Business continuity planning

Business continuity may be defined as "the capability of an organization to continue the delivery of products or services at pre-defined acceptable levels following a disruptive incident",[1] and **business continuity planning** [2][3] (or **business continuity and resiliency planning**) is the process of creating systems of prevention and recovery to deal with potential threats to a company.[4] In addition to prevention, the goal is to enable ongoing operations before and during execution of disaster recovery.[5] Business continuity is the intended outcome of proper execution of both business continuity planning and disaster recovery.

Business continuity planning life cycle

Several business continuity standards have been published by various standards bodies to assist in checklisting ongoing planning tasks.[6]

An organization's resistance to failure is "the ability ... to withstand changes in its environment and still function".[7] Often called resilience, it is a capability that enables organizations to either endure environmental changes without having to permanently adapt, or the organization is forced to adapt a new way of working that better suits the new environmental conditions.[7]

Contents

Overview

Any event that could negatively impact operations should be included in the plan, such as supply chain interruption, loss of or damage to critical infrastructure (major machinery or computing /network resource). As such, BCP is a subset of risk management.[8] In the US, government entities refer to the process as *continuity of operations planning* (COOP).[9] A Business Continuity Plan[10] outlines a range of disaster scenarios and the steps the business will take in any particular scenario to return to regular trade. BCP's are written ahead of time and can also include precautions to be put in place. Usually created with the input of key staff as well as stakeholders, a BCP is a set of contingencies to minimize potential harm to businesses during adverse scenarios.[11]

Resilience

A 2005 analysis of how disruptions can adversely affect the operations of corporations and how investments in resilience can give a competitive advantage over entities not prepared for various contingencies[12] extended then-common business continuity planning practices. Business organizations such as the Council on Competitiveness embraced this resilience goal.[13]

Adapting to change in an apparently slower, more evolutionary manner - sometimes over many years or decades - has been described as being more resilient,[14] and the term "strategic resilience" is now used to go beyond resisting a one-time crisis, but rather continuously anticipating and adjusting, "before the case for change becomes desperately obvious".

This approach is sometimes summarized as: preparedness,[15] protection, response and recovery.[16]

Resilience Theory can be related to the field of Public Relations. Resilience is a communicative process that is constructed by citizens, families, media system, organizations and governments through everyday talk and mediated conversation.[17]

The theory is based on the work of Patrice M. Buzzanell, a professor at the Brian Lamb School of Communication at Purdue University. In her 2010 article, "Resilience: Talking, Resisting, and Imagining New Normalcies Into Being"[18] Buzzanell discussed the ability for organizations to thrive after having a

crisis through building resistance. Buzzanell notes that there are five different processes that individuals use when trying to maintain resilience- crafting normalcy, affirming identity anchors, maintaining and using communication networks, putting alternative logics to work and downplaying negative feelings while foregrounding positive emotions.

When looking at the resilience theory, the crisis communication theory is similar, but not the same. The crisis communication theory is based on the reputation of the company, but the resilience theory is based on the process of recovery of the company. There are five main components of resilience: crafting normalcy, affirming identity anchors, maintaining and using communication networks, putting alternative logics to work, and downplaying negative feelings while foregrounding negative emotions.[19] Each of these processes can be applicable to businesses in crisis times, making resilience an important factor for companies to focus on while training.

There are three main groups that are affected by a crisis. They are micro (individual), meso (group or organization) and macro (national or interorganizational). There are also two main types of resilience, which are proactive and post resilience. Proactive resilience is preparing for a crisis and creating a solid foundation for the company. Post resilience includes continuing to maintain communication and check in with employees.[20] Proactive resilience is dealing with issues at hand before they cause a possible shift in the work environment and post resilience maintaining communication and accepting chances after an incident has happened. Resilience can be applied to any organization.

Continuity

Plans and procedures are used in business continuity planning to ensure that the critical organizational operations required to keep an organization running continue to operate during events when key dependencies of operations are disrupted. Continuity does not need to apply to every activity which the organisation undertakes. For example, under ISO 22301:2019, organisations are required to define their business continuity objectives, the minimum levels of product and service operations which will be considered acceptable and the maximum tolerable period of disruption (MTPD) which can be allowed.[21]

A major cost in planning for this is the preparation of audit compliance management documents; automation tools are available to reduce the time and cost associated with manually producing this information.

