Disaster recovery

Disaster Recovery involves a set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster. Disaster recovery focuses on the IT or technology systems supporting critical business functions,[1] as opposed to business continuity, which involves keeping all essential aspects of a business functioning despite significant disruptive events. Disaster recovery can therefore be considered a subset of business continuity.[2][3] Disaster Recovery assumes that the primary site is not recoverable (at least for some time) and represents a process of restoring data and services to a secondary survived site, which is opposite to the process of restoring back to its original place

Contents

IT Service Continuity

IT Service Continuity[4][5] (ITSC) is a subset of business continuity planning (BCP)[6] and encompasses IT disaster recovery planning and wider IT resilience planning. It also incorporates those elements of IT infrastructure and services which relate to communications such as (voice) telephony and data communications.

The ITSC Plan reflects Recovery Point Objective (RPO - recent transactions) and Recovery Time Objective (RTO - time intervals).

Principles of Backup sites

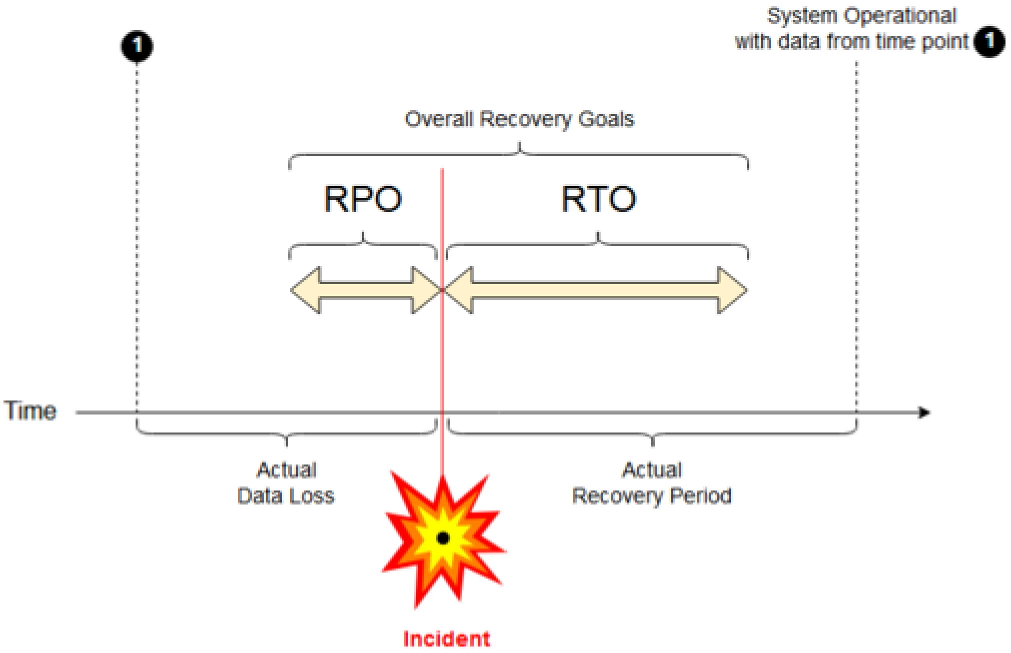
Planning includes arranging for backup sites, be they hot, warm, cold, or standby sites, with hardware as needed for continuity.

In 2008 the British Standards Institution launched a specific standard connected and supporting the Business Continuity Standard BS 25999 titled BS25777 specifically to align computer continuity with business continuity. This was withdrawn following the publication in March 2011 of ISO/IEC 27031 - Security techniques — Guidelines for information and communication technology readiness for business continuity.

ITIL has defined some of these terms.[7]

Recovery Time Objective

The **Recovery Time Objective** (**RTO**)[8][9] is the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.[10]



Schematic representation of the terms RPO and RTO. In this example, the agreed values of RPO and RTO are *not* fulfilled.

In accepted business continuity planning methodology, the RTO is established during the Business Impact Analysis (BIA) by the owner of a process, including identifying options time frames for alternate or manual workarounds.

In a good deal of the literature on this subject, RTO is spoken of as a complement of Recovery Point Objective (RPO), with the two metrics describing the limits of acceptable or "tolerable" ITSC performance in terms of *time lost* (RTO) from normal business process functioning, and in terms of data lost or not backed up during that period of time (RPO) respectively.[10][11]

Recovery Time Actual

A Forbes overview[8] noted that it is *Recovery Time Actual* (RTA) which is "the critical metric for business continuity and disaster recovery."

