Disaster Recovery Planning in Business Continuity Planning

Tenshi C. Hara

Dresden University of Technology, Faculty of Computer Science,
Institute of Systems Architecture, Chair of Computer Networks,
% Dr.-Ing. W. Dargie, 01062 Dresden, Germany
hara@inf.tu-dresden.de

Abstract. IT-downtimes lead to severe financial losses. The necessity for business continuity and/or disaster recovery plans (BCP/DRP) is eminent as history (e.g. the 9/11-attacks) has shown, especially for small- and medium-sized businesses which are most vulnerable to financial losses in case of disasters. Even so, only 39% of these businesses actually have a BCP/DRP. Following the 9/11-attacks governments have issued BCP/DRP-standards in order to keep economy from damage. A key to a BCP/DRP is a well justified business impact analysis (BIA) utilizing economic monetary value results, also giving access to return on investment arguments for financial-appraisal. Results of BIAs are consolidated in a decision upon the design-goals of recovery time object (RTO) and recovery point objective (RPO). BCP/DRP-capabilities often are classified using Share's 7-Tier model and then augmented with RTO/RPO-capabilities. Further aspects given consideration are security and privacy, leading businesses to take their sphere of control into consideration and treat their BCP/DRP as business-secrets and not willing to share their information. This secrecy may be correlated to an exaggerated fear of terror-attacks. After creating a BCP/DRP respecting the security and privacy issues, testing must be conducted in an efficient way. Testing-results lead to changes in the initial analysis and design goals, closing the business continuity planning lifecycle. A rough idea of practical implementations is provided by the use-cases of a generalized banking-group, the administrative department of the alliance of Anna's cemeteries in Dresden, as well as the Swiss Data Safe AG.

Keywords: 7-Tier model by Share, business continuity planning, business continuity planning lifecycle, business impact analysis, disaster recovery planning, economic monetary value, IT-recovery, IT-continuity, return on investment, recovery point objective, recovery time objective, testing, BCP, BIA, BS 25999-1, DRP, EMV, ISO/IEC 27001:2005, NFPA 1600, ROI, RPO, RTO

1 Introduction

It is common knowledge that failures or downtimes in business-infrastructure can lead to severe financial loss for businesses. An estimated 50% of the loss to be expected is directly related to IT-infrastructure, whereas the remaining 50% are distributed over all remaining fields of business-infrastructure (such as man-power, etc.). The interesting questions to be answered for the first 50% from a business' point of view are whether resuming business operations or continuing service during a disaster is financially and technically acceptable, whether continuity and/or recovery plans for IT can be fit into plans for the entire business-processes, and finally, whether plans for IT shall or shall not closely cohere with other (eventually existing) disaster reaction plans. Therefore, the author wishes to discuss the necessity for business continuity and disaster recovery, the necessary steps in order to achieve guarantied[1] disaster recovery, the financial impact of disaster recovery, as well as some use-cases.

2 Necessity for recovery and continuity solutions

Ever since humans run businesses there has been necessity for recovery and continuity solutions. This may be true for field-commanders of ancient Rome issuing orders using multiple messengers simultaneously as means of a redundancy to achieve continuity during battle, or for businessmen in the 18th century making carbon copies of bills as means of backup to achieve restorability. Therefore, it is not astonishing that the same is true for information-age businesses. In the recent history the terrorist attacks of September 11th, 2001 have painfully proven the necessity for recovery solutions. From the view-point of redundant backup-systems, several businesses located within or in the proximity of the World Trade Center had their core IT-infrastructure inside the WTC buildings 1 and 2 or their close proximity, which were meant to be mutual backups for each other. Obviously, nobody expected both WTC-building ever to collapse at closely the same time and devastating the entire downtown of Manhattan, hence brokerage-businesses located in lower Manhattan were out of business for weeks, playing part in the worldwide financial system-collapse in the aftermath of the attacks. There were plans to keep businesses up, but they were all focused on a local scale as *their back-up plans were predicated on localized damage that was easily reparable within a week. Skeleton crews would simply maintain positions in small back-up facilities or other offices until it was safe to return* [Tra01]. After these events many businesses reevaluated their own disaster recovery plans as well as business continuity plans. The question was not about *whether*, but *how* to scale in means of spatial-extend. As an example, one can consider a creative approach to back up the entire data- and server-infrastructure inside a distant mountain, as done by Swiss *Festung Oberland* with their *Datenbunker*-facility in the Brindlistollen in Amsteg[2].

[1] We shall determine what a guaranty in this context is in the later course of this paper.

[2] This facility used to be a (fall-out) shelter for the federal council of Switzerland.

On a more topical note, the United States Small Business Administration[3] stated, that *America's [...] small businesses alone account for more than 99 percent of all companies with employees, employ 50% of all private sector workers and provide nearly 45 percent of the nation's payroll* [SBA06]. Taking this into consideration with their finding that *92 percent of [surveyed businesses] said it was very important or somewhat important for businesses to take steps to prepare for a catastrophic disaster, but only 39 percent said their company had a plan in place*[4], it is self-explanatory why SBA considers *small- to medium-sized businesses being the most vulnerable in the event of an emergency* [SBA06]. This fact may be the reason for the US government to have issued the Emergency Preparedness and Business Continuity Standard[5], which was developed by the National Fire Protection Association and endorsed by the American National Standards Institute (NIST). Also endorsing was the Department of Homeland Security (DHS) aiming on continuity and recoverability after terrorist-attacks. Contradicting the ideas of the NIST and especially the DHS, businesses must always consider security and privacy of business-secrets, which may be jeopardized when having redundant data-storage or IT-infrastructure outside the businesses direct sphere of influence (e.g. at a server-farm provided by a business-partner). Here it is imperative to find a compromise between necessity and risk.

So, as history has always shown, is currently showing, and most likely will always be showing, businesses have a clear demand for recovery and/or continuity solutions, contradicted by considerations of financial benefit, feasibility, security and privacy, availability of necessary spatial distribution, financial asset, man-power and commercial, readily usable solutions which might not meet all expectations, but may be cheaper in acquisition. Important questions to be answered could be, whether it is affordable to have recovery and/or continuity solutions at hand, what the magnitude of the financial loss in case of downtime is, what a solution to prevent downtimes costs, as well as whether there is a suitable compromise in costs.