Inventory

Planners must have information about:

- Equipment
- Supplies and suppliers
- Locations, including other offices and backup/work area recovery (WAR) sites
- Documents and documentation, including which have off-site backup copies:[10]
  - Business documents
  - Procedure documentation

Analysis

The analysis phase consists of

- impact analysis
- threat analysis and
- impact scenarios.

Quantifying of loss ratios must also include "dollars to defend a lawsuit."[22] It has been estimated that a dollar spent in loss prevention can prevent "seven dollars of disaster-related economic loss."[23]

Business impact analysis (BIA)

A Business impact analysis (BIA) differentiates critical (urgent) and non-critical (non-urgent) organization functions/activities. A function may be considered critical if dictated by law.

Each function/activity typically relies on a combination of constituent components in order to operate:

- Human resources (full-time staff, part-time staff, or contractors)
- IT systems
- Physical assets (mobile phones, laptops/workstations etc.)
- Documents (electronic or physical)

For each function, two values are assigned:

- Recovery Point Objective (RPO) – the acceptable latency of data that will not be recovered. For example, is it acceptable for the company to lose 2 days of data?[24] The recovery point objective must ensure that the maximum tolerable data loss for each activity is not exceeded.
- Recovery Time Objective (RTO) – the acceptable amount of time to restore the function

Maximum RTO

Maximum time constraints for how long an enterprise's key products or services can be unavailable or undeliverable before stakeholders perceive unacceptable consequences have been named as:

- **Maximum Tolerable Period of Disruption** (**MTPoD**)
- **Maximum Tolerable Downtime** (**MTD**)
- **Maximum Tolerable Outage** (**MTO**)
- **Maximum Allowable Outage** (**MAO**)[25][26]

According to ISO 22301 the terms *maximum acceptable outage* and *maximum tolerable period of disruption* mean the same thing and are defined using exactly the same words.[27]

Consistency

When more than one system crashes, recovery plans must balance the need for data consistency with other objectives, such as RTO and RPO. [28] **Recovery Consistency Objective** (RCO) is the name of this goal. It applies data consistency objectives, to define a measurement for the consistency of distributed business data within interlinked systems after a disaster incident. Similar terms used in this context are "Recovery Consistency Characteristics" (RCC) and "Recovery Object Granularity" (ROG).[29]

While RTO and RPO are absolute per-system values, RCO is expressed as a percentage that measures the deviation between actual and targeted state of business data across systems for process groups or individual business processes.

The following formula calculates RCO with "n" representing the number of business processes and "entities" representing an abstract value for business data:

$$\mathrm{RCO} = 1 - \frac{(\text{number of inconsistent entities})_n}{(\text{number of entities})_n}$$

100% RCO means that post recovery, no business data deviation occurs.[30]

Threat and risk analysis (TRA)

After defining recovery requirements, each potential threat may require unique recovery steps. Common threats include:

- Epidemic/pandemic
- Earthquake
- Fire
- Flood
- Cyber attack
- Sabotage (insider or external threat)
- Hurricane or other major storm
- Power outage
- Water outage (supply interruption, contamination)
- Telecomms outage
- IT outage
- Terrorism/Piracy
- War/civil disorder
- Theft (insider or external threat, vital information or material)
- Random failure of mission-critical systems
- Single point dependency
- Supplier failure
- Data corruption
- Misconfiguration

The above areas can cascade: Responders can stumble. Supplies may become depleted. During the 2002-2003 SARS outbreak, some organizations compartmentalized and rotated teams to match the incubation period of the disease. They also banned in-person contact during both business and non-business hours. This increased resiliency against the threat.

Impact scenarios

Impact scenarios are identified and documented:

- need for medical supplies[31]
- need for transportation options[32]
- civilian impact of nuclear disasters[33]
- need for business and data processing supplies[34]

These should reflect the widest possible damage.

