

Introduction to Business Continuity Planning

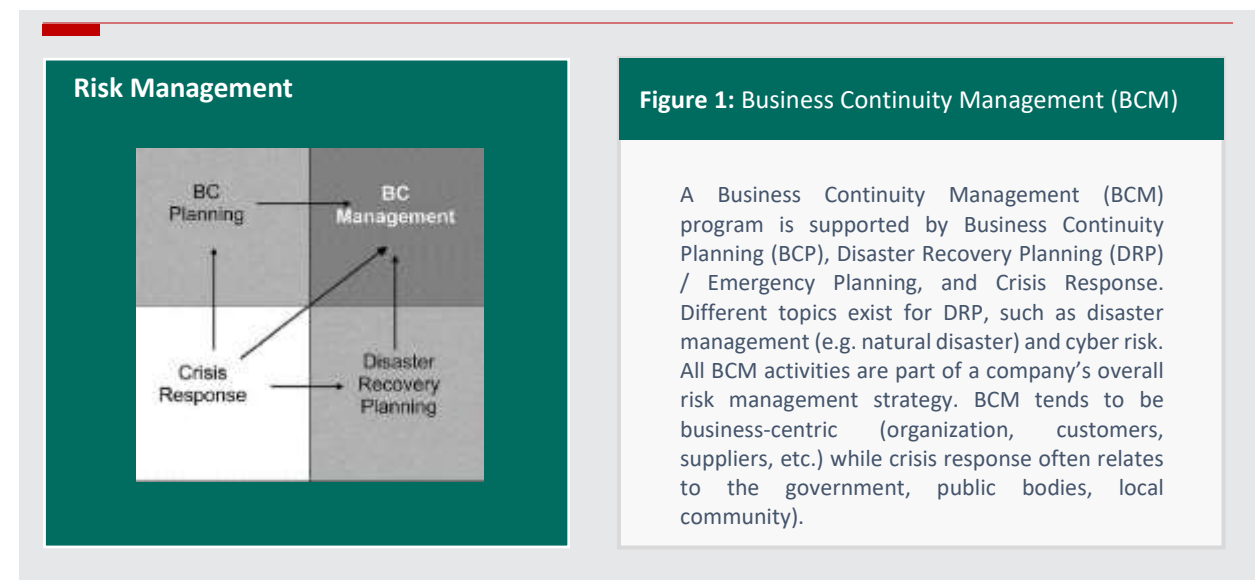
What is Business Continuity Management?

Business Continuity Management (BCM) is the framework to counter the effects of crises and interruptions¹ from external and internal risks to a business. The strategy consists of hard and soft assets for successful prevention and recovery. BCM can be part of a business' risk management (RM) strategy. The term "Business Continuity" is, according to the [ISO 22301 Standard](#), defined as the "capability of an organization to continue the delivery of products and services within acceptable time frames at predefined capacity during and after a disruption." BCM covers disaster recovery, business recovery, crisis management, incident management, emergency management and contingency planning. The following Figure² 1 shows the relationship between BCM, BCP, Disaster Recovery Planning, and Crisis Response.

What is Business Continuity Planning?

Business Continuity Planning (BCP) is a planning process that is part of BCM. The main purpose of a BCP is to address and mitigate all risks affecting a company's business operations for managing and responding to risks, used for public, non-profit, nongovernment and private entities. Risk can include many incidents from cyber-attacks to natural disasters. Between 35 and 50 percent of businesses never recover after major disasters³. These disruptions cause revenue loss and difficulty in recovery if no BCP or inadequate BCPs were implemented.

Not all companies have business continuity planning, however this is quickly changing. BCP is now an important process that should be implemented across all industries.