3 Business continuity planning and disaster recovery planning

A key to answering the questions concluding the necessity-discussion is a *business impact analysis* (BIA) (refer to [Image 1]), especially for the last question, since a BIA compares potential costs in the aftermath of several downtime-scenarios and the costs for maintaining availability with means of recovery and/or continuity solutions.

3.1 Business impact analysis

Generally, in a BIA the cost of recovery and/or continuity solutions is directly calculated against possible losses and therefore leads to a savings potential in case of a

[3] http://www.sba.gov
[4] According to an October 2005 survey of small businesses conducted by The Ad Council.
[5] NFPA 1600

disaster. The assessment of potential losses and especially of disasters to take into consideration proofs to be difficult, since it is never possible to eliminate all risks. E.g. one could consider a burst pipe as a risk and optimize any reaction-plans to this, but this plan would not help against a hurricane. If now taking the hurricane into consideration, what would happen if a meteor crashes into Earth? And what if the Earth is totally devastated or destroyed following a meteorite shower? In the end one can always argument the impossibility of preparing for everything, so businesses must find a compromise and constitute risks which shall be accounted. A 2006 survey of the US National Archives and Records shows that 93% of business struck by a data outage of at least 10 days had to file for bankruptcy within one year (United States National Archives and Records, 2006). The maximum downtime suggested by the International Organization for Standards (ISO) should be short in means of a few days[6]. In the same year DataQuest quantified the mean financial loss for businesses with 17,784 USD per hour [Mar06] [Table 1].

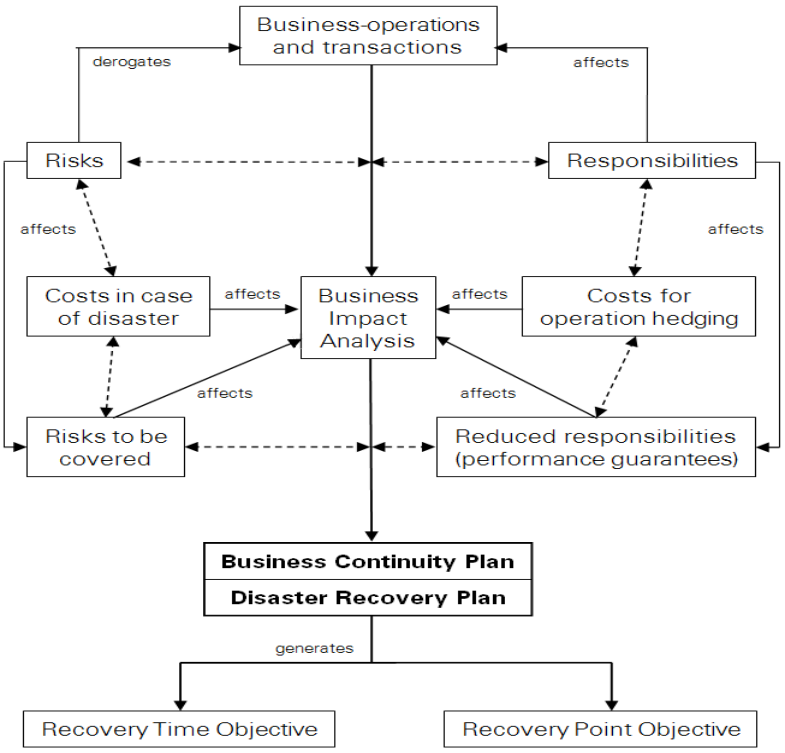

Image 1 Simple schematic of the steps from a running business via BIA to a working BCP and/or DRP including both design objects RTO and RPO.

[6] In order to achieve a minimum of downtime in means of availability of financial data, ISO 17799 suggests extensive rights for the government to quickly inspect documentation.

Taking these two numbers as rough ballpark figures, a maximum downtime of 3 days would cost a brokerage-business 360 million USD, leading to bankruptcy if the financial reserves are not sufficient. A simple IT-continuity solution based on *IBM Peer-to-Peer VTS* with only basic components would cost the business 40,000 USD[7]. Comparing these two numbers, the choice *for* recovery and continuity solutions is self-evident.

Industry	***IT Service***	***(COD/hour)/USD***
Financial	brokerage operations	6,450,000
Financial	credit card sales authorization	2,600,000
Financial	ATM-fees	14,500
Media	pay-per-view	150,000
Media	teleticket sales	69,000
Retail	home shopping	113,000
Retail	catalog sales	90,000
Transportation	airline reservations	89,000
Transportation	package shipping	28,000
	mean (COD/Hour)/USD:	17,784

Table 1 Cost of downtime (COD) per hour for various industries **[Mar06]**

In general one should be aware of the difference in the meanings of disaster recovery planning, business continuity planning, as well as IT-recovery and IT-continuity. The British Standards Institute suggests, that *business continuity planning is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted urgent functions within a predetermined time after a disaster or extended disruption* [BSI06] [ISO05], whereas they define *disaster recovery [as] the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. It is a subset of business continuity planning and shall include planning for resumption of applications, data, hardware and communications* [BSI06] [ISO05][8]. IT-recovery and IT-continuity on the other hand are design-goals within disaster recovery planning, with IT-recovery focusing on the complete, error-tolerant and verifiable restore of data and infrastructure, whereas IT-continuity focuses on the continued provision of services *during* a disaster and the adjacent data entry procedure after restoring normal system-state. On a mathematical basis, one can memorize the dependencies as follows:

$$IT\ recovery \subseteq Disaster\ Recovery \subseteq Business\ Continuity$$
$$IT\ continuity \subseteq Disaster\ Recovery \subseteq Business\ Continuity$$

[7] Rough figure by InRange dated September 2002. Contracts include a maintenance plan, which may lead to further costs in the years following the initial purchase.

[8] This is similarly suggested by an author in the DRP Wikipedia-article.

$$IT\ recovery\ \cap\ IT\ continuity \neq \emptyset$$

Taking the above facts into consideration the question arising now is how to get to an appropriate BIA. In an article published in 2008 Aaron Miller suggests a split into two arguments of financial-asset, the $economic\ utility\ argument$ and the $accounting\ argument$ [Pro08]. Both arguments are to be used in a combined manner when arguing the BIA and consequently the associated *business continuity plan* (BCP) and/or *disaster recovery plan* (DRP), as well as their reevaluation in following discussions, assuming a regular reevaluation to cut costs.