Tiers of preparedness

SHARE's seven tiers of disaster recovery[35] released in 1992, were updated in 2012 by IBM as an eight tier model:[36]

- **Tier 0 - No off-site data** • Businesses with a Tier 0 Disaster Recovery solution have no Disaster Recovery Plan. There is no saved information, no documentation, no backup hardware, and no contingency plan. Typical recovery time: ***The length of recovery time in this instance is unpredictable***. In fact, it may not be possible to recover at all.
- **Tier 1 - Data backup with no Hot Site** • Businesses that use Tier 1 Disaster Recovery solutions back up their data at an off-site facility. Depending on how often backups are made, they are prepared to accept **several days to weeks of data loss**, but their backups are secure off-site. However, this Tier lacks the systems on which to restore data. Pickup Truck Access Method (PTAM).
- **Tier 2** - **Data backup with Hot Site** • Tier 2 Disaster Recovery solutions make regular backups on tape. This is combined with an off-site facility and infrastructure (known as a hot site) in which to restore systems from those tapes in the event of a disaster. This tier solution will still result in the need to recreate several hours to days worth of data, but ***it is less unpredictable in recovery time***. Examples include: PTAM with Hot Site available, IBM Tivoli Storage Manager.
- **Tier 3 - Electronic vaulting** • Tier 3 solutions utilize components of Tier 2. Additionally, some mission-critical data is electronically vaulted. This electronically vaulted data is typically more current than that which is shipped via PTAM. As a result there is ***less data recreation or loss after a disaster occurs***.
- **Tier 4 - Point-in-time copies** • Tier 4 solutions are used by businesses that require both greater data currency and faster recovery than users of lower tiers. Rather than relying largely on shipping tape, as is common in the lower tiers, Tier 4 solutions begin to incorporate more disk-based solutions. ***Several hours of data loss is still possible***, but it is easier to make such point-in-time (PIT) copies with greater frequency than data that can be replicated through tape-based solutions.
- **Tier 5 - Transaction integrity** • Tier 5 solutions are used by businesses with a requirement for consistency of data between production and recovery data centers. There is ***little to no data loss*** in such solutions; however, the presence of this functionality is entirely dependent on the application in use.
- **Tier 6 - Zero or little data loss** • Tier 6 Disaster Recovery solutions ***maintain the highest levels of data currency***. They are used by businesses with little or no tolerance for data loss and who need to restore data to applications rapidly. These solutions have no dependence on the applications to provide data consistency.
- **Tier 7 - Highly automated, business-integrated solution** • Tier 7 solutions include all the major components being used for a Tier 6 solution with the additional integration of automation. This allows a Tier 7 solution to ensure consistency of data above that of which is granted by Tier 6 solutions. Additionally, recovery of the applications is automated, allowing for restoration of systems and applications much faster and more reliably than would be possible through manual Disaster Recovery procedures.

Solution design

Two main requirements from the impact analysis stage are:

- For IT: the minimum application and data requirements and the time in which they must be available.
- Outside IT: preservation of hard copy (such as contracts). A process plan must consider skilled staff and embedded technology.

This phase overlaps with disaster recovery planning.

The solution phase determines:

- crisis management command structure
- telecommunication architecture between primary and secondary work sites
- data replication methodology between primary and secondary work sites
- Backup site - applications, data and work space required at the secondary work site

British standards

The **British Standards Institution (BSI)** released a series of standards:

- 1995: BS 7799, peripherally addressed information security procedures. (withdrawn)
- 2006: BCP — BS 25999-1 Business Continuity Management. Code of Practice (withdrawn)
- 2007: BS 25999-2 Specification for Business Continuity Management, which specifies requirements for implementing, operating and improving a documented business continuity management system (BCMS). (withdrawn)
- 2008: BS 25777, specifically to align computer continuity with business continuity. (withdrawn March 2011)
- 2011: ISO/IEC 27031 - Security techniques — Guidelines for information and communication technology readiness for business continuity.
- BS EN ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements, the current standard for business continuity planning.[37]
- BS EN ISO 22313:2020 Security and resilience - Business continuity management systems - Guidance on the use of ISO 22301

ITIL has defined some of these terms.[38]

Within the UK, BS 25999-2:2007 and BS 25999-1:2006 were being used for business continuity management across all organizations, industries and sectors. These documents give a practical plan to deal with most eventualities—from extreme weather conditions to terrorism, IT system failure, and staff sickness.[39]

Civil Contingencies Act

In 2004, following crises in the preceding years, the UK government passed the Civil Contingencies Act of 2004: Businesses must have continuity planning measures to survive and continue to thrive whilst working towards keeping the incident as minimal as possible.[40]

The Act was separated into two parts:

- Part 1: civil protection, covering roles & responsibilities for local responders
- Part 2: emergency powers

Australia and New Zealand

United Kingdom and Australia[41] have incorporated resilience into their continuity planning.[42][43] In the United Kingdom, resilience is implemented locally by the Local Resilience Forum.