¹

https://www.researchgate.net/publication/240177042_Business_Continuity_Management_Time_for_a_Strategic_Role

² https://www.researchgate.net/publication/240177042_Business_Continuity_Management_Time_for_a_Strategic_Role

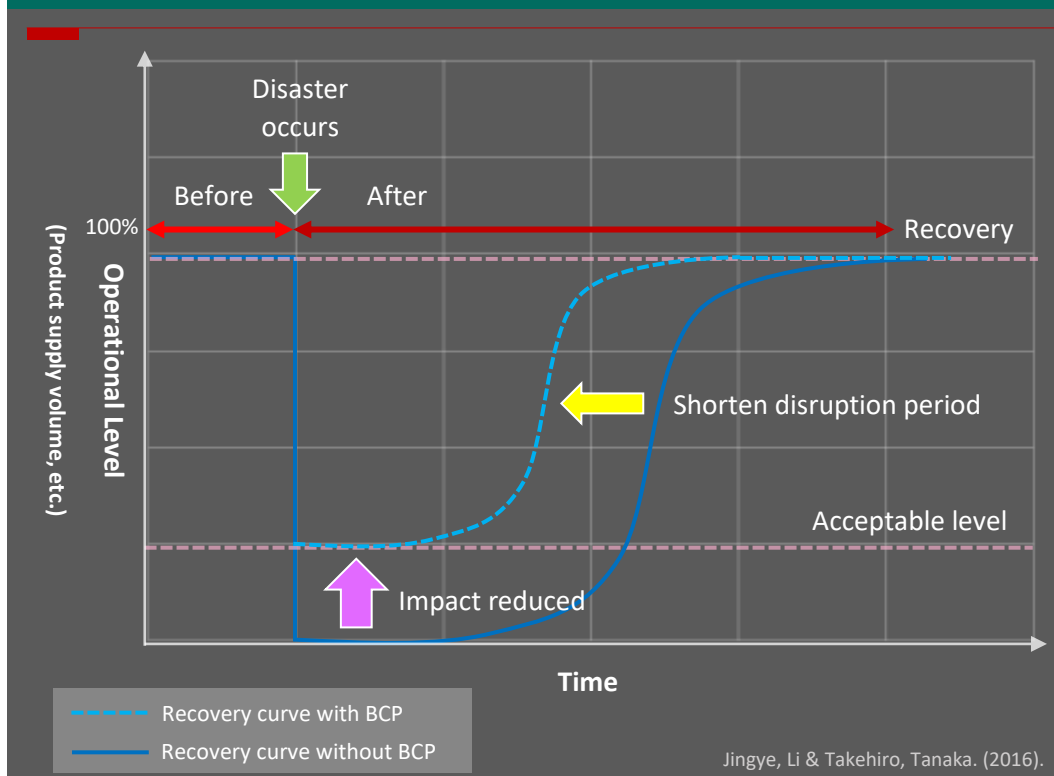
³ <https://www.sciencedirect.com/topics/computer-science/continuity-planning>



Figure 2: IT Risk Management Strategy

An IT Risk Management Strategy, can be regulated by law, whereas BCP is decided by each business's discretion and RM Strategy.

Figure 3: BCP Concept



Jingye, Li & Takehiro, Tanaka. (2016).

Recovery curve with BCP (light blue) shows shorter disruption time and recovery compared to the recovery curve without BCP (dark blue). With BCP, there is reduced impact at the start of the disaster incident as shown in the purple line.

What is an Emergency?

An emergency is an occurrence that needs response to minimize loss of life, property, environment and business operations. These could be human-caused, natural or technology-caused. A typical example of an emergency where BCP is used, is a fire incident that caused property loss.

Other common emergencies include natural disasters such as earthquakes or floods, information security, product liability, long-term delay and suspension of product supplies, impacts of climate change, terrorism, political unrest etc.

