforts to co-ordinate the COVID-19's response, ensuring society remained functional during lockdowns and discovering solutions across the various sectors. Going forward from crisis response, governments continue to work towards recovery and rebuilding.

Through the pandemic, governments implemented initiatives and adopted policies to increase overall connectivity. This was the scenario in all countries. This level of increased connectivity has an impact on the continuity of government as it has reached a scale which is larger than ever before. This level of connectivity was transformative across many sectors.

Virtual communication became the standard which was contrary to the traditional approaches of in-person interaction. Different operating standards were created to allow for increased adaptability and collaboration. Video platforms increased convenience and interaction across multiple geographical regions. This allowed for more real time communication and sharing of information and ideas. With that stated, this move to virtual communication was often completed without a proper assessment of related risks. This includes IT vulnerabilities and potential unauthorised actors participating in online meetings. Going forward, continuity plans must ensure tools and software used in case of extraordinary situations have undergone the necessary security assessments.

Risks surrounding digital literacy need to be addressed. While software creates vulnerabilities, the users are often the gateway to the vulnerability. It is important that when a continuity plan includes introducing alternative methods or tools to support operations, all employees have the necessary training and skills to use them. As part of the plans, there is always preventive action to ensure training is regularly being conducted and refreshed.

Digitalisation also impacted the overall policy process of government everywhere. Prior to the COVID-19 pandemic, regulations and policies were often considered to be rigid and subject to long processes that needed to be adopted. As the pandemic progressed, the urgency was high and decision-making became complex, requiring actions and policies to be adopted in real time.

Continuity planning often requires the necessity for procurement of various goods or services. The increased digitalisation experienced during COVID-19 played a large role in the government improving its processes. They were able to respond more quickly based on the urgent demands related to resolving issues related to the pandemic. Auditors need to be aware that continuity plans for any division, may allow for exceptions related to procurement controls. Understanding that even those plans must be validated by the appropriate authorities and there must be clear requirements as to when they should be acted upon. (United Nations Department of Economic and Social Affairs, 2022[12])

Impact of digitalisation on the internal audit function

Integrated assurance is defined as *the framework which enables an organisation to maximise the coverage of assurance in a coherent and coordinated manner by avoiding duplication or gaps across control functions*. Integrated assurance has the potential to become the new normal in the digital age. There is a wealth of capability for end user analysis and monitoring that will enable stronger first and second lines of defence, with much more automated, real-time assurance. Internal audit will need to differentiate and

articulate its third line role, or a new role, very clearly in order not to become obsolete or ineffective. Organisational data sometimes masks useful stories about control effectiveness, risk management, ethical behaviour, performance and financial stability. Identifying these areas and describing them in a manner that captures the interest of senior management will differentiate the assurance providers of the future. (Chartered Institute of Internal Auditors, 2023[13])

While the traditional role of auditors is to provide assurance on controls and not to provide consultation to the auditee on their topic of expertise, it may be useful to do so in the context of business continuity planning. With the rate of technological development, the following themes should be at the forefront and considered in the context of forward thinking in the digital environment, collaboration, connectivity and communication. (Chartered Institute of Internal Auditors, 2023[13])

In the ever-evolving landscape of digital technologies, public sector organisations face the critical challenge of adapting to changes while ensuring uninterrupted service delivery. Internal audits play a vital role in assessing these organisations' preparedness and resilience against digital disruptions. The digital era has ushered in a transformative wave across the public sector, compelling organisations to integrate advanced technologies and digital processes. This integration, while beneficial, introduces complexities and challenges, particularly in maintaining service continuity amidst rapid technological changes. Internal audits, therefore, must adapt their methodologies to assess the organisation's agility, resilience, and preparedness in this digital landscape effectively. Therefore, one of the main objectives of internal audit is to evaluate the organisation's framework and capabilities for managing changes in digital technologies and processes, ensuring the continuity of public services. This involves scrutinising the strategic alignment of digital initiatives, the robustness of IT infrastructure, and the effectiveness of risk management practices in the face of digital transformations.

Auditors should begin with a comprehensive review of the organisation's risk assessment and management strategies concerning digital technologies. This includes evaluating the processes for identifying, analysing, and mitigating risks associated with digital transformation and how these processes are integrated into the broader organisational risk management framework.

Collaboration

The digitalisation of organisations has created a shift towards a more collaborative culture. Areas which auditors should be aware of include:

- Data governance: as hard file systems are replaced with cloud-based networks, their controls, particularly surrounding access, must be strong.
- Dependency: as organisations often rely on third party platforms to be a part of their operations, there must be proper controls in place to maintain continuity and supplier management.
- Internal controls: as changes are made to all aspects of an organisation there should be a necessary update to respective internal controls, as it is important, that they remain relevant and effective.
- Culture: changes in technology occur much quicker than cultural change. As technology may present opportunities for greater synergy, functions and management working in a silo type manner will pose a risk to operational success.
- Misinformation: as information is shared via wikis or other uncontrolled platforms in organisations, it is important that auditors and decision makers understand the critical risks surrounding this.
- Innovation: as there is pressure for organisations to innovate, auditors must be able to advise upon the risk/reward of those disruptions without hindering any sort of innovation.

Connectivity

Digitalisation has increased the interconnected aspects of people, data and systems. Areas which auditors should be aware of include:

- Data access: the increase in data access across organisations increases the risk of data privacy and effective cybersecurity practices, by having greater non-compliance with current practices and human error.
- Assets: with greater connectivity, there is a larger volume of digital assets. This requires that both operational aspects and auditors themselves become aware of how they function, in order to better safeguard them.
- External stakeholders: depending on the government organisation and its activities, it is important that there are sufficient practices in place, as data becomes more widely accessible.

Communication

Connectivity and collaboration would not function well without effective communication. Areas which auditors should be aware of include:

- People: as organisations adapt to become digital, the focus is often placed on the technology itself. The organisation and auditors must be aware that the risks are placed with the organisational change management and with the people themselves.
- Communications: ensuring that regular education is administered to all employees for them to be aware of the protocol related to internal and external communication.

All the topics listed may be the subjects of audits themselves. They are relevant in the context of continuity plans, as well as related aspects of digitalisation. Even through all the evolution of technology and changes in operations, basic controls will always require to be audited.

The OECD Public Integrity Handbook emphasises that transparency and openness are core principles of strong governance. This can be particularly supported by making information and data more available. Box 1.1 describes it further.

