AdEPT

Disaster Recovery & Business Continuity

An introduction to Disaster Recovery (DR) Solutions and Planning

AdEPT.CO.UK

Contents

Introduction 3

Understanding business continuity 4

The importance of disaster prevention 5

If disaster strikes, is your business prepared? 8

Combatting disruption: first steps 9

An overview of DR solutions 10

Detailing disaster recovery solutions 11

- Virtualisation 11
- Backup 12
- Replication 13
- Network resilience 14
- Hardware contingencies 15
- Alternate locations 16
- IT Business continuity 17

The DR planning process 18

AdEPT - Disaster Recovery, Business Continuity and Prevention 20

Take the test 21

Glossary 22

Introduction

In today's fast-paced digital world, organisations of all sizes need to be ready for the unexpected. This is especially true now so many people are working from home, and so many customers are now transacting online. IT Disaster Recovery (DR) and business continuity are fundamental parts of your IT and business strategy. Here we take you through all the options, bust some myths and aim to simplify this complex topic.

Understanding business continuity

As we'll see in this document, an effective disaster recovery and business continuity programme requires a multi-faceted and connected approach – bringing business planning and technology together.

There is no right or wrong way to begin your planning. However, before diving into the technical solutions it is important to consider the wider business implications - how will your organisation continue to function during an IT disaster, and prior to full recovery?

Here, a solid business continuity plan (BCP) is key. Outlining how the business as a whole will operate during an unplanned disruption in service, the BCP considers the whole business (not just the technology) and will involve looking at a range of measures beyond IT to protect customers, staff, supply chains, company branding and more.

In a purely IT context, Disaster Recovery and Business Continuity is the ability of IT services to remain available in the event of an outage at the primary network location, maintaining uptime until a full recovery is possible.

While this document discusses Business Continuity in the context of IT Disaster Recovery only, it remains important to consider both the IT and the wider business continuity elements to ensure a sufficiently robust plan.

The importance of disaster prevention

A disaster recovery review may inevitably lead to changes in decisions on network design, IT investment and practises. Disaster prevention is a vast topic as it encompasses security, training and other measures, however key preventative measure may be highlighted in the DR plan. These measures may include:

The importance of disaster prevention

Firewall Security	• Deployment of complex firewalls with active subscriptions to prevent access to malicious websites, viruses, and network intrusion
Password policies	• Complex user and administrator password security • Use of non-standard complex passwords for all network equipment
Vendor security subscriptions/ features, such as the following Microsoft 365 policies	• Multi Factor Authentication • Advanced Threat Protection • Conditional Access from permitted devices and locations
Anti-virus	• Automated signature and program updates • Real-time scanning • Monitoring and control of updates
Patching	• Microsoft patching and monitoring • Security updates from other software vendors • Timely implementation of critical updates
Local firewalls	• Software firewalls deployed on servers and workstations
Penetration testing	• Periodic scanning of the network by accredited external agencies to identify network security vulnerabilities
User training	• Cyber security • Anti-phishing • Anti-virus best practises, such as scanning USB drives originating from outside the organisation
Insurance	• Cyber insurance • Hardware insurance
Auditing	• Auditing of licenses and subscriptions so that these can be recovered quickly and redeployed if needed
Physical security	• Security of access to comms rooms and offices • Fire and water detection in IT comms rooms and key office areas • Aircon • CCTV
UPS	• Using a UPS to regulate voltage and provide power failover to essential devices
Cabling and wiring	• Structured cabling to enable network connections to be clearly traceable to patch panels and switches • Electrical cabling of a high standard and which is inspected regularly e.g. PAT testing
Remote working security procedures	• Use of company standard workstations where possible for working from home • Anti-virus, patching and firewall standards for home devices to be the same as for office devices • Corporate security policies to be applied for personal devices, for example via Microsoft Azure Intune • Avoidance of storing company data on personal devices

The importance of disaster prevention

Disruption resulting from major IT changes should be also governed by best practices for project planning and change management. Finally, you'll need to monitor any third-party IT providers to ensure they have their own DR plans in place. This should include providers of services such as:

- Web hosting
- IT hosting
- IT support
- Bespoke software

If disaster strikes, is your business prepared?