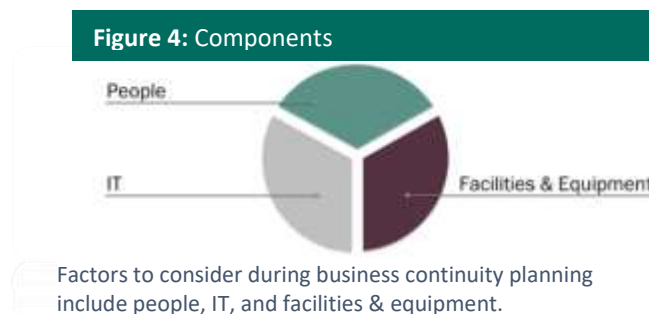
Planning for all possible disruptions is ideal, but most plans try to incorporate as many likely to occur main threats to the business as possible, depending on the type of industry and current global risk trend.

What is the difference between Emergency Planning and BCP?

Emergency planning and business continuity planning play different roles for an effective risk strategy. In general, emergency plans cover response and reactions to the disruption, whereas BCPs deal with continuing the business following the disruption. A single business continuity plan may have many disaster recovery plans.

BCP Standards

Standards provide criteria to develop, implement, assess, and maintain the BCP program to cover prevention, mitigation, preparedness, response, continuity, and recovery. Major standards are **NFPA 1600**, mainly used in the US, and **ISO 22301**⁴, which is internationally used.



⁴ <https://www.iso.org/obp/ui#iso:std:iso:22301:ed-2:v1:en>

Components of BCP





There are 4 main components in BCP. The following is a brief description on how to conduct a BCP program:

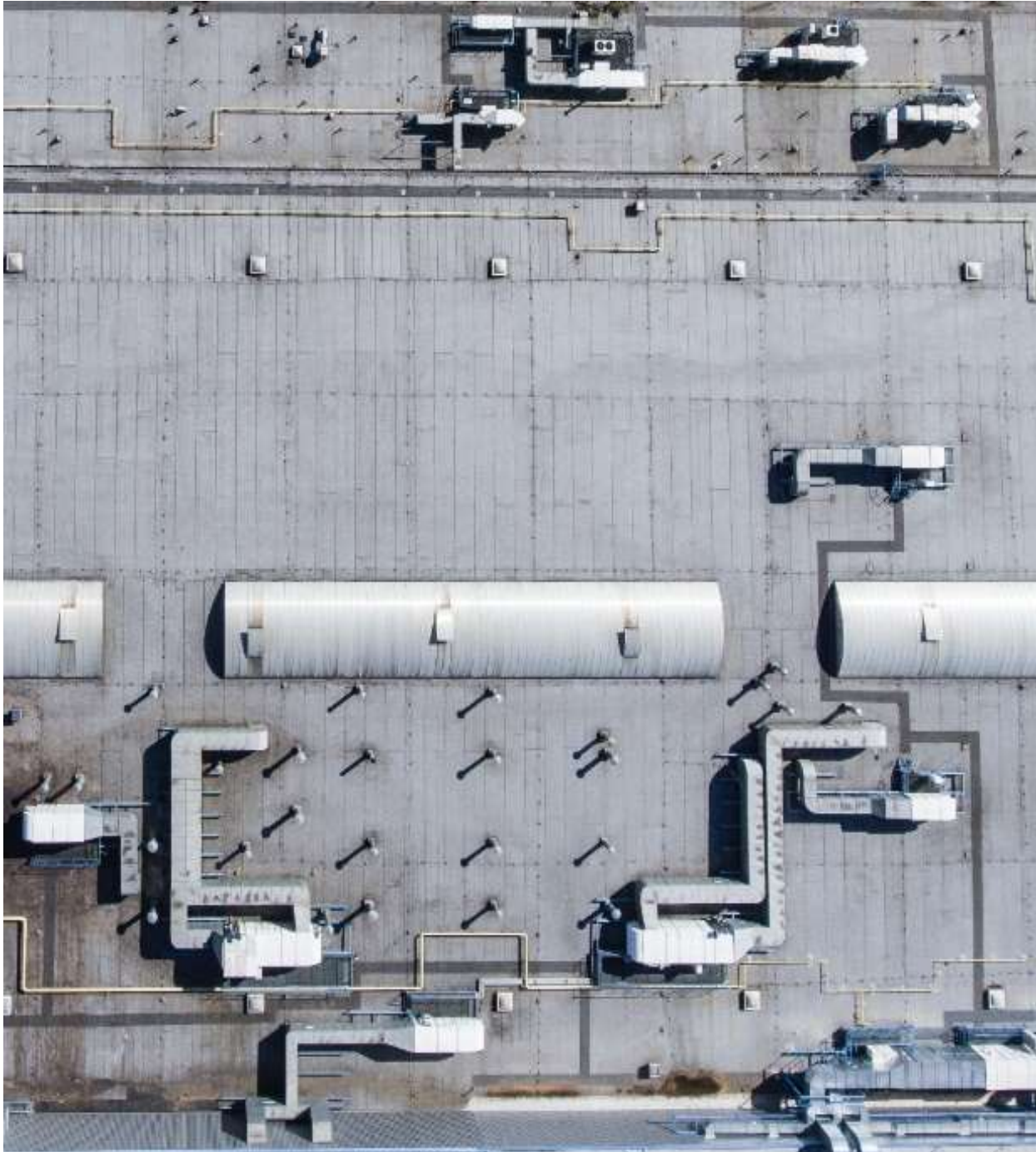
1. **Understand:** Understand your organization's operations and hazards (risk assessment) and how disruptions affect them (Business Impact Analysis).
2. **Plan:** implement and organize the strategies for recovery, allocating people to procedures, and documentation. A clear prevention plan is included.
3. **Improve:** Exercising, testing and changing plans for review. Planning must be tested regularly for different risk scenarios for continuous improvement consistent with the entity's policy, goals, and objectives. Audit activities are included.
4. **Train:** All employees should be aware of such plan.