Box 1.1. OECD Public Integrity Handbook (Chapter 13 – Participation)

Chapter 13.2.1: The government is open and transparent, ensuring timely and unrestricted access to information and open government data

Transparency is necessary for public integrity, as it increases the costs of concealment and fraud associated with corrupt activities. From a behavioural perspective, transparency can also reduce unethical behaviour, because the perception that one's behaviour is visible and potentially observed introduces an element of accountability that makes justifying unethical action more difficult. Open government, access to information and open government data are three critical tools that governments can use to ensure transparency and accountability.

Open Government

Open government can be defined as "a culture of governance that promotes the principles of transparency, integrity, accountability and stakeholder participation in support of democracy and inclusive growth". The key principles of an open government are detailed in the OECD Recommendation on Open Government and include:

- Transparency – the disclosure and subsequent accessibility of relevant government data and information.
- Integrity – the consistent alignment of, and adherence to, shared ethical values, principles and norms for upholding and prioritising the public interest over private interests in the public sector.
- Accountability – the government's responsibility and duty to inform its citizens about the decisions it makes as well as to provide an account of the activities and performance of the entire government and its public officials.
- Stakeholder participation – all the ways in which stakeholders can be involved in the policy cycle and service design and delivery, including through the provision of information, consultation and engagement.

Guidance as well as implementation, co-ordination and evaluation structures and mechanisms (e.g. strategies and action plans, open or digital government task forces or units, platforms or portals, databases, dashboards, toolkits, etc.) support public organisations in their daily efforts to apply open government principles.

Source: (OECD, 2020[14]).

2 Regulations and Standards

Continuity Regulation

ISO 22301 (Business Continuity Management Systems)

ISO 22301:2019[1] (Security and Resilience - Business Continuity Management Systems - Requirements) outlines the criteria for implementing, maintaining, and improving a management system to protect against, reduce the likelihood of, prepare for, respond to, and recover from disruptions when they arise.

ISO 22301 presents seven elements of BCMS, which include the Context of the Organisation, Leadership, Planning, Support, Operation, Performance Evaluation, and Improvement, as shown in Figure 2.1. ISO 22301 explicitly mentions the role of an internal auditor. The internal auditor periodically audits to ensure that the BCMS complies with the organisation's standards and ISO standards and is effectively implemented and maintained. The internal audit forms the crux of BCMS performance evaluation along with management review.

Figure 2.1. ISO 22301 Business Continuity Management Systems – Elements of standards

Context of the Organisation	Leadership	Planning	Support	Operation	Performance evaluation	Improvement
• Understanding the context of the organisation, the needs and expectations of interested parties	• management's commitment, business continuity policy and responsibilities	• BCP risks, opportunities and objectives	• resources and competence	• business impact analysis, risk assessment, BCM strategies, plans and procedures	• internal audit and management review	• corrective actions and continual improvement

Source: Revised from International Standard Organisation (ISO, 2019[2]).

OECD Recommendation on the Governance of Critical Risks

The OECD *Recommendation on the Governance of Critical Risks* encourages all organisations to ensure business continuity, with a particular emphasis on critical infrastructure operators. This can be achieved by:

- Developing standards and toolkits designed to manage risks to operations or the delivery of core services,
- Ensuring that critical infrastructure, information systems, and networks continue to function in the aftermath of a shock,

- Requiring first responders stationed in critical infrastructure facilities to maintain plans. This ensures that they can continue to perform their functions in the event of an emergency, as far as is reasonably practicable,
- Encouraging small, community-based businesses to adopt proportionate business resilience measures (OECD, 2014[4]).

Business Continuity Framework (UK and Canada)

In the UK, the Civil Contingencies Act 2004 was enacted to establish a framework for civil protection in emergency situations. This Act requires frontline responders to maintain internal Business Continuity Management (BCM) arrangements and local authorities to promote BCM to commercial and voluntary organisations. The central government offers a BCM toolkit to help individual institutions effectively establish their BCPs. The toolkit contains information on assigning responsibilities, setting up and implementing BCM within an organisation, and continuous management, as outlined in Box 2.1.

Box 2.1. The UK's Business Continuity Management Toolkit

Effective programme management ensures the establishment and maintenance of BCM capability within your organisation. This process consists of three steps.

Assigning Responsibilities

- Appoint an individual at the management board level to be accountable for BCM.
- Assign one or more individuals the responsibility of advancing the programme.

Establishing and Implementing BCM in the Organisation

- The scope, aims, and objectives of BCM in the organisation.
- The activities or "programme" required to deliver these.
- Communicating the programme to internal stakeholders.
- Arranging appropriate training for staff.
- Ensuring activities are completed.
- Initially exercising the organisation's BCM arrangements.

Ongoing Management

- Regularly review and update the organisation's BCPs and related documents.
- Continue to promote business continuity across the organisation.
- Administer the exercise programme.
- Keep the BCM programme updated through lessons learned and good practice.

Source: (UK Government, n.d.[15])

Box 2.2. Business Continuity Management Strategies in the UK's Toolkit

PEOPLE

- Inventory of staff skills not utilised within their existing roles - to enable redeployment
- Process mapping and documentation - to allow staff to undertake roles with which they are unfamiliar
- Multi-skill training of each individual
- Cross-training of skills across a number of individuals
- Succession planning
- Use of third-party support, backed by contractual agreements
- Geographical separation of • individuals or groups with core skills can reduce the likelihood of losing all those capable of undertaking a specific role

PREMISES

- Relocation of staff to other accommodation owned by your organisation such as training facilities
- Displacement of staff performing less urgent business processes with staff performing a higher priority activity. Care must be taken when using this option so that backlogs of the less urgent work do not become unmanageable.
- Remote working – this can be working from home or working from other locations
- Use premises provided by other organisations, including those provided by third-party specialists
- Alternative sources of plant, machinery and other equipment

TECHNOLOGY

- Maintaining the same technology at different locations that will not be affected by the same business disruption
- Holding older equipment as emergency replacement or spares

INFORMATION

- Ensure data is backed-up and it is kept off-site
- Essential documentation is stored securely (e.g. fireproof safe)
- Copies of essential documentation are kept elsewhere

SUPPLIERS AND PARTNERS

- Storage of additional supplies at another location
- Dual or multi-sourcing of materials
- Identification of alternative suppliers
- Encouraging or requiring suppliers/partners to have a validated business continuity capability
- Significant penalty clauses on supply contracts

STAKEHOLDERS

- Mechanisms in place to provide information to stakeholders
- Arrangement to ensure vulnerable group

Source: (UK Government, n.d.[15]).

The Business Development Bank of Canada (BDC) which is wholly owned by the Government of Canada developed steps to plan for an emergency and disaster plan. These steps apply to a natural disaster, any type of accident or an unforeseen event that would disrupt business operations. Through all scenarios, government activities must be able to continue. Box 2.3 describes the steps which should be taken.