A study by the British Chambers of Commerce found that **93% of business that lost their data for more than 10 days filed for bankruptcy within a year, while almost 50% filed immediately***. Apart from the direct financial effects of loss of productivity, IT disasters can result in high emergency costs, productivity loss, legal actions, compliance breach fines, and the long term loss of customer trust or brand reputation.

Without a DR plan in place, your business could be preparing to fail. To ensure you're ready to face a disaster scenario, you will need to consider some key questions:

- Do you have a single point of failure in your IT & communication environment?
- How much downtime can you realistically manage?
- If your main systems failed, do you know how your users (your staff, customers, suppliers) would continue to engage and access information or communicate with you?
- If your main systems failed, what are your procedures?
- Do you know how they would be activated?
- What applications are hosted on site, off site and in the "cloud"?
- How resilient is the access to these applications?
- How secure are these applications and the data they hold?
- Are you confident that your data is recoverable in the event of disaster?

* http://info.docuvantage.com/blog/prevent-catastrophic-data-loss-from-destroying-your-documents

Combatting disruption: first steps

Determining the best DR plan begins with a business impact analysis that sets out the recovery priorities for your IT systems, applications, and data. This will include networks, servers, desktops/laptops, wireless devices, data, and connectivity.

In this guide, we evaluate best practice approaches for four primary infrastructure types:

- **On premises** – involving single or multiple servers located in the office
- **Private Hosted Cloud** – servers configured and supplied by a third party in a shared datacentre
- **Public Cloud** – for example, Microsoft 365, Google's G-Suite and Amazon Web Services
- **Private Cloud** – a single company tenant in its own data centres, located away from the main offices.

Typically, most organisations today operate a hybrid IT environment; for example, using Microsoft 365 for email and an on-premises file server for file storage. By combining DR solutions, firms ensure they can continue to function during a disaster. So, in the event of a flood at head office, users are able to quickly shift to working from home if the organisation's on-premises servers are replicated to the cloud or a co-location data centre.

An overview of DR solutions

DR planning will involve a combination of the following solution types:

1

Virtualisation

Virtualisation of server infrastructure across diverse data centres is a feature of private and public cloud, and provides resilience in the IT infrastructure that may not be present in on-premise infrastructure.

2

Data Backup

Backup involves making copies of your files, folders, applications and unstructured data and storing this offsite so it can be restored if a data loss occurs.

3

Replication

Replication creates an instant copy of whatever data is stored on a server at any given moment, so you can quickly restore access to mission-critical data and applications. Combined, data backup and replication offer the ultimate recovery solution.

4

Network Redundancy

To protect against the loss of key network connectivity and equipment outside of user data storage, an appropriate network redundancy solution also needs to be in place. For example, automatic switching from a primary broadband line to a secondary line if the primary line fails.

5

Hardware Replacement

Provision for hardware failure, such as server warranties, spare or redundant networking equipment.

6

Alternative Locations

Solutions that make it easy to switch to alternative premises, such as secondary office locations, or work from home.

Ensuring an organisation continues to function during a disaster, and prior to full recovery, includes a combination of the above solutions. If head office is flooded, for example, the on-premise servers would be shut down and users would connect to the cloud servers from home until normal operations are resumed.

Detailing disaster recovery solutions

Virtualisation

More and more businesses are recognising the value of cloud across the business – and DR is no exception. It offers a secure, easy to manage and scalable space to automatically store critical data, and applications – and even protect your critical IT infrastructure. Let's take a look at the key elements to consider.

Cloud networking allows seamless disaster recovery and circumvents many of the challenges presented by the loss of local resources, as services are hosted in remote data centres and users can connect to these services from any internet location. Solutions include private hosted cloud and public cloud solutions.

Offering multiple layers of security, including two-factor authentication, the adoption of cloud solutions has been greatly accelerated by the recent Coronavirus pandemic.

- Hosted Private Cloud. Bespoke solutions provided by a third party service provider, the organisation's servers are hosted in a data centre co-location. This allows data and applications to be presented to the user as virtual desktops – just as if they were working at a local workstation.
- Public Cloud. Public cloud services such as Microsoft 365, Amazon Web Services and Google's G-Suite also enable users to access email and data from any location. These services also provide virtual bespoke server capabilities.