RTA is established during exercises or actual events. The business continuity group times rehearsals (or actuals) and makes needed refinements.[8][12]

Recovery Point Objective

A **Recovery Point Objective** (RPO) is defined by business continuity planning. It is the maximum targeted period in which data (transactions) might be lost from an IT service due to a major incident.[10]

If RPO is measured in minutes (or even a few hours), then in practice, off-site mirrored backups must be continuously maintained; a daily off-site backup on tape will not suffice.[13]

Relationship to Recovery Time Objective

Recovery that is not instantaneous will restore data/transactions over a period of time and do so without incurring significant risks or significant losses.[10]

RPO measures the maximum time period in which recent data might have been permanently lost in the event of a major incident and is not a direct measure of the quantity of such loss. For instance, if the BC plan is "restore up to last available backup", then the RPO is the maximum interval between such backup that has been safely vaulted off-site.

Business impact analysis is used to determine RPO for each service and RPO is not determined by the existent backup regime. When any level of preparation of off-site data is required, the period during which data might be lost often starts near the time of the beginning of the work to prepare backups, not the time the backups are taken off-site.[11]

Data synchronization points

Although a data synchronization point[14] is a point in time, the timing for performing the physical backup must be included. One approach used is to halt processing of an update queue, while a disk-to-disk copy is made. The backup[15] reflects the earlier time of that copy operation, not when the data is copied to tape or transmitted elsewhere.

How RTO and RPO values affect computer system design

RTO and the RPO must be balanced, taking business risk into account, along with all the other major system design criteria.[16]

RPO is tied to the times backups are sent offsite. Offsiting via synchronous copies to an offsite mirror allows for most unforeseen difficulty. Use of physical transportation for tapes (or other transportable media) comfortably covers some backup needs at a relatively low cost. Recovery can be enacted at a predetermined site. Shared offsite space and hardware completes the package needed.[17]

For high volumes of high value transaction data, the hardware can be split across two or more sites; splitting across geographic areas adds resiliency.

History

Planning for disaster recovery and information technology (IT) developed in the mid- to late 1970s as computer center managers began to recognize the dependence of their organizations on their computer systems.

At that time, most systems were batch-oriented mainframes. Another offsite mainframe could be loaded from backup tapes pending recovery of the primary site; downtime was relatively less critical.

The disaster recovery industry[18][19] developed to provide backup computer centers. One of the earliest such centers was located in Sri Lanka (Sungard Availability Services, 1978).[20][21]

During the 1980s and 90s, as internal corporate timesharing, online data entry and real-time processing grew, more availability of IT systems was needed.

Regulatory agencies became involved even before the rapid growth of the Internet during the 2000s; objectives of 2, 3, 4 or 5 nines (99.999%) were often mandated, and high-availability solutions for hot-site facilities were sought.

IT Service Continuity is essential for many organizations in the implementation of Business Continuity Management (BCM) and Information Security Management (ICM) and as part of the implementation and operation information security management as well as business continuity management as specified in ISO/IEC 27001 and ISO 22301 respectively.

The rise of cloud computing since 2010 continues that trend: nowadays, it matters even less where computing services are physically served, just so long as the network itself is sufficiently reliable (a separate issue, and less of a concern since modern networks are highly resilient by design). 'Recovery as a Service' (RaaS) is one of the security features or benefits of cloud computing being promoted by the Cloud Security Alliance.[22]

Classification of disasters

Disasters can be the result of three broad categories of threats and hazards. The first category is natural hazards that include acts of nature such as floods, hurricanes, tornadoes, earthquakes, and epidemics. The second category is technological hazards that include accidents or the failures of systems and structures such as pipeline explosions, transportation accidents, utility disruptions, dam failures, and accidental hazardous material releases. The third category is human-caused threats that include intentional acts such as active assailant attacks, chemical or biological attacks, cyber attacks against data or infrastructure, and sabotage. Preparedness measures for all categories and types of disasters fall into the five mission areas of prevention, protection, mitigation, response, and recovery.[23]