Box 2.3. Business Development Canada's steps for planning an emergency and disaster plan

The following describes steps to be taken to plan for an emergency and disaster.

- Establish an emergency preparedness team.
- Identify essential services and functions.
- Identify required skill sets and staff reallocation.
- Identify potential issue(s).
- Prepare a plan for each essential service/function.
- Compare with "preparedness checklist".
- Review with the emergency preparedness team.
- Revise, test and update the plan.

Source: (Business Development Canada, n.d.[16]).

Continuity Regulation in Poland

Within the European Union, the 2022 EU Directive 2022/2557 on the Resilience of Critical Entities[2] article 13 states that: Member States shall ensure that critical entities take appropriate and proportionate technical, security and organisational measures to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment. This includes item (d) which states measures necessary to: recover from incidents, duly considering business continuity measures and the identification of alternative supply chains, in order to resume the provision of the essential service. (European Union, 2022[17])

In Poland, regulations such as the Regulation on the National Interoperability Framework, the General Data Protection Regulation, the Regulation on the Public Information Bulletin, and the Code of Administrative Procedure stipulate the obligation to provide uninterrupted public services. For instance, Article 8 of the Public Code of Administrative Procedure stipulates that administrative bodies should conduct proceedings in a way that inspires confidence in public authorities. This is guided by the principles of proportionality, impartiality, and equal treatment. According to Article 12, Section 1 of the same Code, public administration bodies should act carefully and promptly, using the simplest possible means to resolve matters. Furthermore, Article 35, Section 1 states that public administration bodies are obliged to deal with matters without undue delay. Also, other specific regulations, for example the Act on National Cybersecurity System, should be considered while planning and performing public service continuity audits.

The internal control standards for the public finance sector require that the head of every public finance sector entity ensure mechanisms to maintain its continuity of operation. In addition, the minister managing a branch of government administration and the head of a local government unit is also responsible for the functioning of internal control – including the responsibility for maintaining continuity – at the level of the whole government administration branch or the whole local government, respectively. For example, the Ministry of Finance, through the Regulation of the Minister of Finance on Business Continuity Management

Policy on 24 February 2022, requires the Ministry of Finance and its subordinate agencies to establish a BCP and provides the policy for the planning and implementation of BCM. Business Continuity Management Policy of the Minister of Finance is based on the ISO 22301 and its essential elements are shown in Box 2.4.

Box 2.4. Business Continuity Management Policy in Poland's Ministry of Finance

The Business Continuity Management Policy carries out the following procedures:

1. Define the roles of individual employees and assign them tasks and responsibilities.
2. Identify the processes and their connections. Specify the main and supporting processes of the organisation.
3. Conduct a Business Impact Analysis (BIA) to identify critical processes.
4. Perform a risk analysis for these critical processes.
5. Develop a business continuity strategy.
6. Formulate BCPs.

The purpose of BIA is to identify vital processes and resources required to sustain or resume these processes, as well as to determine the effects of disrupting these processes during specific time periods. BIA should include key indicators, Recovery Time Objective, and Recovery Point Objective.

The policy explicitly states that the BCMS is influenced by the development and implementation levels of other related systems. In other words, it implies that the BCMS should operate properly with IT security, information security, physical security, crisis management, and protection of personal data.

Notes

[1] This standard is also available in Polish version: PN-EN ISO 22301:2020-04.

[2] Repealing Council Directive 2008/114/EC

3 Audit Attributes

Selecting Audit Type

BCP audit aims to assess the effectiveness, efficiency, and adaptability of continuity plans. Therefore, a BCP audit can be classified as a performance audit. This means that the main parts of the guidelines for performance audit can be applied to a BCP audit. A BCP audit can be part of a more extensive audit that also covers compliance and financial auditing aspects. Where appropriate, the impact of the regulatory or institutional framework on the performance of the audited entity should also be considered. (INTOSAI, 2019[18])

Timing and Resources

ISO 22301 necessitates regular internal audits for BCP. A risk assessment is essential to ascertain the optimal timing for an audit. If BCP has been newly implemented or if known issues exist, more frequent audits may be required. The scheduling of BCP audits should account for risk factors such as resources for BCP implementation, leadership's support, the operational environment, and IT operations' stability and security.

When planning the audit, it is crucial to pragmatically consider time schedules and resource demands. Such an approach ensures the audit process is economical, efficient, effective, and timely, aligning with solid project management principles. Audits are often viewed as projects, involving the planning, organisation, securing, management, leadership, and control of resources to reach specific objectives.

The primary focus should be:

- Establishing practical time schedules for each task, based on the planned methodology and other pertinent factors such as internal audit procedures, previous audits, stakeholder views, expected access to information, and resource availability.
- Identifying and co-ordinating an adequate number of resources, including auditors, supervisors, and stakeholders, to fulfil specific tasks within the expected time frames, factoring in team competence.
- Calculating expenses related to travel, training, equipment, external subject matter experts, and other incidental costs. Typically, internal staff resources are budgeted in terms of workdays and monitored via an internal system.

Objectives

The objectives of BCP focus on assessing the effectiveness, efficiency, and adaptability of continuity plans, particularly in response to digital challenges. This includes: (US GAO, 2014[19]) (INTOSAI, 2016[20]) (IIA, 2019[21])

- Providing assurance that public services have the necessary operational resilience to quickly recover from various disruptions, such as cyber-attacks and IT failures.

- Verifying compliance with relevant laws, regulations, and standards related to continuity planning and digital security during extraordinary times, ensuring that public services meet mandatory requirements.
- Assessing the effectiveness of risk management practices in identifying, evaluating, and mitigating risks associated with digitalisation, including cyber risks and data privacy concerns.
- Evaluating to determine if the resources allocated for continuity planning, including financial, human, and technological resources, are used efficiently and effectively to support resilience objectives. This includes contingency funds and discussing if items are appropriately funded.
- Examining whether the BCP covers all related risks if part of the public service is privatised (if applicable).

Box 3.1. Example of Relevant Audit Objective

Auditor General of Australia – Business Continuity Management (2014)

- Objective: The objective of the audit was to assess the adequacy of selected Australian Government entities' practices and procedures to manage business continuity. To conclude against this objective, the Australian National Audit Office (ANAO) adopted high-level criteria relating to the entities' establishment, implementation and review of business continuity arrangements. The ANAO assessed the BCM framework and approach, including key documentation (such as BCM policy and BCPs), entity responses to actual events, BCM exercises and testing activities, and monitoring and review.

Source: (ANAO, 2014[22]).