Backup

A comprehensive overview of your data infrastructure – whether stored on premises or in the cloud – will be essential to selecting which backup strategy represents a best fit for your business.

Backup Retention

Ask yourself how far back in time data should be recoverable and to how many restore points. For example, regulatory requirements may mean your business needs to retain backups for seven years but with a variety of different restore points. As a result, daily backups need to be retained for one month, monthly backups for up to one year, and annual backups for seven years.

Snapshot and Image Based Backups

Image-based backups to a virtualised (non-physical) server allows you to recover individual files or entire workstations with a single restore, rather than having to first recovering the operating system followed by programmes and data. This capability represents a major advantage of virtualised over physical servers.

File Based Backups

This involves backing up a selection of files on a server, so that individual files and folders can be easily restored in the event of accidental deletion or corruption.

Local and Offsite Backups

Backups can combine local and cloud locations. For example, a NAS (local storage device) can be used to back up files on the local network before data is sent to the cloud location. This allows files to be restored quickly if the network is intact, with the additional security on an offsite backup in the event of a major disaster such as a fire.

Restore Options

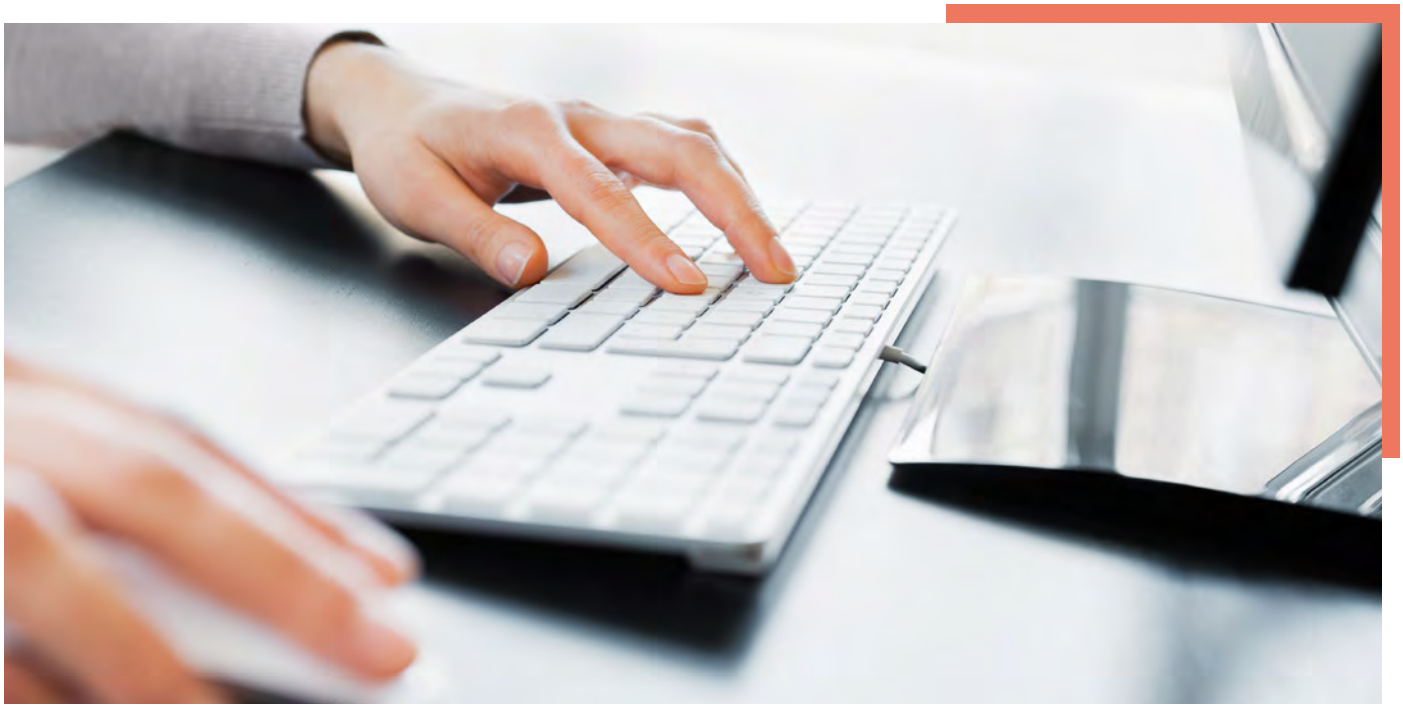
The backup solution you select should allow for different restore options. For example, if a physical server is unavailable, then individual files may need to be restored to another chosen location such as a user's hard drive.