Importance of disaster recovery planning

Recent research supports the idea that implementing a more holistic pre-disaster planning approach is more cost-effective in the long run. Every $1 spent on hazard mitigation (such as a disaster recovery plan) saves society $4 in response and recovery costs.[24]

2015 disaster recovery statistics suggest that downtime lasting for one hour can cost

- small companies as much as $8,000,
- mid-size organizations $74,000, and

- large enterprises $700,000.[25]

As IT systems have become increasingly critical to the smooth operation of a company, and arguably the economy as a whole, the importance of ensuring the continued operation of those systems, and their rapid recovery, has increased. For example, of companies that had a major loss of business data, 43% never reopen and 29% close within two years. As a result, preparation for continuation or recovery of systems needs to be taken very seriously. This involves a significant investment of time and money with the aim of ensuring minimal losses in the event of a disruptive event.[26]

Control measures

Control measures are steps or mechanisms that can reduce or eliminate various threats for organizations. Different types of measures can be included in a disaster recovery plan (DRP).

Disaster recovery planning is a subset of a larger process known as business continuity planning and includes planning for resumption of applications, data, hardware, electronic communications (such as networking), and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication, and reputation protection and should refer to the disaster recovery plan (DRP) for IT-related infrastructure recovery/continuity.

IT disaster recovery control measures can be classified into the following three types:

1. Preventive measures – Controls aimed at preventing an event from occurring.
2. Detective measures – Controls aimed at detecting or discovering unwanted events.
3. Corrective measures – Controls aimed at correcting or restoring the system after a disaster or an event.

Good disaster recovery plan measures dictate that these three types of controls be documented and exercised regularly using so-called "DR tests".

Strategies

Prior to selecting a disaster recovery strategy, a disaster recovery planner first refers to their organization's business continuity plan, which should indicate the key metrics of Recovery Point Objective and Recovery Time Objective.[27] Metrics for business processes are then mapped to their systems and infrastructure.[28]

Failure to properly plan can extend the disaster's impact.[29] Once metrics have been mapped, the organization reviews the IT budget; RTO and RPO metrics must fit with the available budget. A cost-benefit analysis often dictates which disaster recovery measures are implemented.

Adding cloud-based backup to the benefits of local and offsite tape archiving, the *New York Times* wrote, "adds a layer of data protection."[30]

Common strategies for data protection include:

- backups made to tape and sent off-site at regular intervals
- backups made to disk on-site and automatically copied to off-site disk, or made directly to off-site disk
- replication of data to an off-site location, which overcomes the need to restore the data (only the systems then need to be restored or synchronized), often making use of storage area network (SAN) technology

- Private Cloud solutions which replicate the management data (VMs, Templates and disks) into the storage domains which are part of the private cloud setup. These management data are configured as an xml representation called OVF (Open Virtualization Format), and can be restored once a disaster occurs.
- Hybrid Cloud solutions that replicate both on-site and to off-site data centers. These solutions provide the ability to instantly fail-over to local on-site hardware, but in the event of a physical disaster, servers can be brought up in the cloud data centers as well.
- the use of high availability systems which keep both the data and system replicated off-site, enabling continuous access to systems and data, even after a disaster (often associated with cloud storage)[31]

In many cases, an organization may elect to use an outsourced disaster recovery provider to provide a stand-by site and systems rather than using their own remote facilities, increasingly via cloud computing.

In addition to preparing for the need to recover systems, organizations also implement precautionary measures with the objective of preventing a disaster in the first place. These may include:

- local mirrors of systems and/or data and use of disk protection technology such as RAID
- surge protectors — to minimize the effect of power surges on delicate electronic equipment
- use of an uninterruptible power supply (UPS) and/or backup generator to keep systems going in the event of a power failure
- fire prevention/mitigation systems such as alarms and fire extinguishers
- anti-virus software and other security measures

Disaster Recovery as a Service (DRaaS)

Disaster Recovery as a Service DRaaS is an arrangement with a third party, a vendor.[32] Commonly offered by Service Providers as part of their service portfolio.

Although vendor lists have been published, *disaster recovery* is not a product, it's a service, even though several large hardware vendors have developed mobile/modular offerings that can be installed and made operational in very short time.