Scope

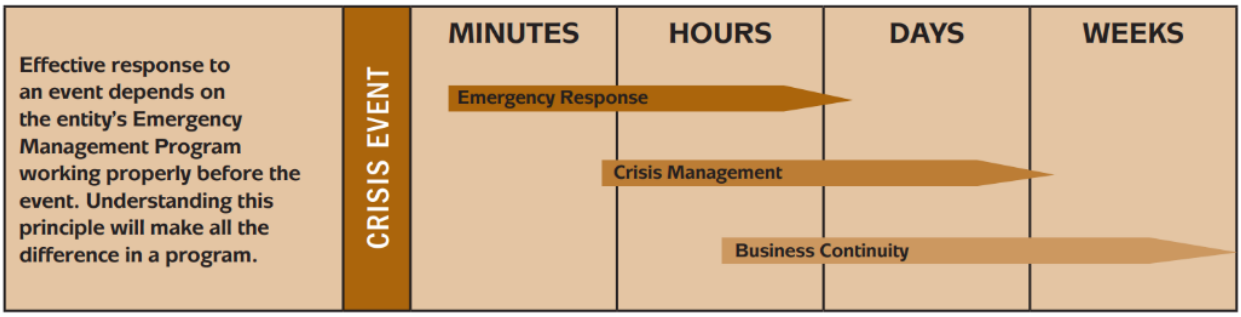
The scope defines the parameters of the audit. It addresses the ultimate questions and the type of review the auditor must complete. It will define the topic that will be assessed/reported upon, the documents/records to be reviewed, the time period under consideration and the locations (if any) to be examined. The scope is clearly impacted by the objectives (and questions) of the audit. It is important to note that any modifications to the objectives may also then impact the scope. The creation of the scope of the audit is an important part of audit design. The scope of the audit may be established by answering a series of questions. This will help properly define them. There should also be additional considerations in the determination of the audit scope. These will vary by each organisation. These include but are not limited to:

- availability of reliable data and sources of information
- internal resources to conduct the audit
- accessibility of auditors with the appropriate skill sets
- accessibility to subject matter experts (as needed)
- costs associated with the audit (i.e. travel or other operational needs)
- time limitations of the audit
- any other item or topic which may impact the coverage of the audit.

The scope of the audit can also include potential topics which were part of recommendations of a previous audit report (if deemed to be pertinent and relevant). (INTOSAI, 2019[18])

As described by the IIA, BCP may be considered part of crisis management measures but each country may define and distinguish it in their own way.[1] Defining the concept in a narrower fashion, along with Emergency Response (ER) and Crisis Management (CM), may help clearly set the scope of the BCP audit as shown in Figure 3.1. ER refers to the initial response to minimise the damage to life, facilities, and assets caused by a crisis or disaster and to mitigate the impact of the crisis. For example, it includes measures such as isolating infected individuals during a pandemic, preventing the spread of infection among employees, and taking evacuation and facility protection measures in the case of a physical disaster. ER should be completed within minutes to hours after a crisis occurs. CM focuses on maintaining the organisation's function after a crisis. For example, it involves restoring essential functions to maintain the organisation, such as communication between management and employees, communication with citizens, and service networks. Therefore, CM occurs within days after a disaster. BCP focuses on minimising service interruptions caused by disasters and maintaining essential service functions. Therefore, BCP takes place over several days or weeks after a disaster, and depending on the situation, it can last even longer. (Everest et al., 2008[23])

Figure 3.1. Differences among Emergency response, Crisis Management and Business Continuity



Source: (Everest et al., 2008[23])

Box 3.2. Examples of Relevant Scope

Public Health Agency of Canada: Audit of Business Continuity Plans for Critical Services (2022)

- Scope: The scope of this audit included a review of a sample of BCPs from the critical services category of Emergency Preparedness and Response against Infectious Disease. The audit did not include a review of the management of BCPs, and their related databases, nor of the appropriateness of templates and Business Impact Assessments. We examined whether Health Canada and Public Health Agency of Canada had up-to-date BCPs to enable continuity of services in the current environment, regardless of the format of these plans.

Indigenous and Northern Affairs Canada: Audit of Business Continuity Planning (2017)

- Scope: The audit scope focused on assessing the governance framework (i.e. policies and accountabilities, as well as the roles and responsibilities and monitoring and oversight in place to implement the BCP Program), the development of BCPs, the readiness and awareness of department's BCP Program, and the management controls in place to ensure that Indigenous and Northern Affairs Canada has the capacity to deliver the BCP Program in compliance with applicable legislation and policies.

Public Safety Canada: Audit of the Business Continuity Planning Program (2016)

- Scope: The scope of the audit included an examination of the Department's business continuity

planning programme governance and risk management arrangements as well as the adequacy of the continuity plans. This included the BCPs for the Government of Canada and the Canadian Cyber Incident Response Centre and related supporting documents as of March 2016. The audit scope excluded the Department's emergency management plans, response frameworks and protocols in place to lead, inform, facilitate and co-ordinate an integrated federal response to a threat or emergency.

Source: (Health Canada, 2022[24]) (Indigenous and North Affairs Canada, 2017[25]) (Public Safety Canada, 2016[26])

Risk Assessment

Risk assessment is necessary for deriving audit criteria and establishing audit strategies. Internal auditors need to identify risks related to the establishment and implementation of BCP at the audit planning stage and evaluate the organisation's risk management activities regarding these risks.

The following are examples of risk categories in BCP and digitalisation.

- The organisation has not established a BCP.
- The BCP is not properly documented - compliance issue.
- The BCP is incomplete (e.g. ineffective/incomplete test,[2] low feasibility, lack of clarity on responsibility, missed stakeholders, and missing outsourced supplies).
- The staff has low awareness of BCP and BCP training is not sufficient.
- Low support from management.
- Lack of skilled staff to implement plans (e.g. staff is not familiar with digital tools or processes).
- BCP does not have enough effect even with a full implementation.
- Known risks or weaknesses are not properly addressed.
- There is a better way to do it with fewer resources in terms of efficiency and economy.
- Risks related to suppliers or contractors.

Criteria

The criteria are developed to measure the organisation's performance against expectations. Criteria are benchmarks which are used to evaluate the topic. As in all internal audits, criteria may be quantitative and/or qualitative. The criteria may be general or specific, focusing on what should be according to laws, regulations, or objectives; what is expected, according to sound principles, scientific knowledge and best practice; or what could be (given better conditions). It should describe the areas the auditee will be assessed against.

Typically, the criteria would be developed and communicated during the planning phase to encourage their acceptance, but more complex audits such as a public service continuity plan may create a situation where they are defined later in the audit process. It may be complex as a public service continuity plan may always be evolving due to various aspects of the organisation.