In New Zealand, the Canterbury University Resilient Organisations programme developed an assessment tool for benchmarking the Resilience of Organisations.[44] It covers 11 categories, each having 5 to 7 questions. A *Resilience Ratio* summarizes this evaluation.[45]

Implementation and testing

The implementation phase involves policy changes, material acquisitions, staffing and testing.

Testing and organizational acceptance

The 2008 book *Exercising for Excellence*, published by The British Standards Institution identified three types of exercises that can be employed when testing business continuity plans.

- **Tabletop exercises** - a small number of people concentrate on a specific aspect of a BCP. Another form involves a single representative from each of several teams.
- **Medium exercises** - Several departments, teams or disciplines concentrate on multiple BCP aspects; the scope can range from a few teams from one building to multiple teams operating across dispersed locations. Pre-scripted "surprises" are added.
- **Complex exercises** - All aspects of a medium exercise remain, but for maximum realism no-notice activation, actual evacuation and actual invocation of a disaster recovery site is added.

While start and stop times are pre-agreed, the actual duration might be unknown if events are allowed to run their course.

Maintenance

Biannual or annual maintenance cycle maintenance of a BCP manual[41] is broken down into three periodic activities.

- Confirmation of information in the manual, roll out to staff for awareness and specific training for critical individuals.
- Testing and verification of technical solutions established for recovery operations.
- Testing and verification of organization recovery procedures.

Issues found during the testing phase often must be reintroduced to the analysis phase.

Information/targets

The BCP manual must evolve with the organization, and maintain information about **who has to know what**

- a series of checklists
  - job descriptions, skillsets needed, training requirements
  - documentation and document management
- definitions of terminology to facilitate timely communication during disaster recovery,[46]
- distribution lists (staff, important clients, vendors/suppliers)
- information about communication and transportation infrastructure (roads, bridges)[47]

Technical

Specialized technical resources must be maintained. Checks include:

- Virus definition distribution
- Application security and service patch distribution
- Hardware operability
- Application operability
- Data verification
- Data application

Testing and verification of recovery procedures

Software and work process changes must be documented and validated, including verification that documented work process recovery tasks and supporting disaster recovery infrastructure allow staff to recover within the predetermined recovery time objective.[48]

Standards

There are many standards that are available to support Business continuity planning and management. ISO has for example developed a whole series of standards on Business continuity management systems [49] under responsibility of technical committee ISO/TC 292:

- ISO 22300:2018 Security and resilience – Vocabulary[50]
- ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements[51]
- ISO 22313:2020 Security and resilience – Business continuity management systems – Guidance on the use of ISO 22301[52]
- ISO/TS 22317:2015 Societal security – Business continuity management systems – Guidelines for business impact analysis[53]
- ISO/TS 22318:2015 Societal security – Business continuity management systems – Guidelines for supply chain continuity[54]
- ISO/TS 22330:2018 Security and resilience – Business continuity management systems – Guidelines for people aspects on business continuity[55]
- ISO/TS 22331:2018 Security and resilience – Business continuity management systems – Guidelines for business continuity strategy[55]
- ISO/IEC/TS 17021-6:2015 Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 6: Competence requirements for auditing and certification of business continuity management systems[56]

See also

- Catastrophe modeling
- Crisis management
- Cyber resilience
- Digital continuity
- Disaster
- Disaster recovery
- Disaster recovery and business continuity auditing

- Disaster risk reduction
- Emergency management
- Man-made hazards
- Natural hazards
- Risk management
- Scenario planning
- Systems engineering
- System lifecycle