- Cisco Systems[33]
- Google (Google Modular Data Center) has developed systems that could be used for this purpose.[34][35]
- Bull (mobull)[36]
- HP (Performance Optimized Datacenter)[37]
- Huawei (Container Data Center Solution),[38]
- IBM (Portable Modular Data Center)
- Schneider-Electric (Portable Modular Data Center)
- Sun Microsystems (Sun Modular Datacenter)[39]
- SunGard Availability Services
- ZTE Corporation

A modular data center connected to the power grid at a utility substation

See also

- Backup site
- Business continuity
- Business continuity planning
- Continuous data protection

- Disaster recovery plan
- Disaster response
- Emergency management
- High availability
- Information System Contingency Plan
- Real-time recovery
- Recovery Consistency Objective
- Remote backup service
- Virtual tape library
- BS 25999

References

1. *Systems and Operations Continuity: Disaster Recovery.* (http://continuity.georgetown.edu/dr/) Georgetown University. University Information Services. Retrieved 3 August 2012.
2. *Disaster Recovery and Business Continuity, version 2011.* (http://www-304.ibm.com/partnerworld/gsd/solutiondetails.do?solution=44832&expand=true&lc=en) Archived (https://web.archive.org/web/20130111203921/http://www-304.ibm.com/partnerworld/gsd/solutiondetails.do?solution=44832&expand=true&lc=en) January 11, 2013, at the Wayback Machine IBM. Retrieved 3 August 2012.
3. [1] (https://drii.org/whatisbcm) 'What is Business Continuity Management', DRI International, 2017
4. M. Niemimaa; Steven Buchanan (March 2017). "Information systems continuity process" (https://dl.acm.org/citation.cfm?id=3062955). *ACM.com (ACM Digital Library)*.
5. "2017 IT Service Continuity Directory" (https://www.drj.com/images/journal/fall-2017-volume30-issue3/2017_ITServiceDir.pdf) (PDF). *Disaster Recovery Journal*.
6. "Defending The Data Strata" (https://www.forbesmiddleeast.com/en/defending-the-data-strata). *ForbesMiddleEast.com*. December 24, 2013.
7. "ITIL glossary and abbreviations" (https://www.axelos.com/glossaries-of-terms).
8. "Like The NFL Draft, Is The Clock The Enemy Of Your Recovery Time" (https://www.forbes.com/sites/sungardas/2015/04/30/like-the-nfl-draft-is-the-clock-the-enemy-of-your-recovery-time-objective). *Forbes*. April 30, 2015.
9. "Three Reasons You Can't Meet Your Disaster Recovery Time" (https://www.forbes.com/sites/sungardas/2013/10/29/three-reasons-you-cant-meet-your-disaster-recovery-time-objectives). *Forbes*. October 10, 2013.
10. "Understanding RPO and RTO" (http://www.druva.com/blog/2008/03/22/understanding-rpo-and-rto). DRUVA. 2008. Retrieved February 13, 2013.
11. "How to fit RPO and RTO into your backup and recovery plans" (https://searchstorage.techtarget.com/feature/What-is-the-difference-between-RPO-and-RTO-from-a-backup-perspective). *SearchStorage*. Retrieved 2019-05-20.
12. "Clock... modifications
13. Richard May. "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.
14. "Data transfer and synchronization between mobile systems" (http://www.freepatentsonline.com/8442943.html). May 14, 2013.
15. "Amendment #5 to S-1" (https://www.sec.gov/Archives/edgar/data/1519917/000119312512125661/d179347ds1a.htm). *SEC.gov*. "real-time ... provide redundancy and back-up to ..."
16. Peter H. Gregory (2011-03-03). "Setting the Maximum Tolerable Downtime -- setting recovery objectives" (https://books.google.com/books?id=YC49DXW-_60C&pg=PA20). *IT Disaster Recovery Planning For Dummies*. Wiley. pp. 19–22. ISBN 978-1118050637.
17. William Caelli; Denis Longley (1989). *Information Security for Managers* (https://books.google.com/books?isbn=1349101370). p. 177. ISBN 1349101370.