3.1.1 Economic utility argument

Aaron Miller suggests businesses shall value a standing BCP/DRP in the same way as prepaid insurance. From an economic point of view, any business creating and keeping a BCP/DRP ready for operation prepays into mitigating disaster expenses. In this manner, the value of the standing BCP/DRP can be calculated as

$$Total\ Benefit \cdot Probability = Economic\ Monetary\ Value\ (\mathrm{EMV})\ \text{[Pro08]}$$

Based on the result of this equation a business can determine whether the expenses for the standing BCP/DRP benefit the business or are unnecessary. If operation-costs of the standing BCP/DRP is less than its EMV, it is a worthy investment. If the costs are higher, the business wastes financial resources. Now, to how the economic utility argument works, assume the following scenario:

- A company has 500,000,000 € in annual revenue.
- The BCP shall prevent a risk affecting a quarter of its revenue (125,000,000 €) over four months, thus 31,250,000 €.
- The probability of the loss is 1.5%, thus 468,750 € (this is the actual EMV-output using the above formula).
- The BCP has annual operation-costs of 250,000 €.
- Additional annual BCP-costs (roughly estimated due to their inexact nature) run at 100,000 €

Putting these facts together and calculating with the EMV-output:

EMV	468,750 €
Well-planned BCP-costs	- 250,000 €
Additional BCP-costs	- 100,000 €
Utility of BCP	118,750 €

The example concludes with a positive annual economic utility for this company's BCP/DRP. Even with costs of 350,000 € and a low 1.5%-probability, the given BCP provides a gross utility of 118,750 €.

3.1.2 Accounting argument

When it comes down to recognizing BCP/DRP as an asset, it is questionable how to value it from an accounting point of view. One could argue, the economic utility equation is solid ground evaluating a BCP using a *return on investment* (ROI) calculation, but the inability to measure annual ROI of BCPs has put it armed with weak arguments when applying for financial resources and thus competing with other departments within the business. However, Miller suggests it is quite possible to fashion a robust ROI-calculation in ways of creating well-competitive arguments for BCP-managers. The basic ROI formula shall be given as:

$$ROI = \frac{Benefits\ -\ Costs}{Costs} \cdot 100\%$$ [Pro08]

Putting the values from the example in the economic utility argument into the equation, one can easily see that the calculation yields a 33.9% ROI:

$$\text{ROI} = \frac{468{,}750\ € - 350{,}000\ €}{350{,}000\ €} \cdot 100\% = \frac{19}{56} \cdot 100\% = 33.9\%$$

But, having a competitive argument also always holds the risk of follow-up counter-arguments, such as the question whether the business should spend less on its BCP/DRP in order to increasing its ROI and therefore economic utility. The board may suggest spending only 275,000 € on BCP/DRP-expenses, raising the economic utility to 193,750 € and thus lifting ROI to 70.4%. Luckily, a strong counter to this argument is the reduced likelihood of achieving the same EMV since the BCP/DRP might be reduced to a less effective solution. The reduced costs might therefore lead to a substantially lower EMV, in combination resulting in a proportionally lower ROI and thus economic utility, rather than a higher one. In the end, cost and utility are indeed strongly correlated.

3.2 Ideas by Share

In detail, businesses must determine what their primary objective for a BCP and – within this – a DRP is. Roughly, Share[9] classified DRPs into *Share's 7-Tier model*, which was introduced in the 1990s. The seven tiers defined are[10]:

- Tier 0: No off-site data (high possibility of no recovery)
- Tier 1: Data backup with no hot site[11] (cold site[12] possible)

[9] SHARE Inc. describes itself as *an independent, volunteer run association providing enterprise technology professionals with continuous education and training, valuable professional networking and effective industry influence.*

[10] An – compared to Share's initial description – easier to understand description of the tiers can be found e.g. on Wikipedia and shall not be provided here.

[11] A hot site is a redundant duplicate of the original site, matching the original infrastructure exactly or only in a reduced manner with fewer capabilities. Commonly it is implemented in the reduced manner since it must only bridge the outage-time of the original. Real time synchronization between the sites is practical. Normally the hot site is not in permanent standby (contrary to e.g. standby-routers within a HSRP-net), but in case of a disaster a hot site can

- Tier 2: Data backup with a hot site
- Tier 3: Electronic vaulting/bunkering
- Tier 4: Point-in-time copies
- Tier 5: Transaction integrity
- Tier 6: No or almost no data loss
- Tier 7: Highly automated and integrated solution

Other than one might expect, these layers are not based on each other and higher tiers do not necessary include the lower. This can lead to misunderstandings when businesses assume they are provided with certain services, which are actually not included in the solution they have determined for their tier of choice. At argumentum e contrario BCP/DRP solution-providers might use this misunderstanding to trick potential customers into – for the solution-provider – more profitable contracts, which is delicate especially when businesses have a smattering of BCP/DRP and are keen to cut costs as low as somehow possible. In the end, these businesses might end up in a situation with results equal to actually not having a BCP/DRP. On a more realistic note, one should acknowledge that any solution-provider not only interested in their customers' data safety, but actually their customers' business integrity (and therefore does not just simply want to earn money), will not seriously suggest any solution classified by Tier 4 or below. As a matter of fact, most of the time ready-to-use solutions with a sort of "turn on; works fine"-guarantee (classified by Tier 6 and 7) are the solutions of choice for sales.

3.3 Ideas thereinafter Share

As mentioned, the original concept by Share dates back to the 1990's, but still today, BCP-specialists and DRP-specialists continue to use the 7-Tier model to illustrate continuity capabilities and costs on a level understandable for end customers without expansive IT-knowledge. Following the original 7-Tier model, specialists today suggest a split into the goals *recovery time objective* (RTO) and *recovery point objective* (RPO), which are closely related to business' interests of continuity in business-processes. The strict disjunction of IT-recovery and IT-continuity is given up in favor of a merged solution-approach providing business-continuity on a larger scale.

3.3.1 Recovery time objective

RTO is defined as the duration of time within which, and a service level to which, a business process must be restored after a disaster in order to avoid an unacceptable break in business continuity. It focuses on the time for repair-attempts (without recov-

---

be up and running within a matter of hours. Personnel is not kept in redundant standby, so it may still have to be moved to the hot site, thus it is possible that the hot site operates autonomous before staff-relocation.

[12] A cold site does not include backups from the original and it does not have hardware already set up and thus is not quickly ready to use, requiring some time following the disaster to be up and running.

ery), a possible recovery and associated tests following these repair-attempts, as well as the information of the system-users. It does not respect decision-time for representatives. The RTO attaches to business-processes, not to the resources required to support the process, requiring BCP/DRP to take place on an abstract continuity-level, such as "the website must be continuously accessible" instead of "the one dedicated WWW-server (with IP-address 123.123.123.123) must be continuously accessible".