As part of the design phase, it is important for the internal audit function (IAF) to discuss the audit criteria with the auditee. This level of collaboration will help to ensure there is a shared and common understanding of the criteria that will be used as benchmarks (during the evaluation of the audit area). It will also provide feedback on their applicability and legitimacy. Involving the auditee may also increase the likelihood that they will agree with the findings and recommendations. While transparency is necessary, it will be the

ultimate decision of the IAF to determine the appropriate audit criteria based on the type of audit. (INTOSAI, 2019[18])

It is important to that when defining objectives and criteria for auditing public service continuity plans, there are several topics which are relevant across all organisations. The following areas may be considered when developing criteria: (ISO, 2019[2]; US NIST, 2020[27]; ISACA, 2024[28])

- Continuity plans align with the organisation's overall strategic objectives and digital transformation goals, ensuring it supports the mission-critical services most important to stakeholders.
- Continuity plans are based on a comprehensive risk assessment that includes digital risks, identifying potential threats to service continuity and the impact of those threats.
- Third-party suppliers and partners, especially those providing digital services, should be assessed to ensure they do not become a weak link in the continuity planning. Ensure this is included as testing when assessing each supplier, software, provider, etc.
- Mechanisms for continuously monitoring, reviewing, and improving the continuity plan, incorporating lessons learned from exercises, incidents, and changes in the digital landscape.

Those criteria address the overarching topic of continuity planning. The following should be considered when developing operational or technical criteria and/or sub-criteria: (FEMA, 2010[29]; CISA GOV, 2024[30])

- Include the presence of clear incident response and recovery procedures that are regularly tested and updated, ensuring rapid restoration of services with minimal disruption. This can encompass all activities of an organisation.
- Evaluate the adequacy of IT infrastructure and technology solutions in supporting continuity plans, including data backup, recovery solutions, and cybersecurity measures; ensuring that usual organisational activities can continue with minimal disruption.
    - Cybersecurity Measures: assessing the robustness of cybersecurity defences in protecting digital public services.
    - Interoperability and System Integration: the capacity for seamless service delivery across different digital platforms and systems.
    - Data Protection and Privacy: the continuity plans address data protection laws and privacy considerations.
- Assess if employees are adequately trained and aware of their roles in the continuity plan, with special attention to digital literacy and cybersecurity awareness to mitigate digital risks effectively. This will include regular updating of roles and responsibilities.
- Identify if effective communication plans are in place to inform stakeholders, including the public and partner organisations, during and after an incident, maintaining transparency and trust. The overall strategy and process of the communication plan may be incorporated into a holistic lesson learned process.

Box 3.3. Examples of Relevant Audit Criteria

Public Health Agency of Canada: Audit of Business Continuity Plans for Critical Services (2022)

- Criterion 1: The Department and Agency have developed BCPs to ensure the continuity of their critical services and critical support services and these are tested and kept current for identified critical services.

Conducted in 2022, this criterion was the sole one for this audit. As the agency was one of the leading ones in the national response to the pandemic, risks were continually emerging and evolving. As the working environment has changed drastically, continuity plans had been outdated. This increased the risk of non-continuity in critical services (pending further disruption). The ultimate intention of the audit was to provide assurance that: *the Department and Agency have maintained up-to-date BCPs during the pandemic*.

Indigenous and Northern Affairs Canada: Audit of Business Continuity Planning (2017)

- Criterion 1: Governance Framework
  - A departmental BCP Program is in place with appropriate and clearly defined objectives, roles, responsibilities, and accountabilities.
  - Important aspects of other continuity programmes, including Information Technology (IT) security, incident management, and internal emergency management are effectively integrated into the BCP Program.
- Criterion 2: Development of BCPs
  - There are appropriate and adequate management controls in place to support the development of BCPs.
- Criterion 3: BCP Program Readiness and Awareness
  - There are appropriate and adequate management controls in place to support the maintenance of BCPs.
  - There are appropriate and adequate management controls in place to support the readiness of BCPs.
  - There are appropriate and adequate management controls in place to promote awareness of BCPs.
- Criterion 4: BCP Program Resources
  - There are appropriate and adequate management controls in place to maintain the capacity necessary to deliver the BCP Program in compliance with applicable legislation and policies.

Conducted in 2017, the audit was a high priority for the department as recent events required the use of continuity plans.

Public Safety Canada: Audit of the Business Continuity Planning Program (2016)

- Criterion 1: A governance framework is in place that is integrated with the Federal Emergency Response Plan and includes approved descriptions of roles, responsibilities, policies, oversight committees and resources.
- Criterion 2: A BIA exists that clearly identifies critical business services integral to keeping the business functioning during an incident and to determine the recovery requirements and priority of the critical services to be recovered.

- Criterion 3: Business continuity and recovery strategies have been identified, assessed, selected and approved, and BCPs are consistent with policy, government standards and guidelines.
- Criterion 4: BCPs are subject to testing and validation, which includes the preparation of lessons learned reports and the updating of BCPs after testing activities or actual events to reflect lessons learned and to account for changes to the Department and its operating environment.

Conducted in 2016, this audit was a result of a BIA which occurred 5 years prior. The analysis identified the main critical service of the department to be the management of the integrated federal response to emergencies provided by the Government Operations Centre. Following that a BCP was created in 2013. 3 years later the next version was created and was the catalyst of the audit to be conducted.

Source: (Health Canada, 2022[24]; Indigenous and North Affairs Canada, 2017[25]; Public Safety Canada, 2016[26]).

Involvement of Stakeholders

Engaging both internal (including internal audit team management and members) and external stakeholders is crucial for effectively planning and conducting an audit. The development of a fitting audit plan is contingent on the extent of communication with internal stakeholders. The audit plan should be a collaborative effort among internal stakeholders. It is beneficial for all audit team members to converse and reach a consensus on the audit plan, the design matrix, the project timeline, and other selected tools. As the audit unfolds, it is critical to keep the communication channels open, and management should strive to implement the audit plan. The chosen tools should promote continuous involvement from stakeholders and management.

Initiating communication with external stakeholders, like the auditee, during the planning phase and maintaining it throughout the process is essential. All elements, including the subject, objective, criteria, questions, etc., should be discussed. This will provide a transparent overview and clarify potential impacts on the auditee. Although there should be a relationship, the auditee will not be able to influence the audit process. The goal is to foster a collaborative and positive interaction.

In a BCP audit, the following stakeholders may be involved:

- Leadership.
- Crisis management control tower.
- Risk Management function.
- Digital, IT operations functions, IT security and Data protection office.
- BCP planning and maintenance managers.
- Resource managers for implementing BCP.
- Facilities (building, office, infrastructure) maintenance function.
- Business operations managers in each department/division/unit.
- Training function related to BCP.