Why conduct BCP?

Reasons to conduct BCP

Businesses can't always rely on insurance alone, as insurance doesn't always cover every cost associated with the incident. Other benefits include:

-  **Prove** to existing and potential clients that having an effective BCM will enable continued service delivery in the event of an incident.
-  **Ensure** fast enough recovery and minimize major downtime
-  **Provide** assurance to stakeholders and the board.
-  **Meet** regulatory requirements



Your business could stop indefinitely if no BCP is in place.

BCP in Thailand

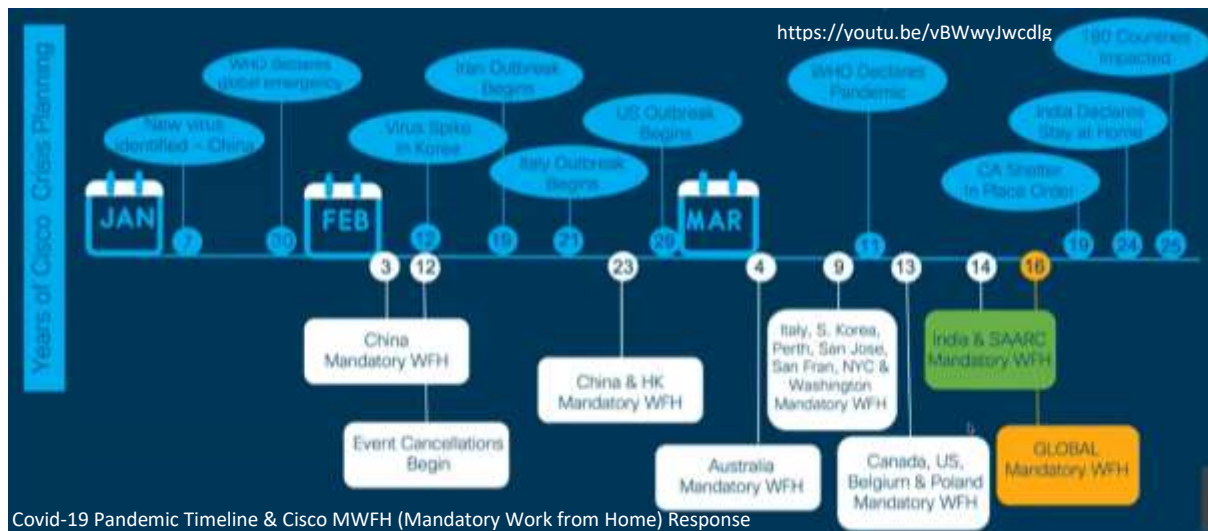
In terms of preparedness, Thailand has no clear plan in business continuity on a national level. Most large corporations will already have BCPs as part of their risk management plan to comply with the company's good business practice and risk policies. In addition, only businesses with direct disaster experience will have BCPs or partial BCPs in place. Much more awareness creation is needed.