Desired RTO is often seen to be Zero, but in practice often implemented "as close to Zero as financially possible", making its implementation directly correlated to businesses' readiness to spend, and – on a more profound level – the financial importance of the business-processes to be protected. The rough rule of thumb here is: The more important the business-process at risk, the higher the expenditure for RTO being within the neighborhood of Zero.

3.3.2 Recovery point objective

RPO on the other hand describes the acceptable amount of data loss measured on a time-based scale. Therefore, it is defined as a point in time to which data is to be recovered. Typically, this is a specification of an acceptable loss in a disaster situation. The calculation of RPOs is straight forward for replication elements. Typically, the RPO is measured in seconds (physical measurand) or dirty track-entries, which changed in the master copy but not in the replica (transcendent measurand). Measuring RPO for entire data sets such as database or application data (both actually based on physically stored data within a file-system or on transcendent data within the RAM) is more complex and requires usage of the lowest common denominator possible of all physical elements involved protecting the logical data set.

Typically, RPO is the default design-goal in any database-architecture (e.g. Oracle), with it being close to zero for a bank with thousands of transactions per minute, with each transaction itself being imperatively important (any mustn't be lost), or just covering the temporal difference between two shipments from a depository, in which the stock can be easily recounted after a loss of data. The rough rule of thumb here is: The more attached business-processes' importance is to transaction-level, the higher the expenditure for RPO being within the neighborhood of Zero.

3.4 Security and privacy issues

After deciding upon design-goals and maximum expenses ready to pay, a business must still evaluate further interconnected factors. Most businesses will have some sort of company-secrets not to be shared with concurring businesses, or – in a not so core-secretive manner – data of privacy, which shall not be shared publicly. Having data or infrastructure redundantly always leads to additional work and expense maintaining these redundant structures as secure as the primaries in the business' direct access. If redundancy is achieved by means of not only duplicating, but also distributing remotely, work and expense will rise up further since security-means cannot be reused as true for redundant structures within the same sphere of security-control. Shall the redundant structures not only be distributed, but additionally be provided by business-

associates instead of the business itself, secrecy and privacy of the business' resources are at stake, especially in the case of the provider providing its services to several partners chaffering in the same field.

On a more abstract level, one can also consider businesses' continuity and recovery preparations and BCPs/DRPs a matter of privacy itself. There seems to be an eminent fear of information about BCPs/DRPs leaking out of a business' sphere of control, leading to BCPs/DRPs being considered business-secrets. While creating this paper, the author experienced severe difficulties in finding businesses and providers willing to share their continuity and recovery solutions in a detailed matter. Mostly information is limited to relative specifications rather than absolute numbers, or implementation details are covert behind abstracted structural schemas. Out of 17 contacted businesses only 2 replied with useful BCP/DRP-data and from 6 contacted solution-providers only one actually replied, whereas the reply itself contained only vague information. This impression is supported by the fact that the contacted businesses were even more cautious when asked for material backing up their information (such as financial asset data or blueprints and engineering detail drawings of their continuity- and/or recovery-solutions). This behavior may be correlated with the exaggerated fear of terror-attacks[13], leading to most businesses being afraid of larger damages to their business in case of terrorists knowing about their BCP/DRP and therefore focusing their attacks on key-elements of the BCP/DRP-solution. This can be considered an actual threat, having attackers focusing their attacks not on the infrastructure itself, but rather on the measures taken to counter such an attack. This type of attack can be considered as *BCP -focused attack.*

3.5 Steps required after BCP/DRP-creation

Even after taking all aspects of the previous steps into consideration many businesses do not actually have a working BCP/DRP-solution. In theory their BCP/DRP may be able to prevail against any thinkable disaster[14], but in practice it might fail. The reason for this is that many businesses forget the probably most important step of BCP/DRP-creation: testing. But, even if businesses test their newly created BCP/DRP, most testing is limited to one initial test, since periodic testing of continuity and recovery procedures leads to additional expenses. These additional expenses may be the result of hardware-replacements, travel to cold site centers, real downtimes due to lack of aptitude to simulate certain circumstances or just basically the personnel costs (a simple testing-schema can be seen in [Image 2]). What is generally forgotten is, regular testing leads to a training-effect, preparing all affected resources (most importantly the employees) to face actual recovery challenges, making their response more effi-

[13] Following the 9/11-attacks the US-government introduced an easy to understand, color-based terror-risk information board, which actually – according to Michael Moore – never showed a low or non-existent risk in the years following the attacks. On the contrary, statistics do not show an elevated risk of attacks against businesses; this fact only exists for government-facilities.

[14] "Thinkable" as defined by the BIA.

cient As true for the arguments in the BIA, it is difficult for IT-experts to justify testing-expenses when facing the board. Harry L. Waldron comments on this: *The severity rather than the frequency of loss is what can be used to justify the additional expenses associated with disaster recovery planning and testing. In a worst-case scenario, information critical to the business may be permanently lost* [Wal08].

In order to achieve a maximum gain from each test, Waldron suggests following a disaster recovery testing checklist, containing 7 simple steps to success [Wal08]:

- Gain the support of top management for the business continuity process.
- Set an annual date for reviewing and updating the disaster recovery plan.
- Obtain specific training for how to recover the infrastructure.
- Allow plenty to time to work out production problems, as resources permit.
- Don't try to test everything at once.
- Use principles of continuous improvement based on testing feedback to ensure that plans stay up to date.
- Integrate disaster recovery into the change management process. That way, when new systems are implemented, they are also protected.

The testing designed like this must be an integrated, non-negligible part of maintaining any part of the infrastructure at base. Benefit of testing is hardly quantifiable, but its costs are still easier to calculate than the potential loss in case of a disaster and the following – due to missing testing and training – improper recovery process, which most definitely leads to more severe financial damage than the initial disaster.