References

1. BCI Good Practice Guidelines 2013, quoted in Mid Sussex District Council, Business Continuity Policy Statement (https://www.midsussex.gov.uk/media/1838/mid-sussex-business-continuity-plan.pdf), published April 2018, accessed 19 February 2021
2. "How to Build an Effective and Organized Business Continuity Plan" (https://www.forbes.com/sites/johnrampton/2015/06/26/how-to-build-an-effective-and-organized-business-continuity-plan). *Forbes*. June 26, 2015.
3. "Surviving a Disaster" (https://www.americanbar.org/content/dam/aba/events/disaster/surviving_a_disaster_a_lawyers_guide_to_disaster_planning.authcheckdam.pdf) (PDF). *American Bar.org (American Bar Association)*. 2011.
4. Elliot, D.; Swartz, E.; Herbane, B. (1999) Just waiting for the next big bang: business continuity planning in the UK finance sector. Journal of Applied Management Studies, Vol. 8, No, pp. 43–60. Here: p. 48.
5. Alan Berman (March 9, 2015). "Constructing a Successful Business Continuity Plan" (http://www.businessinsurance.com/article/20150309/ISSUE0401/303159991/constructing-a-successful-business-continuity-plan). *Business Insurance Magazine*.
6. "Business Continuity Plan" (https://www.ready.gov/business/implementation/continuity). United States Department of Homeland Security. Retrieved 4 October 2018.
7. Ian McCarthy; Mark Collard; Michael Johnson (2017). "Adaptive organizational resilience: an evolutionary perspective". *Current Opinion in Environmental Sustainability*. **28**: 33–40. doi:10.1016/j.cosust.2017.07.005 (https://doi.org/10.1016%2Fj.cosust.2017.07.005).
8. Intrieri, Charles (10 September 2013). "Business Continuity Planning" (http://flevy.com/blog/business-continuity-planning/). Flevy. Retrieved 29 September 2013.
9. "Continuity Resources and Technical Assistance | FEMA.gov" (https://www.fema.gov/emergency-managers/national-preparedness/continuity). *www.fema.gov*.
10. "A Guide to the preparation of a Business Continuity Plan" (https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/property-insights/business-continuity-planning-guidelines-for-preparation-of-your-plan.pdf) (PDF).
11. "Business Continuity Planning (BCP) for Businesses of all Sizes" (https://web.archive.org/web/20170424090047/http://www.williamadvisorygroup.com/business-continuity-planning-bcp-for-businesses-of-all-sizes/). 19 April 2017. Archived from the original (http://www.williamadvisorygroup.com/business-continuity-planning-bcp-for-businesses-of-all-sizes/) on 24 April 2017. Retrieved 28 April 2017.
12. Yossi Sheffi (October 2005). *The Resilient Enterprise: Overcoming Vulnerability for Competitive Enterprise* (http://resilient-enterprise.mit.edu). MIT Press.
13. "Transform. The Resilient Economy" (http://www.compete.org/publications/detail/31/the-resilient-economy-integrating-competitiveness-and-security).
14. "Newsday | Long Island's & NYC's News Source | Newsday" (https://www.newsday.com/2.811/jamie-herzlich/small-business-a-good-plan-shields-from-storm-clouds-1.1322137?firstfree=yes).