18. "Catastrophe? It Can't Possibly Happen Here" (https://www.nytimes.com/1995/01/29/business/catastrophe-it-can-t-possibly-happen-here.html). *The New York Times*. January 29, 1995. ".. patient records"
19. "Commercial Property/Disaster Recovery" (https://www.nytimes.com/1994/10/09/realestate/commercial-property-disaster-recovery-business-whose-clients-hope-never-use-it.html). *NYTimes.com*. October 9, 1994. "...the disaster-recovery industry has grown to"
20. Charlie Taylor (June 30, 2015). "US tech firm Sungard announces 50 jobs for Dublin" (https://www.irishtimes.com/business/technology/us-tech-firm-sungard-announces-50-jobs-for-dublin-1.2267857). *The Irish Times*. "Sungard .. founded 1978"
21. Cassandra Mascarenhas (November 12, 2010). "SunGard to be a vital presence in the banking industry" (http://www.ft.lk/it-telecom-tech/sungard-to-be-a-vital-presence-in-the-banking-industry/50-7581). Wijeya Newspapers Ltd. "SunGard ... Sri Lanka’s future."
22. *SecaaS Category 9 // BCDR Implementation Guidance* (https://cloudsecurityalliance.org/download/secaas-category-9-bcdr-implementation-guidance/) CSA, retrieved 14 July 2014.
23. "Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR): Guide Comprehensive Preparedness Guide (CPG) 201, 3rd Edition" (https://www.fema.gov/media-library-data/1527613746699-fa31d9ade55988da1293192f1b18f4e3/CPG201Final20180525_508c.pdf) (PDF). US Department of Homeland Security. May 2018.
24. "Post-Disaster Recovery Planning Forum: How-To Guide, Prepared by Partnership for Disaster Resilience" (https://1.usa.gov/1IBkvv0). University of Oregon's Community Service Center, (C) 2007, www.OregonShowcase.org. Retrieved October 29, 2018.
25. "The Importance of Disaster Recovery" (http://www.techadvisory.org/2016/01/the-importance-of-disaster-recovery/). Retrieved October 29, 2018.
26. "IT Disaster Recovery Plan" (http://www.ready.gov/business/implementation/IT). FEMA. 25 October 2012. Retrieved 11 May 2013.
27. "Use of the Professional Practices framework to develop,implement,maintain a business continuity program can reduce the likelihood of significant gaps" (https://drii.org/resources/professionalpractices/EN). *DRI International*. 2021-08-16. Retrieved 2021-09-02.
28. Gregory, Peter. CISA Certified Information Systems Auditor All-in-One Exam Guide, 2009. ISBN 978-0-07-148755-9. Page 480.
29. "Five Mistakes That Can Kill a Disaster Recovery Plan" (https://web.archive.org/web/20130116112225/http://content.dell.com/us/en/enterprise/d/large-business/mistakes-that-kill-disaster.aspx). Dell.com. Archived from the original (http://content.dell.com/us/en/enterprise/d/large-business/mistakes-that-kill-disaster.aspx) on 2013-01-16. Retrieved 2012-06-22.
30. J. D. Biersdorfer (April 5, 2018). "Monitoring the Health of a Backup Drive" (https://www.nytimes.com/2018/04/05/technology/personaltech/backup-drive-health.html). *The New York Times*.
31. Brandon, John (23 June 2011). "How to Use the Cloud as a Disaster Recovery Strategy" (http://www.inc.com/guides/201106/how-to-use-the-cloud-as-a-disaster-recovery-strategy.html). *Inc*. Retrieved 11 May 2013.
32. "Disaster Recovery as a Service (DRaaS)" (https://searchdisasterrecovery.techtarget.com/definition/disaster-recovery-as-a-service-DRaaS).
33. "Info and video about Cisco's solution" (https://web.archive.org/web/20080519213241/http://www.datacenterknowledge.com/archives/2008/May/15/ciscos_mobile_emergency_data_center.html). Datacentreknowledge. May 15, 2007. Archived from the original (http://www.datacenterknowledge.com/archives/2008/May/15/ciscos_mobile_emergency_data_center.html) on 2008-05-19. Retrieved 2008-05-11.

