DISASTER RECOVERY AND BUSINESS CONTINUITY: A SHORT INTRODUCTION

Few things concern operational and technical staff more than major outages and technical failures. These, and disasters affecting the ability to remain in control, are the subjects of disaster recovery and business continuity planning. In this article, **Stefan Maes** gives a short introduction, relevant to all of us who depend on IT for business operations.

KEY POINTS

- **Disaster recovery and business continuity are closely related, but differ in scope.**
- **Disaster recovery is the process of making all important IT infrastructure and operations available again following an outage, whereas the business continuity process focuses on the business applications (IT centric vs application centric).**
- **Different solutions will have to be put in place depending on business needs and budget and technology availability.**
- **Building a disaster recovery and business continuity plan is not sufficient: it needs to be continuously rehearsed, reviewed, refined, and retested.**

"What to do if they discover World War II ordnance and we have to evacuate our site, in part or as a whole, for its safe disposal?" This was one of the questions we in EUROCONTROL asked ourselves before the start of the excavation works for the construction of the new NM Operations Centre. The answer was quickly found as it was already documented in EUROCONTROL's disaster recovery plan. Following a risk assessment, some disaster recovery procedures have been activated as a precautionary measure.

Disaster recovery and business continuity

Today, IT is essential to almost all business operations, and for that reason, it is at the centre of business continuity and disaster recovery planning. While closely related, disaster recovery and business continuity are not the same thing. The key difference between the two is in their scope. Disaster recovery is the process of getting all important IT infrastructure (data, servers, software, applications, operating systems, etc.) and operations up and running following an outage or disaster.

The following types of outages are typically considered for a disaster recovery scenario:

- computer systems and services failures,
- power outages and power failure, and
- natural disasters (earthquake, fire, floods, etc.).

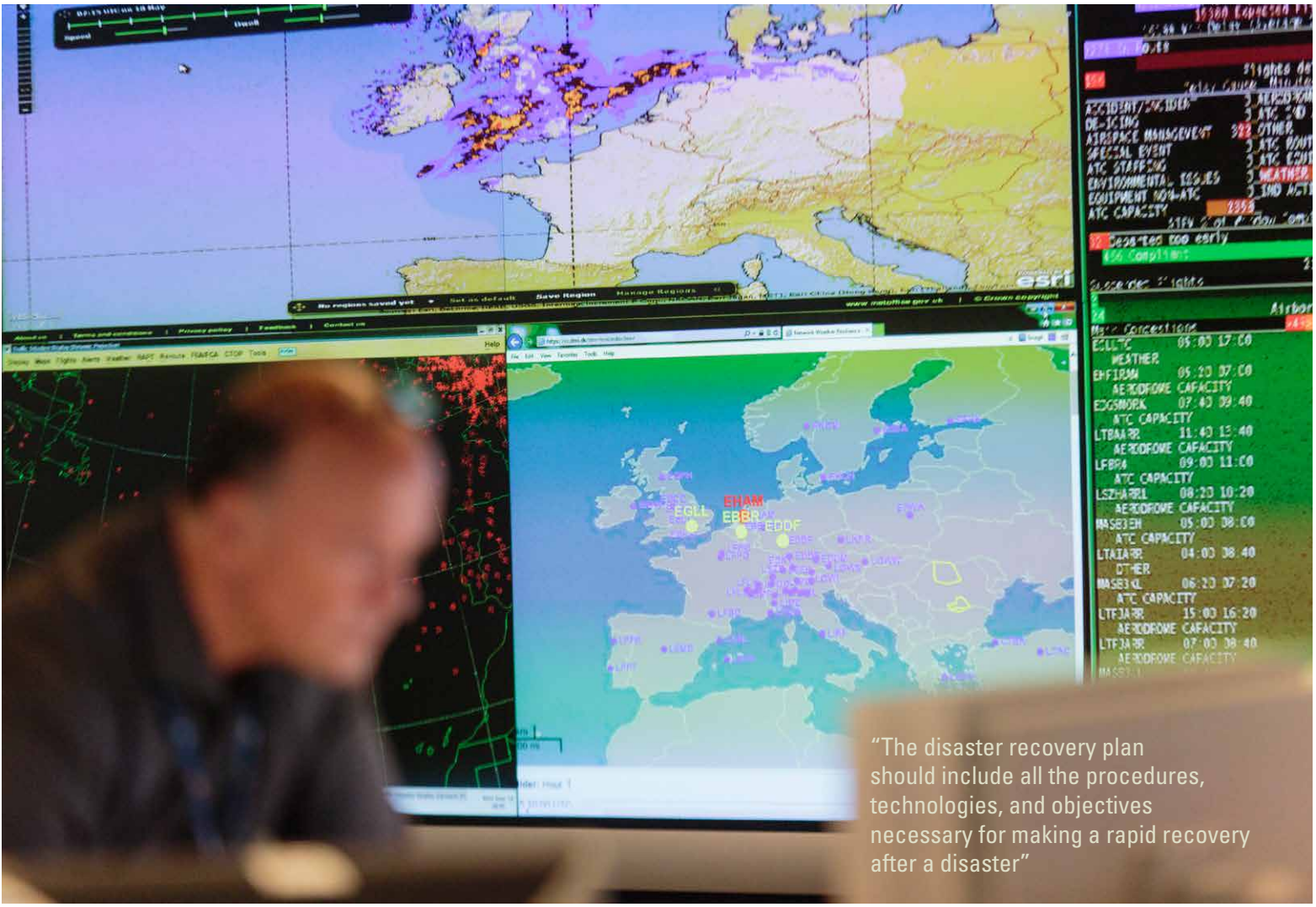
Business continuity differs in that it is the process of getting the business applications and business services back to full functionality after a disaster.