15. Tiffany Braun; Benjamin Martz (2007). "Business Continuity Preparedness and the Mindfulness State of Mind". S2CID 7698286 (https://api.semanticscholar.org/CorpusID:7698286). ""An estimated 80 percent of companies without a well-conceived and tested business continuity plan, go out of business within two years of a major disaster" (Santangelo 2004)"
16. "Building A Resilient Nation: Enhancing Security, Ensuring a Strong Economy report" (https://www.policyarchive.org/bitstream/handle/10207/9662/Building_Resilience_OCT6.pdf?sequence=1) (PDF). Reform Institute. October 2008.
17. "Communication and resilience: concluding thoughts and key issues for future research" (https://www.researchgate.net/publication/322693327). *www.researchgate.net*.
18. Buzzanell, Patrice M. (2010). "Resilience: Talking, Resisting, and Imagining New Normalcies Into Being". *Journal of Communication*. **60** (1): 1–14. doi:10.1111/j.1460-2466.2009.01469.x (https://doi.org/10.1111%2Fj.1460-2466.2009.01469.x). ISSN 1460-2466 (https://www.worldcat.org/issn/1460-2466).
19. Buzzanell, Patrice M. (March 2010). "Resilience: Talking, Resisting, and Imagining New Normalcies Into Being". *Journal of Communication*. **60** (1): 1–14. doi:10.1111/j.1460-2466.2009.01469.x (https://doi.org/10.1111%2Fj.1460-2466.2009.01469.x). ISSN 0021-9916 (https://www.worldcat.org/issn/0021-9916).
20. Buzzanell, Patrice M. (2018-01-02). "Organizing resilience as adaptive-transformational tensions". *Journal of Applied Communication Research*. **46** (1): 14–18. doi:10.1080/00909882.2018.1426711 (https://doi.org/10.1080%2F00909882.2018.1426711). ISSN 0090-9882 (https://www.worldcat.org/issn/0090-9882). S2CID 149004681 (https://api.semanticscholar.org/CorpusID:149004681).
21. ISO, ISO 22301 Business Continuity Management: Your implementation guide (https://www.bsigroup.com/globalassets/Documents/iso-22301/resources/iso-22301-implementation-guide-2016.pdf), published, accessed 20 February 2021
22. "Emergency Planning" (http://www.jcrcny.org/wp-content/uploads/2013/10/EmergencyManual.2.0.pdf) (PDF).
23. Helen Clark (August 15, 2012). "Can your Organization survive a natural disaster?" (http://www.riema.ri.gov/berhodyready/files/Session_1_Business%20Continuity.pdf) (PDF). *RI.gov*.
24. May, Richard. "Finding RPO and RTO" (https://web.archive.org/web/20160303224604/http://www.virtualdcs.co.uk/blog/business-continuity-planning-rpo-and-rto.html). Archived from the original (http://www.virtualdcs.co.uk/blog/business-continuity-planning-rpo-and-rto.html) on 2016-03-03.
25. "Maximum Acceptable Outage (Definition)" (http://www.riskythinking.com/glossary/maximum_acceptable_outage.php). *riskythinking.com*. Albion Research Ltd. Retrieved 4 October 2018.
26. "BIA Instructions, BUSINESS CONTINUITY MANAGEMENT - WORKSHOP" (http://www.driecentral.org/biainstructions.pdf) (PDF). *driecentral.org*. Disaster Recovery Information Exchange (DRIE) Central. Retrieved 4 October 2018.
27. "Plain English ISO 22301 2012 Business Continuity Definitions" (http://www.praxiom.com/iso-22301-definitions.htm). *praxiom.com*. Praxiom Research Group LTD. Retrieved 4 October 2018.
28. "The Rise and Rise of the Recovery Consistency Objective" (https://web.archive.org/web/20200926060225/https://www.opscentre.com/blog/2016/03/22/recovery-consistency-objective/). 2016-03-22. Archived from the original (https://www.opscentre.com/blog/2016/03/22/recovery-consistency-objective) on 2020-09-26. Retrieved September 9, 2019.
29. "How to evaluate a recovery management solution." West World Productions, 2006 [1] (http://www.thefreelibrary.com/How+to+evaluate+a+recovery+management+solution-a0147748661)