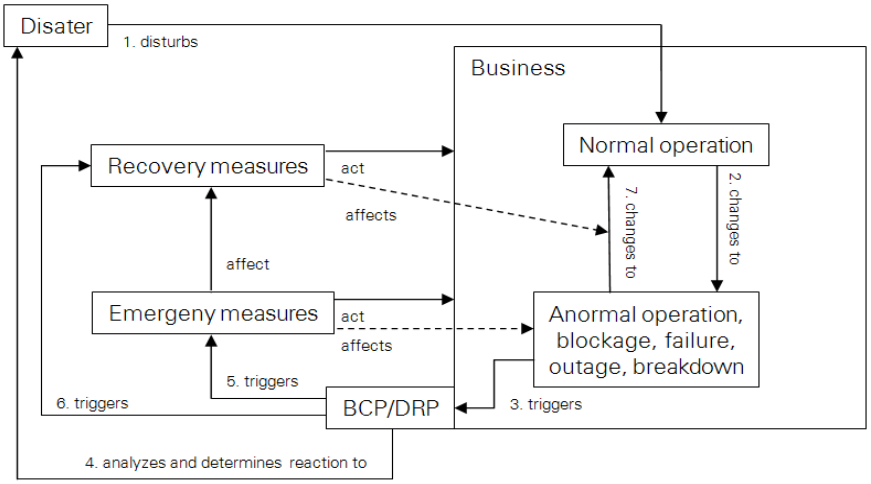

Image 2 Simple testing-schema to ensure functionality of the BCP/DRP

In a final step after testing, businesses must evaluate the results of the tests. No test is worthy of conduction if the results are left unread. Test-results are a key to ensure adaptability and adaptivity of the existing infrastructure and its continuity- and recovery-capabilities to changes in the infrastructure. Also, the regular tests of the entire BCP/DRP ensure the compatibility of smaller parts of the BCP/DRP-infrastructure, if

these are maintained and extended individually. This is especially true for management-approaches in which the basic infrastructure is modified in small dimensions leading to resulting small-scale changes in BCP/DRP-processes, followed by small-scale tests of compatibility and positive results on the small scale. But, these small-scale results do not give a combined result for the entire BCP/DRP-processes on well founded facts, which can only – if possible – be provided by a global-scale test.

3.6 Closing the business continuity planning lifecycle

In a keen on continuous optimization business, testing-results will lead to changes in the BCP/DRP-infrastructure, which then need to be analyzed and tested again. In optimal implementation, business continuity planning is a constant process following the lifecycle of analysis→design→implementation→testing→maintenance→analysis, with the closure of the circle letting it start over again. In this lifecycle, any of the earlier mentioned pillars of business continuity planning are reevaluated, possibly causing changes in the BIA, the RPO or the RTO.

3.7 Dependencies on surroundings

As a side-note to the steps to be taken while assembling a useful BCP/DRP, one should consider dependencies on surrounding. There might be influences of any nature within geography, politics, ethnics, demographics, etc. which need to be taken into consideration.

An example for such surroundings can be seen in the city of Dresden, Saxony. In 2002 a 100-year flood of the Elbe River struck great parts of Europe, leaving yet alone Saxony with an estimated damage of $8.6 \cdot 10^9$ € [Kup09]. In the years following the flood, designated areas of the city have been declared building-free zones, prohibiting any construction work to take place within those areas. Also, the city-area has been categorized into several endangering-zones, orienting the classification depending on the flood-levels of the 1845 and 2002 floods (refer to [Image 3] and [Image 4]) as well as the (directly and indirectly) affected areas of the 2002 flood.

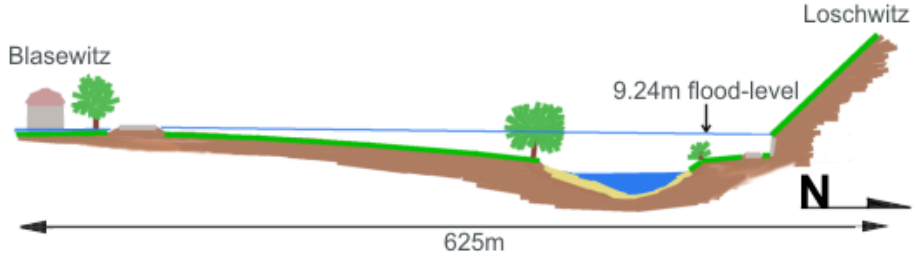

Image 3 Lateral cut of the riparian areas at Dresden's Elbwiesen with 2002 flood-level. Published Feb. 14, 2005 under Creative Commons License 3.0; cc-by-sa

As a result, this classification leads to many areas of the city being considered *extremely endangered* within a gauge of 8m, *endangered* within the range from 8m to 10m, *marginally endangered* within the range from 10m to 11m and *not endangered*

above 11m[15]. The crux about the classification is the fact that businesses planning to build within the city-area are not adverted to the existing classification of the desired building-area of its own volition, but are actually only adverted when explicitly asking for the classification[16]. Another crux might be the fact of the city actually preparing flood-protection barricades when acknowledging the risk of a flood, but not actively prompting businesses to start their BCP/DRP-preparations in order to quickly respond to damages caused by a potential flooding. This lack of centralized (government triggered) propagation of the information leads to the imperative necessity for businesses to actively seek for these information themselves (e.g. by regularly checking the city's website[17]).

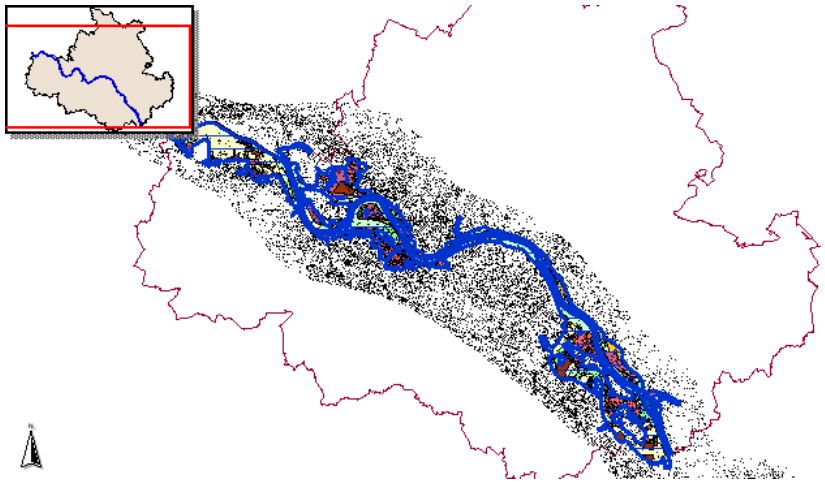

Image 4 Areas of Dresden directly and indirectly affected by the 2002 flood (blue: Elbe River; red: city limits; black: affected areas).