34. Kraemer, Brian (June 11, 2008). "IBM's Project Big Green Takes Second Step" (https://web.archive.org/web/20080611114732/http://www.crn.com/hardware/208403225). ChannelWeb. Archived from the original (http://www.crn.com/hardware/208403225) on 2008-06-11. Retrieved 2008-05-11.
35. "Modular/Container Data Centers Procurement Guide: Optimizing for Energy Efficiency and Quick Deployment" (https://web.archive.org/web/20130531191212/http://hightech.lbl.gov/documents/data_centers/modular-dc-procurement-guide.pdf) (PDF). Archived from the original (http://hightech.lbl.gov/documents/data_centers/modular-dc-procurement-guide.pdf) (PDF) on 2013-05-31. Retrieved 2013-08-30.
36. Kidger, Daniel. "Mobull Plug and Boot Datacenter" (https://web.archive.org/web/20101119103409/http://bull.com/extreme-computing/mobull.html). Bull. Archived from the original (http://www.bull.com/extreme-computing/mobull.html) on 2010-11-19. Retrieved 2011-05-24.
37. "HP Performance Optimized Datacenter (POD) 20c and 40c - Product Overview" (https://web.archive.org/web/20150122213504/http://h18004.www1.hp.com/products/servers/solutions/datacentersolutions/pod/index.html). H18004.www1.hp.com. Archived from the original (http://h18004.www1.hp.com/products/servers/solutions/datacentersolutions/pod/index.html) on 2015-01-22. Retrieved 2013-08-30.
38. "Huawei's Container Data Center Solution" (http://www.huawei.com/ilink/enenterprise/download/HW_143893). Huawei. Retrieved 2014-05-17.
39. "Technical specs of Sun's Blackbox" (https://web.archive.org/web/20080513090300/http://www.sun.com/products/sunmd/s20/specifications.jsp). Archived from the original (http://www.sun.com/products/sunmd/s20/specifications.jsp) on 2008-05-13. Retrieved 2008-05-11.

Further reading

- Barnes, James (2001). *A guide to business continuity planning*. Chichester, NY: John Wiley. ISBN 9780470845431. OCLC 50321216 (https://www.worldcat.org/oclc/50321216).
- Bell, Judy Kay (2000). *Disaster survival planning : a practical guide for businesses*. Port Hueneme, CA, US: Disaster Survival Planning. ISBN 9780963058027. OCLC 45755917 (https://www.worldcat.org/oclc/45755917).
- Fulmer, Kenneth (2015). *Business Continuity Planning : a Step-by-Step Guide With Planning Forms*. Brookfield, CT: Rothstein Associates, Inc. ISBN 9781931332804. OCLC 712628907 (https://www.worldcat.org/oclc/712628907), 905750518 (https://www.worldcat.org/oclc/905750518), 1127407034 (https://www.worldcat.org/oclc/1127407034).
- DiMattia, Susan S (2001). "Planning for Continuity". *Library Journal*. **126** (19): 32–34. ISSN 0363-0277 (https://www.worldcat.org/issn/0363-0277). OCLC 425551440 (https://www.worldcat.org/oclc/425551440).
- Harney, John (July–August 2004). "Business Continuity and Disaster Recovery: Back Up Or Shut Down" (https://web.archive.org/web/20080204225856/http://www.edocmagazine.com/archives_articles.asp?ID=29114). *AIIM E-DOC Magazine*. ISSN 1544-3647 (https://www.worldcat.org/issn/1544-3647). OCLC 1058059544 (https://www.worldcat.org/oclc/1058059544). Archived from the original (http://www.edocmagazine.com/archives_articles.asp?ID=29114) on 2008-02-04.
- "ISO 22301:2019(en), Security and resilience — Business continuity management systems — Requirements" (https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en). ISO.
- "ISO/IEC 27001:2013(en) Information technology — Security techniques — Information security management systems — Requirements" (https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en). ISO.
- "ISO/IEC 27002:2013(en) Information technology — Security techniques — Code of practice for information security controls" (https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en). ISO.

External links

- "Glossary of terms for Business Continuity, Disaster Recovery and related data mirroring & z/OS storage technology solutions" (https://web.archive.org/web/20201114001623/https://recoveryspecialties.com/glossary.html). *recoveryspecialties.com*. Archived from the original (https://recoveryspecialties.com/glossary.html) on 2020-11-14. Retrieved 2021-09-02.
- "IT Disaster Recovery Plan" (https://www.ready.gov/it-disaster-recovery-plan). *Ready.gov*. Retrieved 2021-09-02.
- "RPO (Recovery Point Objective) Explained" (https://www.ibm.com/services/business-continuity/rpo). *IBM*. 2019-08-08. Retrieved 2021-09-02.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Disaster_recovery&oldid=1051009791"

This page was last edited on 21 October 2021, at 03:59 (UTC).