SMEs: 99% of Thai business enterprises are SMEs⁵ (Small and Medium Enterprises), which is defined as private organizations with less than 200 people. The Office of Small and Medium Sized Enterprises Promotion (OSMEP), under the Ministry of Industry, showed that there are 2.9 million SMEs in Thailand.

Thai SMEs have low-level preparedness on business continuity planning, according to a study⁶ from 2018. In addition, the degree of knowledge on BCP depends on the size of the business, period in which the business is in operation, and disaster experience. Those with disaster experience are more likely to have BCP. In another survey⁷ conducted in 2012, only 13% of SMEs have a business continuity plan, while 34.8% are in the process of developing one. Supporting business resilience in disaster-prone areas will need public and private support in promoting BCM practices.

Industrial Estates: In the past, BCP of industrial estates in Thailand mainly focused on natural disasters. This is inevitably due to the direct experiences with catastrophes such as the 2011 Flood, where Thai businesses who activated their BCP strategy after the flood recovered better than those without. Increased interest in developing business continuity usually results from these crises.

Others: More immediate opportunities have emerged for Thailand to develop BCP in other areas which applies to all businesses. This is shown recently by the case of Covid-19 pandemic this year, as most businesses were caught off-guard and were unprepared to handle the global virus pandemic which affected all business across the country. Cyber security will be another key risk in the future for Thailand.



<https://doi.org/10.1016/j.ijdr.2017.10.002>

⁶ <https://doi.org/10.1016/j.ijdr.2017.10.002>

⁷ https://www.adrc.asia/publications/bcp/survey_2012.pdf

Frameworks⁸ in Thailand on BCP

In Thailand, The National Economic and Social Development Board (NESDB) conducted a BCP study⁹ in 2011.

Implementation of the BCP is classified into 3 levels: the national, regulatory and business enterprise levels and identifies that at:

The national level: Thailand has no clear plan in business continuity. The Department of Disaster Prevention and Mitigation (DDPM) manages and handles emergency situations, and the agency only focuses on the implementation and management of disasters that affect the lives and property of citizens.

The regulatory level: This is an agency that links the implementation of the BCP between the national level and the business enterprise level.

Currently, regulators encourage the development of BCP by some financial institutions, such as the [Bank of Thailand](#). The group actively promotes and pushes the development of more robust BCP measures.

The Industrial Estate Authority of Thailand Area BCP Bangkok Industrial Park Area, Pathumthani Province, Thailand also promotes the development of BCP in their industrial and entrepreneurial networks together with exercise of a drill at least once a year.

The business enterprise level: Large enterprises have been implementing business continuity management (BCM), which is caused by the awareness of the organization itself and because it is also regulated, such as by the [ISO 22301](#). This has influenced some sectors such as the banking sector to comply with the regulations.

Despite these implementations, some organizations may manage and plan for BCP, but still have not understood its concept well, which hinders co-operation on the national level.

Figure 5: Private Sector BCP

Increased Private Sector Resilience (SDGs 11, 13)
UNDRR will work with the Department of Disaster Prevention and Mitigation to train up to 40 SMEs in Business Continuity Planning to increase SME resilience to natural hazards and disasters in Thailand.