Both are obviously relevant not only to technical staff, but also operational staff, safety staff, management, and almost everyone else. Many ANSPs, airlines, airports and other such organisations have experienced an outage or disaster, and operational and technical staff tend to remember them well. When they affect flight operations, resulting in long delays and cancellations making the headlines, the public remember them too.

"Many ANSPs, airlines, airports and other such organisations have experienced an outage or disaster, and operational and technical staff tend to remember them well"

The disaster recovery plan

The disaster recovery plan dictates how the business should respond to a disaster. Before creating a disaster recovery plan, an organisation should first review its business continuity strategy and cautiously consider the potential impacts of disasters: Which areas are vulnerable? What are the potential losses if the business applications processes go down for a day, a few days, or a week?



"The disaster recovery plan should include all the procedures, technologies, and objectives necessary for making a rapid recovery after a disaster"

The disaster recovery plan is then developed according to business needs. Most likely, different solutions for different business applications will be required.

The disaster recovery plan should include all the procedures, technologies, and objectives necessary for making a rapid recovery after a disaster. As a minimum, a plan should account for the following:

- *Recovery point objective:* This refers to the desired state after recovery. To define the recovery point objective value, the following questions are relevant: *"What data should be restored?" "What data can I afford to lose?"*
- *Recovery time objective:* This refers to your desired timeframe for completing recovery before the situation becomes critical. In other words, it answers the following question: *"When should data be restored and business applications running again?"*
- *Recovery technologies:* This refers to all systems currently implemented, or those that should be, in support of recovery. The following question is relevant here: *"What technologies are required to recover from disaster?"*

Again, these are not merely technical issues. The involvement of operational staff is necessary to deal with each and to answer the questions above.

Depending on the values of the recovery point objective and recovery time objective, different recovery technologies may be needed for different business applications, each with their own price tag. When the business criticality dictates very small recovery objectives (minutes), one has to think of so-called 'active-active' solutions where applications and infrastructure are running in parallel in multiple locations.

As recovery objectives become larger, one can think of:

- *active-standby solutions*, where recovery infrastructure is available and ready in a disaster recovery site and only application data needs to be restored,
- *restore solutions*, where infrastructure capacity is reserved, but operating systems and applications need to be installed from scratch and application data needs to be restored, and
- *rebuild solutions*, where infrastructure first needs to be acquired, after which a restore as described above can start.

Other important information in the disaster recovery plan includes:

- *Recovery protocols:* These protocols should identify who does what in the event of a disaster, including clearly defined roles and how you expect recovery personnel to communicate with each other.
- *Vendors, suppliers, and other third parties:* This is a list of all parties who may be needed to support recovery, as well as their emergency contact details.

What about…?

…the workplace?

The major focus of disaster recovery and business continuity is on the business applications hosted in a data centre. One should, however, not forget about providing business users access to their applications in a disaster recovery situation. Application access from home is increasing, but is not always feasible. Hence it may be necessary to foresee off-site office space to be used in case of disaster.

…the cloud?

While hosting applications on the cloud (public or private) typically removes the burden to build a data centre recovery scenario, this does not remove the need for a disaster recovery or business continuity plan. It is still necessary to have a plan on how to deal with (extended) outage of the cloud services.

The business continuity plan

The disaster recovery plan should be complemented by a business continuity plan, which acts as a single, multifaceted document for managing every aspect of disaster preparedness.

A business continuity plan will usually include a risk assessment (a thorough assessment of disaster scenarios, their likelihood, and their impact) and impact analysis (an outline of how each possible disaster scenario could impact your business, e.g., costs of repair, disruption to services).

Linked to these will be steps and systems to help prevent each of the disasters listed, such as implementing anti-malware to prevent cyberattacks, and detail on how the business will respond to each disaster to minimise the impact.

There will also be areas for improvement identified during the creation of the plan, as well as recommended solutions, and contingencies such as a backup office location to be used in the event of a disaster. And there will be protocols for maintaining communication with recovery personnel, such as a text alert system.

The importance of testing

Testing the plan is the only way to know it will work. Obviously, a real incident is the true test of whether everything is correctly covered in the plan. However, a controlled testing strategy is much more comfortable and provides an opportunity to identify gaps and improve.

Many organisations test a business continuity plan two to four times a year. The schedule depends on the type of organisation, the amount of turnover of key personnel, and the number of business processes and IT changes that have occurred since the last round of testing.