30. Josh Krischer; Donna Scott; Roberta J. Witty. "Six Myths About Business Continuity Management and Disaster Recovery" (http://www.gartner.com/it/content/868800/868812/six_myths_about_bcm.pdf) (PDF). Gartner Research.
31. "Medical supply location and distribution in disasters". doi:10.1016/j.ijpe.2009.10.004 (https://doi.org/10.1016%2Fj.ijpe.2009.10.004).
32. "transportation planning in disaster recovery" (https://scholar.google.com/scholar_url?url=https://orbi.uliege.be/bitstream/2268/8333/1/JORS_Barbarosoglu_Arda_2004.pdf%26hl=en%26sa=X%26scisig=AAGBfm0xx_ynzP503rz-gtdgZVSN_h-m7w%26nossl=1%26oi=scholarr). *SCHOLAR.google.com*.
33. "PLANNING SCENARIOS Executive Summaries" (https://www.globalsecurity.org/security/library/report/2004/hsc-planning-scenarios-jul04_exec-sum.pdf) (PDF).
34. Chloe Demrovsky (December 22, 2017). "Holding It All Together". Manufacturing Business Technology Magazine.
35. developed by SHARE's Technical Steering Committee, working with IBM
36. Ellis Holman (March 13, 2012). "A Business Continuity Solution Selection Methodology" (https://share.confex.com/share/118/webprogram/Handout/Session10387/Session%2010387%20Business%20Continuity%20Soloution%20Selection%20Methodology%2003-7-2012.pdf) (PDF). IBM Corp.
37. "ISO 22301 Business Continuity Management" (http://www.bsigroup.com/en-CA/ISO-22301-Business-Continuity-Management/). *www.bsigroup.com*.
38. "Glossaries of Terms" (https://www.axelos.com/glossaries-of-terms). *AXELOS*.
39. British Standards Institution (2006). Business continuity management-Part 1: Code of practice :London
40. Cabinet Office. (2004). overview of the Act. In: Civil Contingencies Secretariat Civil Contingencies Act 2004: a short. London: Civil Contingencies Secretariat
41. "Business Continuity Plan Template" (https://publications.qld.gov.au/dataset/05765d5a-91b3-45fd-af43-699ede65dd8a/resource/63f7d2dc-0f40-4abb-b75f-7e6acfeae8f3/download/businesscontinuityplantemplate.doc).
42. Resilient Nation (http://www.demos.co.uk/publications/resilientnation) Archived (https://web.archive.org/web/20150923213646/http://www.demos.co.uk/publications/resilientnation) 2015-09-23 at the Wayback Machine. Demos. April 2009.
43. Improving Disaster Resilience (http://www.royalcommission.vic.gov.au/getdoc/cd99d136-6195-4b70-b6f4-46202d717f1e/TEN.047.001.0001.pdf) Archived (https://web.archive.org/web/20190207014917/http://royalcommission.vic.gov.au/getdoc/cd99d136-6195-4b70-b6f4-46202d717f1e/TEN.047.001.0001.pdf) 2019-02-07 at the Wayback Machine. Australian Government. May 12, 2009.
44. "Resilient Organisations" (http://www.resorgs.org.nz). March 22, 2011.
45. "Resilience Diagnostic" (https://resiliencei.com/resilience-diagnostic). November 28, 2017.
46. "Glossary | DRI International" (https://drii.org/resources/viewglossary). *drii.org*.
47. "Disaster Recovery Plan Checklist" (https://www.cms.gov/Medicare/Medicare-Contracting/FFSProvCustSvcGen/Downloads/Disaster-Recovery-Plan-Checklist.pdf) (PDF). *CMS.gov*.
48. Othman. "Validation of a Disaster Management Metamodel (DMM)" (https://scholar.google.com/scholar_url?url=http://ro.uow.edu.au/cgi/viewcontent.cgi%253Farticle%253D2748%2526context%253Deispapers%26hl=en%26sa=X%26scisig=AAGBfm0CkEknKpMQtJeZBAWSgF_CqnzjNg%26nossl=1%26oi=scholarr). *SCHOLAR.google.com*.
49. "ISO - ISO/TC 292 - Security and resilience" (https://www.iso.org/committee/5259148/x/catalogue/p/1/u/0/w/0/d/0). *www.iso.org*.
50. "ISO 22300:2018" (https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/84/68436.html). *ISO*.

51. "ISO 22301:2019" (https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/51/75106.html). *ISO*.
52. "ISO 22313:2020" (https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/51/75107.html). *ISO*.
53. "ISO/TS 22317:2015" (https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/00/50054.html). *ISO*.
54. "ISO/TS 22318:2015" (https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/53/65336.html). *ISO*.
55. "ISO/TS 22330:2018" (https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/00/50067.html). *ISO*.
56. "ISO/IEC TS 17021-6:2014" (https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/49/64956.html). *ISO*.

Further reading

United States

Bibliography

- Business Continuity Planning, FEMA (http://www.ready.gov/business/implementation/continuity), Retrieved: June 16, 2012
- Continuity of Operations Planning (https://web.archive.org/web/20060818044954/http://www.ready.gov/business/plan/planning.html) (no date). *U.S. Department of Homeland Security*. Retrieved July 26, 2006.
- Purpose of Standard Checklist Criteria For Business Recovery (https://web.archive.org/web/20060810074640/http://www.fema.gov/business/bc.shtm) (no date). *Federal Emergency Management Agency*. Retrieved July 26, 2006.
- NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs (2010). *National Fire Protection Association*.
- United States General Accounting Office Y2k BCP Guide (https://web.archive.org/web/20041225114909/http://www.gao.gov/special.pubs/bcpguide.pdf) (August 1998). *United States Government Accountability Office*.
- SPC.1-2009, "Organizational Resilience: Security, Preparedness, and Continuity Management Systems—Requirements with Guidance for Use", approved by American National Standards Institute

International Organization for Standardization

- ISO 22300:2018 Security and resilience - Vocabulary
- ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements
- ISO 22313:2013 Security and resilience - Business continuity management systems - Guidance on the use of ISO 22301
- ISO/TS 22315:2015 Societal security – Business continuity management systems – Guidelines for business impact analysis (BIA)
- ISO/PAS 22399:2007 Guideline for incident preparedness and operational continuity management (withdrawn)