BCP Audit Checklist

When a BCP audit adopts a system-oriented approach, a checklist can be utilised effectively. This type of audit, focused on assessing the performance of management systems, answers a wide range of questions as shown in Box 3.4. These questions detail how activities function, identify any weaknesses and evaluate the potential for improvement.

Box 3.4. Checklist for BCP Audit

BCP Program Governance

1. A departmental BCP Program is in place with appropriate and clearly defined objectives, roles, responsibilities, and accountabilities.

1.1. Adequate BCP policy, operational security standards and technical documentation are developed within the department or adapted from Government of Canada policy. BCP policy has been approved by senior management and describes key roles and responsibilities for managing the organisation's BCP activities, and the organisation`s approach to conducting BIAs, developing plans and arrangements, and maintaining readiness.

1.2. The Departmental Security Officer (DSO) directs and coordinates the BCP Program.

1.3. A Departmental BCP Coordinator has been formally appointed to fulfil roles and responsibilities established in the Operational Security Standard – Business Continuity Planning Program.

1.4. A BCP working group has been appointed by senior management, has had appropriate roles and responsibilities defined, meets regularly and presents to the Executive Committee on a regular basis.

1.5. The Departmental BCP Coordinator maintains regular communication on, and coordination of, BCP activities with the IT Security Coordinator and DSO.

2. Senior management actively and appropriately supports the development and implementation of the BCP Program.

2.1. Senior management is responsible for supporting, overseeing, directing, approving and funding the development, implementation and testing of the Business Continuity programme, policy, plans, activities and arrangements.

2.2. Sufficient financial and other resources are committed to BCP.

Business Impact Analysis

3. The department's business and critical services have been identified and a Business Impact Analysis conducted.

3.1. Processes exist to determine the nature of the department's business (e.g. role, mandate) and the services it must deliver according to its constituent or other legislation, government policy, obligations to other departments, and service sharing arrangements, treaties, contracts, memoranda of understanding or other agreements.

3.2. Critical services have been identified and prioritized based on: Minimum Service Levels (MSL); Maximum Allowable Downtimes (MAD); Recovery Point Objectives (RPO); and Recovery Time Objectives (RTO).

3.3. A recent threat and risk/vulnerability assessment has been performed for critical services to identify and assess: All potential sources of disruption; The direct and indirect impacts of disruptions on the department; Degrees of injury to Canadians and the government in the event of their disruption.

3.4. Dependencies that support critical services directly or indirectly, both internally and externally to the department have been identified.

3.5. Senior management reviews and approves the departmental Business Impact Analysis.

BCPs and Arrangements

4. Business continuity and recovery strategies have been identified, assessed, selected and approved for each critical service.

4.1. Business continuity and recovery options have been identified for all critical services.

4.2. An assessment of each option has been performed, considering impacts on the department, benefits, risks, feasibility, capacity requirements, and cost.

5. BCPs are developed to support the implementation of approved strategies and are consistent with policy requirements.

5.1. BCPs are developed identifying: Critical services, information assets, and dependencies identified in the Business Impact Analysis; Approved continuity and recovery strategies; Measures to deal with the impacts and effects of disruptions on the department; Response and recovery teams, including membership and contact information; Roles, responsibilities and tasks of the teams, including internal and external stakeholders, and clearly identify organisational authorities and replacements; Resources and procedures for continuity of service; Coordination and reporting mechanisms and procedures, including processes to liaise with other departments, agencies and first responders as necessary to coordinate BCP; Authority for activation of BCP; Emergency Operation Centres at all levels (local, regional and national); and Procedures for evacuation and sheltering in place.

5.2. All single points of failure have been identified and addressed in BCPs.

5.3. Adequate communications plans and materials are developed to support crisis communications with employees, business partners, vendors, government, external media and other key stakeholders.

5.4. Senior management reviews, approves and funds selected continuity plans, including review and approval of third-party plans.

5.5. BCPs are available in a readily accessible location(s) and format(s) in the event of a disruption.

6. Arrangements are completed to ensure that plans can be put into effect, and where necessary, formal contracts or MOUs are in place.

6.1. All necessary arrangements have been completed and formalized to ensure that plans can be put into effect, and where necessary, contracts or MOUs are in place to formalize arrangements and establish priorities for access amongst competing interests.

6.2. Where departments and/or third parties share in the delivery of a critical service, arrangements exist to ensure that the plans of the sharing departments are concerted.

Maintenance of BCP Program Readiness

7. An effective training and awareness programme for BCP is in place.

7.1. The Departmental BCP Coordinator has been appropriately trained to undertake the functions and responsibilities assigned.

7.2. An appropriate BCP training (including cross-training) and awareness programme is in place, is documented, includes a training and awareness plan, and has been delivered to all levels of the organisation.

7.3. BCP training (including cross-training) and awareness are continually reinforced, periodically verified and validated.

8. BCPs are reviewed and updated on a regular basis.

8.1. Processes exist to ensure BCPs are updated and validated for any changes such as contact lists,

new programmes, strategic planning frameworks, legislative changes, and physical relocations and reviewed annually by management and the BCP Coordinator.

8.2. An up-to-date inventory of critical services and associated information, assets and dependencies are maintained and provided to Public Safety Canada as requested.

9. BCPs are regularly tested and validated through exercises to ensure efficient and effective response and recovery.

9.1. Testing and validation of all plans occurs on a regular basis and includes stress testing and exercise documentation.

9.2. An After-Action Report and action plan are prepared following all exercises and any disruptions, and action plans have been approved by senior management and implemented.

9.3. BCPs are revised to reflect lessons observed.

10. Where identified as necessary, Emergency Operations Centres (EOCs) and alternate sites are supplied and maintained in a ready state.

10.1. Procedures exist to ensure emergency supplies and resources are acquired and maintained for EOCs and alternate sites.

11. The Departmental BCP Coordinator monitors all activities of the BCP Program, including BIAs, BCPs, exercises, After Action Reports, and training and awareness programmes.

11.1. The Departmental BCP Coordinator reviews all BIAs to ensure completeness of justifications and specifications (MSLs, MADs, RTOs, and RPOs).

11.2. The Departmental BCP Coordinator reviews all BCPs to ensure completeness and currency of content.

11.3. The Departmental BCP Coordinator reviews all exercise materials and After-Action Reports for appropriateness and completeness.

11.4. The Departmental BCP Coordinator monitors training and awareness activities to verify they have been delivered as scheduled.

Source: Modified from Public Safety Canada (2016[26]), Audit of the Business Continuity Planning Program, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-bsnss-cntnty-plnnng-prgrm/2016-bsnss-cntnty-plnnng-prgrm-en.pdf.