Common tests include table-top exercises, structured walk-throughs, and simulations. Test teams are usually composed of the recovery coordinator and members from each functional unit.

- A *table-top exercise* usually occurs in a conference room with the team going over the plan, looking for gaps and ensuring that all business units are represented.
- In a *structured walk-through*, each team member walks through his or her components of the plan in detail to identify weaknesses. Often, the team works through the test with a specific disaster in mind. Some organisations incorporate drills and disaster role-playing into the structured walk-through. Any weaknesses should be corrected and an updated plan distributed to all pertinent staff.
- Lastly, *disaster simulation testing* can be challenging and should be performed annually. The test requires an environment that simulates an actual disaster, with all the equipment, supplies and personnel (including business partners and vendors) that would be needed. The purpose of a simulation is to determine if you can carry out critical business functions during the event.

During each phase of plan testing, some new employees should be included on the test team. 'Fresh eyes' might detect gaps or lapses of information that experienced team members could overlook.

Review and improve

Much effort goes into creating and initially testing disaster recovery and business continuity plans. Once that job is complete, some organisations let the plan sit while seemingly more critical tasks get attention. When this happens, plans go stale and may not support staff as well as they should, when needed.

Technology evolves, and people come and go, so the plan needs to be updated too. Key personnel should be brought together at least annually to review the plan and discuss any areas that must be modified.

Prior to the review, feedback should be sought from staff to incorporate into the plan. All departments or business units should review the plan, including branch locations or other remote units. If you have had the misfortune

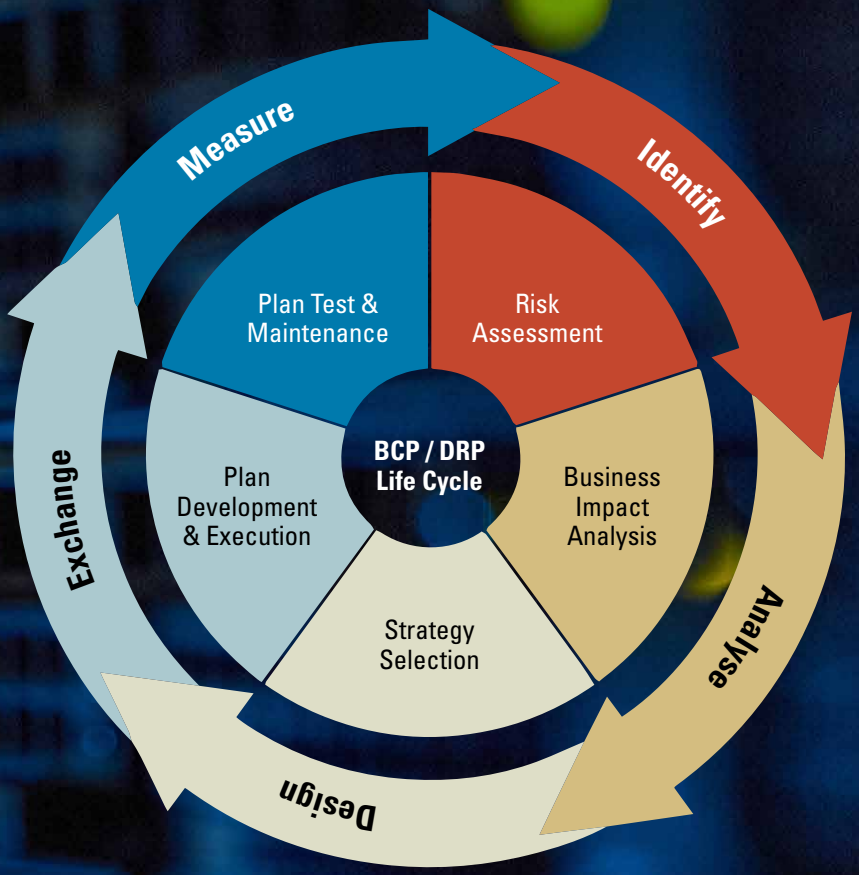


Figure 1: Life cycle of the business continuity and disaster recovery plans

of facing a disaster and had to put the plan into action, lessons learned should be incorporated. Many organisations conduct a review in tandem with a table-top exercise or structured walk-through.

"It is important is that key staff, including operational, technical or safety staff, are involved in the lifecycle of business continuity and disaster recovery planning"

In Closing

This article provides only a brief introduction of what is involved in disaster recovery and business continuity, the related plans and what is required to keep these up-to-date and relevant to your company. Your IT experts and business analysts can provide you with more information and guidance, as can several companies specialised in these matters. It is important that key staff, including operational, technical or safety staff, are involved in the lifecycle of business continuity and disaster recovery planning (see Figure 1). If you are not, then it is time to ask questions to ensure that your operation can recover from disaster.

And in case you were wondering, no World War II explosives have been discovered during construction of the new NM operations centre. So far…

Stefan Maes works as an IT infrastructure architect at EUROCONTROL. He graduated from the University of Antwerp with a PhD in Chemistry. For his professional career, he took a very different direction, pursuing his interest in information and communications technology. He is currently actively involved in various tracks of EUROCONTROL's iNM programme.