<http://www.un.or.th/wp-content/uploads/2019/09/UN-Thailand-Annual-Report-2018.pdf>

Table 1: BCP Standards in Thailand

Code	Title	Year
ISO22300	Societal security - Terminology	2012
ISO22301	Societal security – Business continuity management systems - Requirements	2012
ISO22313	Societal security - Business continuity management systems - Guidance	2012
ISO22320	Societal security – Emergency management – Requirements for incident response	2011
ISO22399	Societal security – Guideline for incident preparedness and operational continuity management	2007
CPS232	Prudential Standard: Business Continuity Management	2014
มอก 22301	มาตรฐานผลิตภัณฑ์อุตสาหกรรม – ระบบการบริหารความต่อเนื่องทางธุรกิจ – ข้อกำหนด	2010
ISO27001	Information Technology – Security techniques – information security management systems	2013
ISO20000	IT Service Management	2011
BS25777	ICT Continuity Management	2008

https://dga.or.th/upload/download/file_51e3e02b538bbe574b9b3c0da63fb96b.pdf

⁸ <https://www.adpc.net/igo/contents/Publications/publications-Details.asp?pid=1163>

⁹ https://www.adpc.net/igo/category/ID1163/doc/2017-kpg6Jv-ADPC-01_AreaBCP_English_Final_Report_20170220.pdf

Tools

Developing BCP should be a dynamic, ongoing process, as ‘crisis adaptability is the key to continuity’. Many different tools and services are available to facilitate BCPs. Gathering this information could be done manually or automated with the help of software to reduce time and cost, common for IT recovery planning. An example guidance for BCP can be found from [WHO \(World Health Organization\)](#).

#1 Risk assessment:

1. Identify and evaluate risk
2. Actions to manage/mitigate the risk
3. Future monitoring and procedures to prevent risks from occurring

#2 Business Impact Analysis (BIA): an analysis that identifies, quantifies, and qualifies the impacts resulting from interruptions or disruptions of an organization’s resources by using engineering analysis, mathematical modeling, simulations, surveys, questionnaires, interviews, structured workshops, or a combination thereof.

1. Assess impact over time on the products and services and at what cost
2. Prioritize recovery from key areas and critical functions, identifying the critical business processes and “Single Points of Failure” (SPOFs)
3. Identify dependence between business areas and functions
4. Determine the acceptable downtime for each function
5. Identify resources for continuity support
6. Make an initial plan to maintain operations

#3 Recovery strategy planning: The risks (see Figure 4) could either be controlled, transferred, avoided, or accepted. The most common strategies involve some type of third-party data center for backup, an alternate, off-site processing location and alternate workspace to restore operations to a minimally acceptable level¹⁰.

Figure 6: Recovery Planning

Operational Risks:

People	Premises	Technology	Equipment	Information	Suppliers
Who are responsible for each task? Can staff be trained to replace each other?	Can staff work from home? Are there backup facilities and sites for production?	Is there backup for disasters and networks?	Is there spare equipment, repair or reinstallation arrangements?	Is data stored offsite or backed up regularly?	Are the suppliers resilient? Are there alternative suppliers?

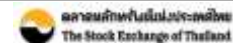
¹⁰ <https://www.sciencedirect.com/sdfe/pdf/download/eid/3-s2.0-B9780123822338000169/first-page-pdf>

#4 Testing: Many organizations test several times a year to improve the plan, depending on the business type of the organization. Employee turnover, number of business processes, and other changes will affect the frequency of testing. Drills or disaster role-playing could be incorporated once a year through discussions (tabletops) with key business units or actual disaster walk-through (exercises).

Figure 7: Example of BCP Activity Testing from The Stock Exchange of Thailand

	Year 1 (2006)	Year 2 (2007)	Year 3 (2008)	Year 4 (2009)
Scenario Test	Bomb	Pandemic Influenza	Terrorist	Flood
Participant	- SET Group	- SET Group - Brokerage Firms	- SET Group - Brokerage Firms - Clearing Members - Depository Members - Listed Companies - BOT	- SET Group - Brokerage Firms - Clearing Members - Depository Members - Listed Companies - BOT

https://www.set.or.th/th/regulations/supervision/files/Disclosure_Focus/Aug_%2053.pdf



A **PDCA (Plan-Do-Check-Act Cycle)**, shown in Figure 5, can be used in the BCM strategy.