Recommendations

As similar to general audit principles, the connection between the findings, conclusions, and recommendations must be sufficiently understood. It is vital that recommendations are developed to correct deficiencies in the organisational BCP. The implications of the BCP will be significant and therefore, they should be specific, measurable, attributable, relevant and time bound. They should address the causes of the deficiencies and support in improving the programmes, operations, and performance. Generally, recommendations should be aimed at eliminating or reducing the deviation between the evidence and audit criteria. (INTOSAI, 2019[18]) Box 3.5 describes an example of a relevant recommendation pertaining to an audit of BCM.

Box 3.5. Example of Relevant Recommendations

United Nations Joint Inspection Unit – Business Continuity Management in United Nations System Organisations (2021)

- Recommendations:
  - Review their BCM framework and ensure that the core elements identified in the present report are established and owned by relevant stakeholders to enable effective co-ordination of business continuity processes and practices, build coherence in their implementation and promote accountability at all levels.
  - Ensure that the maintenance, exercise and review components of their BCPs are applied through a consistent and disciplined approach to confirm that the plans remain relevant and effective.
  - Strengthen their learning mechanisms to contribute to organisational resilience by requiring after-action reviews following disruptive incidents and periodic internal management reviews of their BCM frameworks.
  - Report to their legislative organs and governing bodies on progress towards the implementation of the policy on the organisational resilience management system and its revised performance indicators, and highlight good practices and lessons learned, especially in the area of BCM.
  - Conduct an internal management assessment of the continuity of business operations during the COVID-19 pandemic to identify gaps, enablers, good practices and lessons learned and adjust policies, processes and procedures, in particular in areas such as human resources, information and communications technology management and occupational safety and health, and indicate necessary measures to better prepare for and respond to future disruptive incidents.
  - Should consider, at the earliest opportunity, the conclusions of the internal management assessment of the continuity of operations during the COVID-19 pandemic prepared by the executive heads of their respective organisations and, on that basis, take appropriate decisions to address the identified gaps and risks and to ensure continuity of business operations.

Source: (UN JIU, 2021[31]).

Reporting

General audit report principles can be applied to the reporting of a BCP audit. An audit report should be comprehensive, convincing, timely, reader-friendly, and balanced. It should include all necessary information to address the audit objective and questions, present a convincing argument, be issued in a timely manner, be written in simple and clear language, and present audit evidence in an unbiased manner. As described in the Regulation,[3] the report structure should include the following sections: subject/purpose, scope, start date, findings/assessment according to criteria, recommendations, possible reservations, assessment of the respective internal controls, date and name(s) of internal auditor (including signature(s)). Quality control procedures should be integrated into the audit process to ensure consistency and accuracy. The audit findings should be discussed with the auditees before finalising the report. With that collaboration, the recommendations will be finalised, and the report should be distributed to all relevant stakeholders.

With regard to a BCP audit report, the following should be noted:

- Ensure the audit report is timely. Given the rising risk of crises, it is crucial to get the timing right.

- As the BCP is part of the crisis management package, make sure the audit recommendations are clear and actionable.
- Make sure to include a detailed overview of digital risks and their potential impact on business continuity.
- Highlight any gaps in the organisation's digital risk management and recommended improvements.
- Make sure to include the BCP's adaptability to changes in the operational environment, including changes in IT operations, cyber threats, and digitalisation.
- Make sure to include an examination of the efficiency and effectiveness of resource allocation related to BCP, including financial, human, and technological resources.
- Make sure to include an evaluation of the BCP's compliance with relevant laws, regulations, and standards, particularly in times of crisis.

Competencies Supporting Auditors in Digitalisation

There are several competencies required to support auditors in the digital age. Whether the subject matter is public service continuity plans or other related topics, internal audit functions must ensure their auditors have the necessary knowledge and skills to perform the audits and other assurance reviews effectively. Possible skills that must be particularly emphasised include: (Chartered Institute of Internal Auditors, 2023[13]):

- Agile: digital transformations are occurring in all programmes in all government. All auditors need to be able to work in an environment that is adaptable. All involved must be willing to learn as it evolves.
- Analysis: it is integral that auditors are knowledgeable on root cause analysis techniques (e.g. five whys, fault tree analysis, etc.). It is a core audit skill which is used to derive the key elements of audit issues.
- Coding: having skills related to coding should no longer be an asset qualification but instead should be a minimum-level requirement. Basic coding becomes an essential skill for talking to information technology and other new entrants to the workforce.
- Facilitation: in the digital age, collaboration is an important skill which is needed. This includes management of online meetings, small groups and/or workshops. These interpersonal skills are necessary for all auditors going forward in an environment which includes virtual meetings.
- Initiative: work environments are changing across the world. Auditors physically being around colleagues on a different day (through hybrid and teleworking models), should allow for their skills to be utilised when having in-person meetings with auditees, observing practices and learning about cultural insights.
- Presentation: having the capability to communicate and present information to groups is essential for auditors. As the concept of reporting is constantly evolving, being able to appropriately present information to stakeholders is a necessary skill for all auditors.

Notes

[1] For instance, in Poland, Article 2 of the Act on Crisis Management defines crisis management as including "[…] crisis prevention and preparation to take control over them through planned actions, reacting in the event of occurrence crisis situations, removing their effects and restoring resources and critical infrastructure.

[2] Examples of possible tests may include staffing (e.g. increased workloads, processing of transactions, and other operational specific processes), technology (e.g. testing back and recovery process of data, systems, applications and networks) and facilities (e.g. environmental factors, backup power and physical security).

[3] § 18 - Regulation of the Minister of Finance on internal audit and information on this audit work and results

References

ANAO (2014), *Business Continuity Management*, https://www.anao.gov.au/sites/default/files/ANAO_Report_2014-2015_06.pdf (accessed on 26 April 2024). [22]

Business Development Canada (n.d.), *8 steps for planning your emergency and disaster plan*, Strategy and Planning, https://www.bdc.ca/en/articles-tools/business-strategy-planning/manage-business/business-continuity-8-steps-building-plan (accessed on 31 July 2024). [16]

Chartered Institute of Internal Auditors (2023), *Impact of digitisation on the internal audit activity*. [13]

CISA GOV (2024), *Cybersecurity Best Practices*, https://www.cisa.gov/topics/cybersecurity-best-practices (accessed on 28 April 2024). [30]

European Union (2022), *DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities*, https://eur-lex.europa.eu/eli/dir/2022/2557/oj (accessed on 13 October 2024). [17]

Everest, D. et al. (2008), *Business Continuity Management*, The Institute of Internal Auditors, https://iiabrasil.org.br/korbilload/upl/ippf/downloads/businesscontinu-ippf-00000001-24012018114224.pdf. [23]