4 Strategies followed

Both, RTO and RPO emerge during the creation of the BIA and do not exclude each other. The question to be answered is more likely, whether RTO and RPO can be obtained in parallel, or if a compromise must be found.

---

[15] There are regional deviations depending on existing buildings and topology.

[16] As a matter of fact, construction of new buildings within the extremely endangered areas is prohibited, so one would actually be adverted to the classification within the denial.

[17] The gauge of the Elbe is presented on the city's website www.dresden.de as well as on a special website of the *Bundesministerium für Verkehr, Bau und Stadtentwicklung* (Federal Department of Traffic, Contruction and Urban Development) under: http://www.pegelonline.wsv.de/webservices/zeitreihe/visualisierung?pegelnummer=501060&ansicht=einzeln

The easy answer is definitely "yes", with one simply looking at solutions used by major banking groups, for which it is important, to have continuity in no-time (RTO = 0; fully automated repair- and recovery-attempts) without any loss of transactions (RPO = 0). But, looking closely at this easy answer, one should wonder about the costs involved. On one hand, banking groups are oblique to minimal outage-times with catastrophic outcomes if violated, justifying immense expenditures for BCP/DRP-solutions. On the other hand, banking groups earn with each single transaction, meaning this base of income must be protected at (almost) any cost, justifying branching off e.g. 4% of transaction-profits towards BCP/DRP-expenses. One must consider the demand for instantaneous recovery and continuous service for businesses relying on real-time business. → Sadly, the author was not able to obtain useful data upon this strategy from the answers provided by contacted banking-groups. We will therefore have a look at a general example for this strategy consolidated upon the intersecting aspects of the answers provided [see page 14, heading 4.1].

The more complex answer is a "maybe" with a tendency to "one shouldn't". A business relying on day-end closing or even only month-end closing will definitely not require an instantaneous recovery; it may be sufficient to recover just in time before the next closing, or – if paper-work can fulfill data-continuity – recover before the next major closing-deadline (e.g. the next audit by the tax office). If this business relies on customers filling in orders via a web-based service, continuity for this service may be desirable, but it might be sufficient for it to be restorable within several hours. A business relying totally on human-interaction (e.g. face-to-face meetings or telephone-calls) might have the dictum of having continuous telephone-roaming, whereas the business' website may be down for several days or weeks. → We will have a look at an example for this strategy when looking at the similar strategy followed by the administrative department of the alliance of Anna's cemeteries in Dresden (Dresden, Germany; *Verband der Annenfriedhöfe Dresden*) [see page 15, heading 4.2].

The most complex answer would be a "definitely yes" when looking from the view-point of a BCP/DRP-solution provider. From the provider's side, both objectives must be obtained for themselves in order to be able to provide them simultaneously or in separatly. Or, in more general terms: In order to provide failsafe, the provider must have a failsafe themselves. → We will have a look at a BCP/DRP-provider using the short[18] example of *Swiss Data Safe AG* [see page 17, heading 4.3].

4.1 Real-time continuity, immediate recovery (RPO=RTO=0): Consolidated aspects of banking-groups

Any bank or banking-group is subject of strict government requirements and demand. At any time customers must be assured payout of monetary values (up to a certain amount specified by law), redemption of insurances, availability of services, and most importantly vested execution of transactions. Apart from human-error risky invest-

[18] Due to an obvious non-disclosure policy, the example has to stay reduced to data which can be promulgated in public.

ments, the first two can be guaranteed as long as the latter two are present. Therefore, continuity and recovery must be focused on availability of services (RTO=0) and transaction-integrity (RPO=0).

In order to achieve either RTO=0 or RPO=0 the first and logical step is investing in own infrastructure. Banks depending on infrastructure shared with or provided by business-associates are always at risk of losing service-availability. The second step is the enforcement of hot sites, 24/7-redundancy and most importantly 24/7-readiness amongst decision-makers. Obviously the last enforcement is not human-doable, therefore forcing banking-groups to actually choose a Tier-7-solution, thus this is the only level of solution which does not require human interaction in the moment a disaster occurs or the moments right after it. The problem in implementing the Tier-7-solution is the determination of which decisions to take ex ante in order to virtually provide 24/7-readiness of decision-makers, de facto finding an answer to the question what to decide upon overcoming a disaster-situation beforehand without actually knowing what the actual (future) disaster will look like. Essential to finding a solution for this dilemma is profound evaluation of possible disaster-scenarios, since it is proven to be impossible to find one single strategy which answers to all situations which may occur during a disaster. The tricky part is the creation of a decision-algorithm, which identifies the disaster(s) occurred and commencing the necessary steps in coping, but also evaluating the result of the steps and – if necessary – adapt to a change of situation in the result. A final question to be answered is the problem of remoteness, dealing with the problem of the influence-radius of expected disasters, without wasting money due to immoderate spatial distance and conjoint with it possible altering legal constraints. A European bank keen on keeping customer-data secret will certainly abstain from placing a backup-facility in the USA, since legal constraints in the US would allow public authorities to access the backup-data and therefore obtain the valued customer-data[19].

4.2 Delayed continuity, deferred recovery (RPO=RPO≠0): Administrative department of the alliance of Anna's Cemeteries in Dresden (Dresden, Germany)

The City of Dresden in Saxony hosts several cemeteries within the city-limits, out of which three (the Old and New Anna's Cemeteries (*Alter Annenfriedhof*, *Neuer Annenfriedhof*[20]) and the Cemetery of Peace and Hope (*Friedhof Frieden und Hoff-*

[19] The US-government pressures banks and other governments to guarantee accessibility of bank-data to (US) public authorities, leading to a treaty signed by the EU and the US to actually grant the US public authorities almost unrestricted access to European banking-data. For this reason the Society for Worldwide Interbank Financial Telecommunication (SWIFT) is moving their BIC/IBAN-Servers from the USA to sites in Switzerland, which is not part of the European Union.