- ISO/IEC 24762:2008 Guidelines for information and communications technology disaster recovery services
- ISO/IEC 27001:2013 (formerly BS 7799-2:2002) Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls
- ISO/IEC 27031:2011 Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity
- IWA 5:2006 Emergency Preparedness (withdrawn)

British Standards Institution

- BS 25999-1:2006 Business Continuity Management Part 1: Code of practice (superseded, withdrawn)
- BS 25999-2:2007 Business Continuity Management Part 2: Specification (superseded, withdrawn)

Australia Standards

- HB 292-2006, "A practitioners guide to business continuity management"
- HB 293-2006, "Executive guide to business continuity management"

Others

- James C. Barnes (2001-06-08). *A Guide to Business Continuity Planning*. ISBN 978-0471530152.
- Kenneth L Fulmer (2004-10-04). *Business Continuity Planning, A Step-by-Step Guide*. ISBN 978-1931332217.
- Richard Kepenach. *Business Continuity Plan Design, 8 Steps for Getting Started Designing a Plan*.
- Judy Bell. *Disaster Survival Planning: A Practical Guide for Businesses*. ISBN 978-0963058003.
- Dimattia, S. (November 15, 2001). "Planning for Continuity" (http://eric.ed.gov/?id=EJ645580). *Library Journal*. **126** (19): 32–34.
- Andrew Zolli; Ann Marie Healy (2013). *Resilience: Why Things Bounce Back*. Simon & Schuster. ISBN 978-1451683813.
- International Glossary for Resilience (https://drii.org/resources/glossary), DRI International.

External links

- *The tiers of Disaster Recovery and TSM. (https://web.archive.org/web/20150801223921/http://www.redbooks.ibm.com/redbooks/SG246844.html)* Charlotte Brooks, Matthew Bedernjak, Igor Juran, and John Merryman. In, *Disaster Recovery Strategies with Tivoli Storage Management.* Chapter 2. Pages 21–36. Red Books Series. IBM. Tivoli Software. 2002.
- *SteelStore Cloud Storage Gateway: Disaster Recovery Best Practices Guide.* (https://web.archive.org/web/20140811064656/https://splash.riverbed.com/servlet/JiveServlet/downloadBody/3897-102-2-5505/Best%20Practices%20Guide%20-%20SteelStore%20DR%20Replication.pdf) Riverbed Technology, Inc. October 2011.

- *Disaster Recovery Levels.* (https://web.archive.org/web/20181203152111/http://ibmsystemsmag.com/mainframe/administrator/backuprecovery/disaster-recovery-levels/?page=2) Robert Kern and Victor Peltz. IBM Systems Magazine. November 2003.
- *Business Continuity: The 7-tiers of Disaster Recovery.* (http://recoveryspecialties.com/7-tiers.html) Archived (https://web.archive.org/web/20180926124124/http://recoveryspecialties.com/7-tiers.html) 2018-09-26 at the Wayback Machine Recovery Specialties. 2007.
- *Continuous Operations: The Seven Tiers of Disaster Recovery.* (http://storagecommunity.org/forums/t/326.aspx) Mary Hall. The Storage Community (IBM). 18 July 2011. Retrieved 26 March 2013.</ref>
- Maximum Tolerable Period of Disruption (MTPOD) (http://www.continuitycentral.com/feature0675.html)
- Maximum Tolerable Period of Disruption (MTPOD): BSI committee response (http://www.continuitycentral.com/feature0677.html)
- Wayback Machine (https://web.archive.org/web/20160303215200/http://www.bccmanagement.com/mtpod.html)
- Janco Associates (https://web.archive.org/web/20090717220729/http://e-janco.com/MaximumTolerablePeriodofDisruption%20.html)
- Department of Homeland Security Emergency Plan Guidelines (https://web.archive.org/web/20041207212256/http://www.ready.gov/business/index.html)
- CIDRAP/SHRM Pandemic HR Guide Toolkit (http://www.cidrap.umn.edu/cidrap/files/33/cidrap-shrm-hr-pandemic-toolkit.pdf)
- Adapt and respond to risks with a business continuity plan (BCP) (https://www.ibm.com/services/business-continuity/plan)