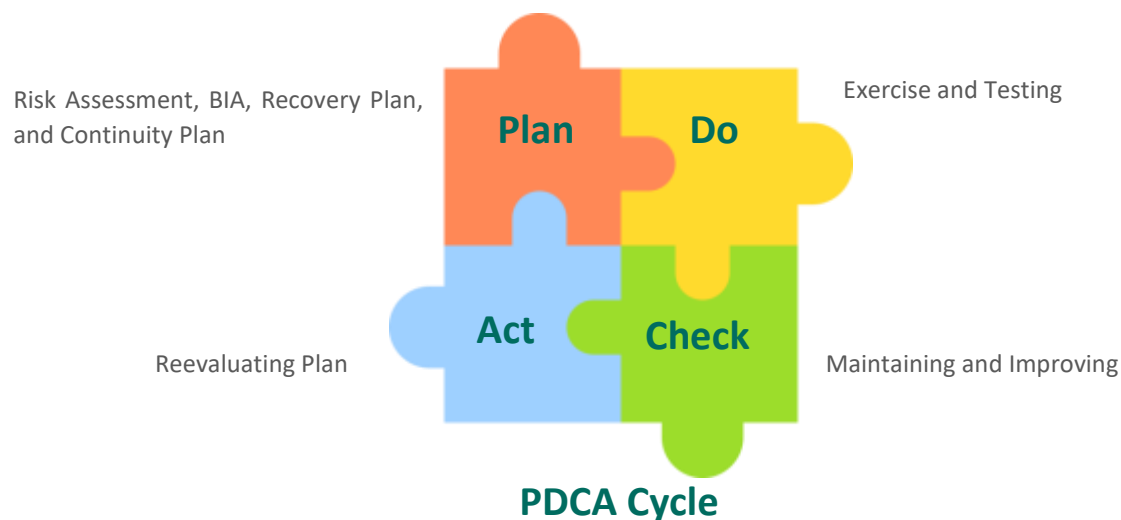


Figure 8: PDCA Cycle

Example BCP Scenarios

The following could be used as example for tabletop exercises:

Scenario 1: A fire occurs in the office. Employees are safely outside, however, client information cannot be accessed as most computers and servers were destroyed in the fire. Hard copies of files and documents

containing important data are lost. How is data backed up? Where? How much can be recovered? How are clients to be notified of the fire accident?

Scenario 2: Viral pandemic

An ongoing flu pandemic is occurring globally. Staff numbers are likely to fluctuate due to sickness or care for family members. Loss of 25% of staff is likely. How can the organization continue to serve customers? What is the chain of command? How to communicate during the crisis and what are the policies? What should happen when attendance drops and fatalities occur? What if the pandemic disease continues for longer than one year?

Conclusion

To ensure a successful plan, companies must be proactive about implementing technologies and protocols that will prevent disruptive events from occurring in the first place. Creating a clear path to recovery with an ongoing BCP will give the organization confidence in dealing with such protocols and systems, hence, rapid business recovery will result.

Find out more about our BCP services.

Reference

1. NFPA 1600, Standard on Disaster/Emergency Management and Business Continuity Programs 2019 Edition
2. "Business Continuity Management" GAP.1.15, Global Asset Protection Services LLC 2015
3. <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience/bc-rm-interfaces>
4. Doi: 10.1016/j.proeng.2016.06.390
5. Practical Process for Introducing Smart Business Continuity Management of Smart City in Japan - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/BCP-concept_fig1_304713463 [accessed 18 May, 2020]
6. Photo by Curioso Photography from Pexels
7. Video on BCP <https://youtu.be/vBWwyJwcdlg>
8. WHO Guidance for Business Continuity Planning. Geneva: World Health Organization; [2018]. License: CC BY-NC-SA 3.0 IGO
9. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience/files/ic_relationship.jpg