[20] Anna's cemeteries are named not after St. Anna, but after Princess Anna of Denmark and Norway (a.k.a. "Mother Anna"), Prince-Elector of Saxony (as Prince-Elector in the Holy Roman Empire), * 11/22/1532, † 10/01/1585.

nung[21]) are administrated by the administrative department of the alliance of Anna's cemeteries. Department-administration is centralized within facilities of the New Anna's Cemetery, where as facility-administration is distributed over the cemeteries. All active data concerning graves, finances, employee-management, facility-management, etc. is handled on ordinary desktop-PCs (no central server; one PC functions as database-sharing partner to the others) with paper-backup, whereas older data (in general all data before the collapse of the GDR[22]) exists in paper-form only. In means of definition, the phrase IT-infrastructure shall only cover the desktop-PCs and networking-elements within the cemeteries facilities. Telephone and internet are not covered since they are assumed not imperative for business-operations since an employee can always carry data on a external device (e.g. USB-stick or HDD) to the other facilities. Power-supply is considered continuous and stable and expected outage-times are to be short. Therefore, no UPS-units are in place. Procedure following a power-outage is equal to the procedure following an IT-outage with the advantage of having application-based backups of the dataset's state at the time the outage occurred (which would be inaccessible following an IT-outage). Business continuity is eminent during opening-hours of the cemeteries offices so that bereaved persons are not sent away due to e.g. computer-problems. Continuity is achieved seamless by simply using pen and paper with the obligation of entering the collected data into the (by then repaired) IT-system later. Closure can be done without working IT-recourses for existing accounting-data, but may take some time. For data within the IT-based database not copied to paper yet no closure can be done. RTO in this case is "as soon as possible with low costs", RPO equals "last data-set entered completely before the crash", abolishing any data partially entered or saved at crash-time. Since all paper-backups are stored at almost the same location as the PCs are set up (within the same level of the same building), continuity can obviously only be provided as long as the office is accessible and physically undamaged. Hazards are limited to fire (and conjoining extinguishing-attempts) with the BIA (and therefore also BCP) assuming impossibility of floods due to the elevation of the cemeteries areas [see endangerment classification on page 12, heading 3.6] as well as the historical proof of never having the cemeteries flooded, impossibility of traffic-exposure due to hardened walls and storage at walls opposing passing traffic as well as the locations of the cemeteries being off-sides typical approach and departure routes of the Dresden International Airport, and the impossibility of theft due to the missing attractiveness of the stored paper-backups (this may exclude the financial data; assumption suggests nobody wanting to steal and carry several hundredweights of old books) and dispensability of the PCs (assuming that all data entered during normal office-hours are copied to the paper-backup at the end of the day). As long as no fire destroys the paper-based backups, all business-processes can be restored on any hardware and any software providing the necessary

[21] Actually, this is one cemetery providing services toward two communities in parallel: the Church of Peace (*Gemeinde der Friedenskirche*) on the one side and the Church of Hope (*Gemeinde der Hoffnungskirche*) on the other.

[22] The German Democratic Republic collapsed in 1990 leading to changes in business-processes within the cemeteries administration and IT-upgrades in the middle and end of the 1990s. The current IT-infrastructure originates in the late 1990s and early 2000s.

functionality, where as in the moment the paper-backups are destroyed, all data prior to digitalization is irrecoverable lost and, if the IT-infrastructure is lost at the same time, all data is lost for good, leading to business being forced to continue with new data only, which would be a total catastrophe for the cemetery-administration[23].

As a result of the BIA seeing no actual threat to continuity or recoverability of IT-infrastructure, BCP/DRP-expenses are kept on a minimal level. Actual expenses are reduced to an IT-expert costing 40 € (~60 USD) per quarter, a bureau-license of *Kaspersky Internet Security at 60 € (~90 USD)* [Kas09] per year as well as approximately 300 € (~449 USD) consolidated within a repair-funds from which hardware repairs or replacements and special expenses are paid. The total asset sums up to approximately 400 € (~599 USD)[24].

4.3 Solution-provider: Swiss Data Safe AG[25]

Swiss Data Safe AG provides solutions and services for housing & hosting, storage, backup, archive, data-management, physical storing and ESCROW[26]. The facilities used are placed in hardened bunkers within mountains in the Swiss Alps (one inside the Brindlistollen mentioned in heading 2 [see page 2]; also refer to [Image 5]), physically detached and separated by 30km of distance as flown by birds. Each facility is connected to the WWW using several, redundant connections and is able to maintain operational even if the outside world should sustain severe outages. It may even preserve data over a nuclear incident due to EMP[27]-resistivity. RTO=0 and RPO=0 are achieved by hot standby solutions using different sorts of raids and redundancy on all levels of consideration (telecommunications-infrastructure, IT-hardware, operating-software, applications used). *Swiss Data Safe AG* is a good example for the genuine practice of providing BCP/DRP-solutions capable of resisting considerable kinds of disasters under compliance to international standards (such as [BSI06]), but at the same time keeping any details as secretive as possible. The obvious conclusion to be drawn is the existence of a "we deliver what you need, but don't ask how it works"-mentality.

---

[23] In Germany graves are not allocated for eternity, but for a limited time only, and this only, if a yearly expense loading is paid. Contrary to this, older graves (mostly from the founding-times of the cemeteries) have an eternal allocation-right. → When all data on existing graves should be lost, nobody would know about the allocation-rights of any existing grave.

[24] All approximated USD-values based on exchange-rates as of November 16th, 2009.

[25] Due to an obvious non-disclosure policy, the example has to stay reduced to data which can be promulgated in public; technical details are very hard to obtain, therefore the author wishes to on focus on available data.

[26] ESCROW is an account established by a broker, for the purpose of holding funds until the consummation or termination of a transaction, or it is a trust account to pay obligations such as property taxes and insurance premiums.

[27] An electro-magnetic pulse is proven to occur with nuclear explosions and is able to disable any electronic device within its optical range (in means of visibility on the EMP's wavelength, not the spectrum visible to humans).