FEMA (2023), *Federal Continuity Directive*, https://www.fema.gov/sites/default/files/documents/fema_federal-continuity-directive-planning-framework.pdf (accessed on 31 July 2024). [3]

FEMA (2010), *Developing and Maintaining Emergency Operations Plans*, https://www.fema.gov/sites/default/files/2020-05/CPG_101_V2_30NOV2010_FINAL_508.pdf (accessed on 28 April 2024). [29]

FEMA Office of National Continuity Programs (2023), *Federal Continuity Directive Continuity Planning Framework for the Federal Executive Branch*. [5]

Health Canada (2022), *Audit of Business Continuity Plans for Critical Services*, https://www.canada.ca/content/dam/hc-sc/documents/corporate/transparency/corporate-management-reporting/internal-audits/business-continuity-plans-critical-services/business-continuity-plans-critical-services-en.pdf (accessed on 31 July 2024). [24]

IIA (2024), *The Definition of Internal Auditing*, What are the Standards, https://www.theiia.org/en/standards/what-are-the-standards/definition-of-internal-audit/ (accessed on 7 February 2024). [1]

IIA (2019), *GTAG 3: Continuous Auditing: Coordinating Continuous Auditing and Monitoring to Provide Continuous Assurance*, https://www.theiia.org/en/content/guidance/recommended/supplemental/gtags/gtag-continuous-auditing/ (accessed on 28 April 2024). [21]

Indigenous and North Affairs Canada (2017), *Audit of Business Continuity Planning*, [25]

https://www.rcaanc-cirnac.gc.ca/DAM/DAM-CIRNAC-RCAANC/DAM-AEV/STAGING/texte-text/au_bucp_1513259607995_eng.pdf (accessed on 31 July 2024).

INTOSAI (2019), *ISSAI 300 Performance Audit Principles*, https://www.intosai.org/fileadmin/downloads/documents/open_access/ISSAI_100_to_400/issai_300/ISSAI_300_en_2019.pdf (accessed on 7 February 2024). [18]

INTOSAI (2016), *Disaster Risk Reduction - Business Continuity Planning (2013)*, https://intosaibc.wpengine.com/download/business-continuity-planning-2/ (accessed on 28 April 2024). [20]

ISACA (2024), *Effective IT Governance at your Fingertips*, https://www.isaca.org/resources/cobit (accessed on 28 April 2024). [28]

ISO (2019), *ISO 22301:2019 Business continuity management systems Requirements*, International Organization for Standardization, https://www.iso.org/standard/75106.html (accessed on 28 April 2024). [2]

Kuhfeld, M. et al. (2022), "The pandemic has had devastating impacts on learning. What will it take to help students catch up?", *Brookings*, https://www.brookings.edu/articles/the-pandemic-has-had-devastating-impacts-on-learning-what-will-it-take-to-help-students-catch-up/ (accessed on 13 May 2024). [8]

OECD (2024), *PISA 2022 Results (Volume IV): How Financially Smart Are Students?*, PISA, OECD Publishing, Paris, https://doi.org/10.1787/5a849c2a-en. [7]

OECD (2024), *Poland*, OECD Going Digital Toolkit, https://goingdigital.oecd.org/countries/pol (accessed on 31 July 2024). [11]

OECD (2021), *Global Scenarios 2035: Exploring Implications for the Future of Global Collaboration and the OECD*, OECD Publishing, Paris, https://doi.org/10.1787/df7ebc33-en. [10]

OECD (2020), *OECD Public Integrity Handbook*, OECD Publishing, Paris, https://doi.org/10.1787/ac8ed8e8-en. [14]

OECD (2019), *Going Digital: Shaping Policies, Improving Lives*, OECD Publishing, Paris, https://doi.org/10.1787/9789264312012-en. [9]

OECD (2014), "Recommendation of the Council on the Governance of Critical Risks", *OECD Legal Instruments*, OECD/LEGAL/0405, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0405. [4]

Public Safety Canada (2016), *Audit of Business Continuity Planning Program*, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-bsnss-cntnty-plnnng-prgrm/2016-bsnss-cntnty-plnnng-prgrm-en.pdf (accessed on 31 July 2024). [26]

UK Government (n.d.), *How prepared are you?*, https://assets.publishing.service.gov.uk/media/5a7b283de5274a34770e9d01/Business_Continuity_Managment_Toolkit.pdf (accessed on 31 July 2024). [15]

UN (2020), *The role of public service and public servants during the COVID-19 pandemic*, https://www.un.org/development/desa/dpad/publication/un-desa-policy-brief-79-the-role-of-public-service-and-public-servants-during-the-covid-19-pandemic/ (accessed on 31 July 2024). [6]

UN JIU (2021), *Business continuity management in United Nations system organizations*, https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_6_english_2.pdf (accessed on 26 April 2024). [31]

United Nations Department of Economic and Social Affairs (2022), *The Future of Digital Government: Trends, Insights and Conclusions*, https://www.un-ilibrary.org/content/books/9789210019446c010/read (accessed on 9 April 2024). [12]

US GAO (2014), *Standards for Internal Control in the Federal Government*, https://www.gao.gov/assets/gao-14-704g.pdf (accessed on 28 April 2024). [19]

US NIST (2020), *Security and Privacy Controls for Information Systems and Organizations*, https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (accessed on 28 April 2024). [27]

Glossary

Terms with definitions

Term	Definition
Business Impact Analysis	The process of determining the criticality of organisational activities and associated resource requirements to ensure operational resilience and continuity of operations during and after an organisational disruption.
Digitisation	To put information into digital form, that can be used by computers and other electronic equipment.
Digitalisation	Use of digital technologies to change an organisational model and provide new-producing activities and opportunities.
Emergency Operations Centres (EOC)	A central command and control "coordination structure" responsible for managing emergency response, emergency preparedness, emergency management, and disaster management functions at a strategic level during an emergency.
Information and Communication Technology (ICT)	The extensional term for information technology (IT) that stresses the role of unified communications and the integration of telecommunications (telephone lines and wireless signals) and computers, as well as necessary enterprise software, middleware, storage and audiovisual, that enable users to access, store, transmit, understand and manipulate information.
Maximum Allowable Downtimes (MAD)	The absolute longest amount of downtime an organisation can tolerate before facing serious repercussions.
Minimum Service Levels (MSL)	The level to which the process must be recovered during the recovery period: recovery to normal service levels can be deferred until later.
Recovery Point Objectives (RPO)	The age of files that must be recovered from backup storage for normal operations to resume if a computer, system or network goes down as a result of a hardware, programme or communications failure.
Recovery Time Objectives (RTO)	The maximum tolerable length of time that a computer, system, network or application can be down after a failure or disaster occurs.