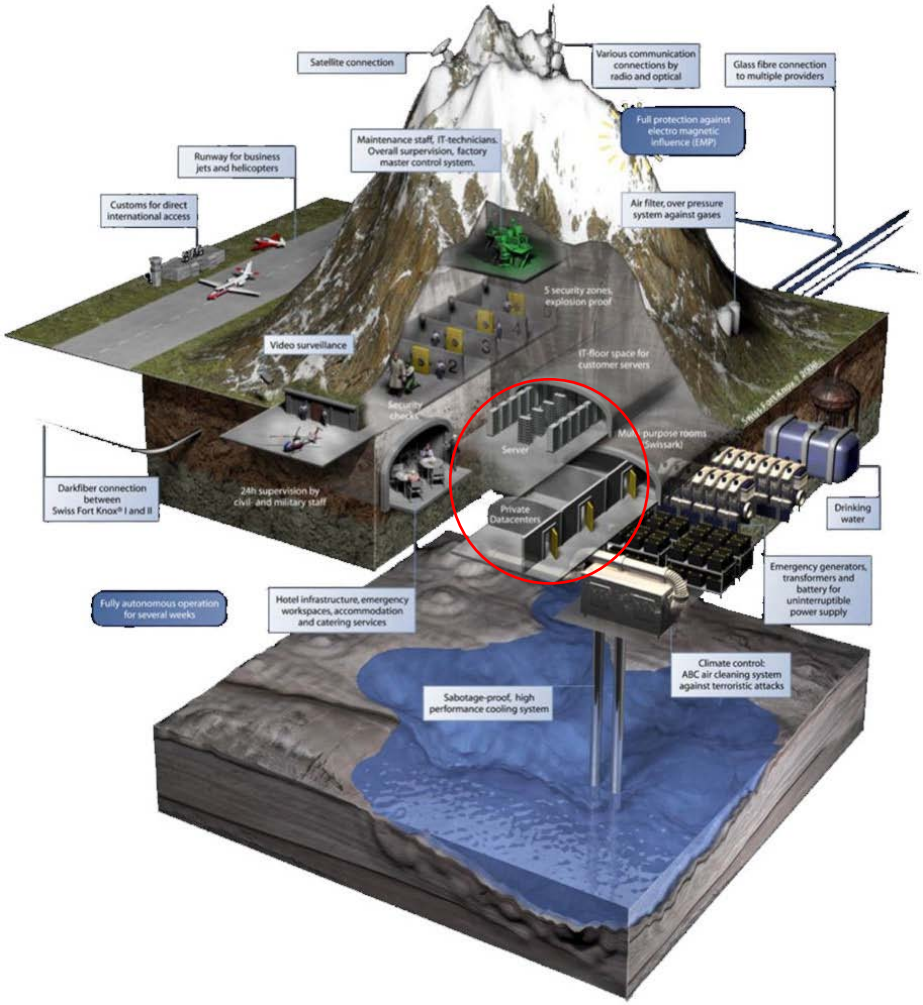

Image 5 Schematics of the Brindlistollen; within the red circled area are located the actual facilities within the mountain used by civil data-centers such as Swiss Data Safa AG. © Hans Rudolf Schneider (www.festung-oberland.ch); SIAG

5 Conclusion and outlook

Business continuity planning and disaster recovery planning are – if measures are taken – inextricably interlaced, thus this paper often used the term *BCP/DRP*. This "if" is an important one since government regulations suggest the existence of standing plans within "important" businesses, but many businesses actually do not take the necessary steps in order to have a BCP/DRP, with a better part of those taking steps having ineffective plans. Businesses taking the necessary steps actually are very de-

pendent on IT, leaving the impression that BCP/DRP-measures are often only taken when IT is directly involved. After the 9/11-attacks BCP/DRP-expenses have risen, but there is no actual proof for a higher risk of disasters. In contrast, businesses slowly start recognizing the importance of IT-readiness for disasters, being ready to actually invest into BCP/DRP-infrastructure. Even though research in the field of BCP/DRP is not topical, the current secrecy of solution-providers and solution-users (obviously due to fear of espionage or terror) combined with the future demand for disaster-readiness the author assesses a necessity of academic research in this field to prepare future system-administrators for the tasks awaiting them when creating continuity- and recovery-solutions.

6 References

[BSI06] British Standards Institute. BS 25999-1, BS 25999-1. *Standard.* 2006.

[ISO05] International Organization for Standardization. ISO/IEC 27001:2005. *Standard.* 2005.

[Kas09] Kaspersky Lab. Kaspersky Lab: Anti-Virus, Internet Security, Mobile Security & Antiviren-Software und Services für Unternehmen. http://www.kaspersky.de.

[Kup09] Kupfer, Frank (Saxonian Secretary of Environment). Bericht über die Folgen des Elbe-Hochwassers im September 2002. Dresden, 08/05/2009.

[Mar06] Marquis, Hank. The Paradox of the 9s. 2006. http://www.itsmsolutions.com/newsletters/DITYvol2iss47.htm.

[Pro08] Miller, Aaron (Protiviti Inc.). From Expense to Asset. *KnowledgeLeader.* 2008.

[Tra01] Traders. Thinking the Unthinkable - Trading Firms Look for Backups Sites. October 1, 2001.

[NAR06] United States National Archives and Records. *2006 Annual NARA-report.*

[SBA06] United States Small Business Administration. How to prepare for Disaster. *SBA Small Business Resource.* Summer 2006.

[Wal08] Waldron, Harry L. Windows Tips. *Testing Windows disaster recovery plans.* 02 14, 2008. http://searchwinit.techtarget.com/tip/0,289483,sid1_gci1299649,00.html.

7 Glossary of abbreviations

A

ATM	automatic teller machine Automated machine used to draw money from a bank-account using only an identification card and a personal identification number (PIN) (also used: “ABM” for automatic banking machine)

B

BCP	business continuity plan/planning Plan of actions to take affect while business interruptions in order to maintain business operations and continue services, or the steps required to creating the plan
BIA	business impact analysis Analysis of costs in case of business interruptions and often also of the benefits of having a continuity or recovery solution
BS 25999	British Standards Institute definition on business continuity
BSI	British Standards Institute

C

COD	costs of downtime Expected/calculated or proven financial impact of downtimes to businesses

D

DRP	disaster recovery plan/planning Plan of events to take affect while business interruptions in order to recover from the interruption and restore normal business processes, or the steps required to creating the plan

E

EMV	economic monetary value Actual cost-benefit-calculation within a business impact analysis

I

IEC	International Electrotechnical Commission
ISO/IEC 27001:2005	International Organization for Standardization definition on information technology, security techniques, information security management systems, as well as their requirements
ISO	International Organization for Standardization

N

NARA	United States National Archives and Records
NFPA 1600	National Fire Protection Association standard on disaster/emergency management and business continuity programs
NFPA	National Fire Protection Association

R

ROI	return on investment Used to evaluate the efficiency of an investment in finance/economics
RPO	recovery point objective Duration within which, and a service level to which, business processes must be restored after a disaster in order to avoid an unacceptable break in business continuity
RTO	recovery time objective Point in time to which data must be recovered after a disaster in order to avoid an unacceptable loss of business-data management

S

SBA	United States Small Business Association

U

USD	United States Dollar The currency of the United States of America (a.k.a. US-$ or just $)

W

WTC	World Trade Center Within this paper only the building-complex in lower Manhattan of New York City, NY (USA) as of 2001