Backup Quota

The chosen retention will require an overall quota for the backup, which will need to be budgeted for.

Backup planning considerations

Care must be taken that company data is not held on unknown locations, such as on USB drives, and overlooked when planning backups.



Replication

Replication should be considered separately from backups. While backing up data involves taking snapshots of data at a specific moment in time and storing it for the long term, replication is the continual mirroring of data to multiple storage devices in real-time for short term retention. This enables workloads to be 'failed over' to the DR site and be online and available in a matter of minutes.

Replication - Private Hosted Cloud & Colocation

Hosted private cloud solutions in data centres typically have replication to secondary and tertiary data centres which allows failover in the event of a disaster at the primary data centre. On premises servers can also be replicated to the data centres as part of a high availability Business Continuity solution.

Replication - Public Cloud

Public cloud solutions such as Microsoft 365 and Google G-Suite have a data replication architecture between multiple data centres. Replication can also occur locally on workstations using features like Microsoft 365 OneDrive, which replicates data between Microsoft Cloud and a location on the workstation hard disk.

Replication vs Backup – Public Cloud

Public cloud services have features like the OneDrive Recycle Bin and Deleted Items in Outlook which allow deleted data to be restored within a specified time period. There are also various options to completely prevent data deletion, such as Litigation Hold in Microsoft 365.

However, backups should also be considered in addition to any resilience offering provided by public cloud providers due to shared responsibility models. For example, while Microsoft 365 is responsible for maintaining the uptime of its cloud service, customers are responsible for access and control of data residing in Microsoft 365. So, if your data is completely deleted or corrupted, you are responsible for restoring it.

This responsibility extends to scenarios like loss of data through accidental or malicious deletion. Should a folder be deleted and not be discovered for weeks, it may have already been removed from the recycle bin and any replicated locations. Which means that the only recourse for restoring data is from a location outside of the Microsoft 365 cloud.

A cloud backup located outside the relevant public cloud platform and with appropriate retention levels is therefore required. These backups are normally cloud-to-cloud solutions which access portals directly, without any need for direct user intervention.

Replication vs. Backup – Private Cloud / Office

The same principles apply with regard to private cloud and office replication solutions. For example, if replication is set up between two on premises servers, then backups will still be required to guard against the risk of the live data becoming corrupted.

Replication + Back Up in Action

If a file server in an office is mirrored to a remote datacentre, your organisation could quickly switch to the replicated server in the event of a complete power loss. However, if your the organisation were infected with a virus which corrupted data gradually and was not discovered for a few days, then you'd be able to restore your file server data using a backup taken prior to the infection.

All of which explains why backup + replication = the best strategy.

Network resilience

Boosting the resilience of the devices - such as firewalls, routers and switches - that facilitate IT connectivity but do not store user data is further key element of your DR strategy. This resilience can be achieved through a combination of network configuration and hardware redundancy practices:

- **Failover for broadband and wide area networks** – in the event of an outage of a primary broadband line, the firewall or router will enable failover to a secondary line.
- **Firewall clustering** – two or more firewalls are grouped together with the same configuration, so that if one firewall fails services are not interrupted.
- **Switch stacking and redundancy** – office network connections are arranged so that computers are distributed between two or more switches. Should one pair of switches fail, only half of users are then be affected.
- **Spare network ports** – if ports and connections are damaged, devices can be connected to alternative ports.
- **Capacity planning** – the network needs to be able to handle extra load in the event of an emergency. During the recent Covid-19 pandemic, for example, users working from home via a VPN placed additional strain on hardware firewalls and network bandwidth.

Hardware contingencies

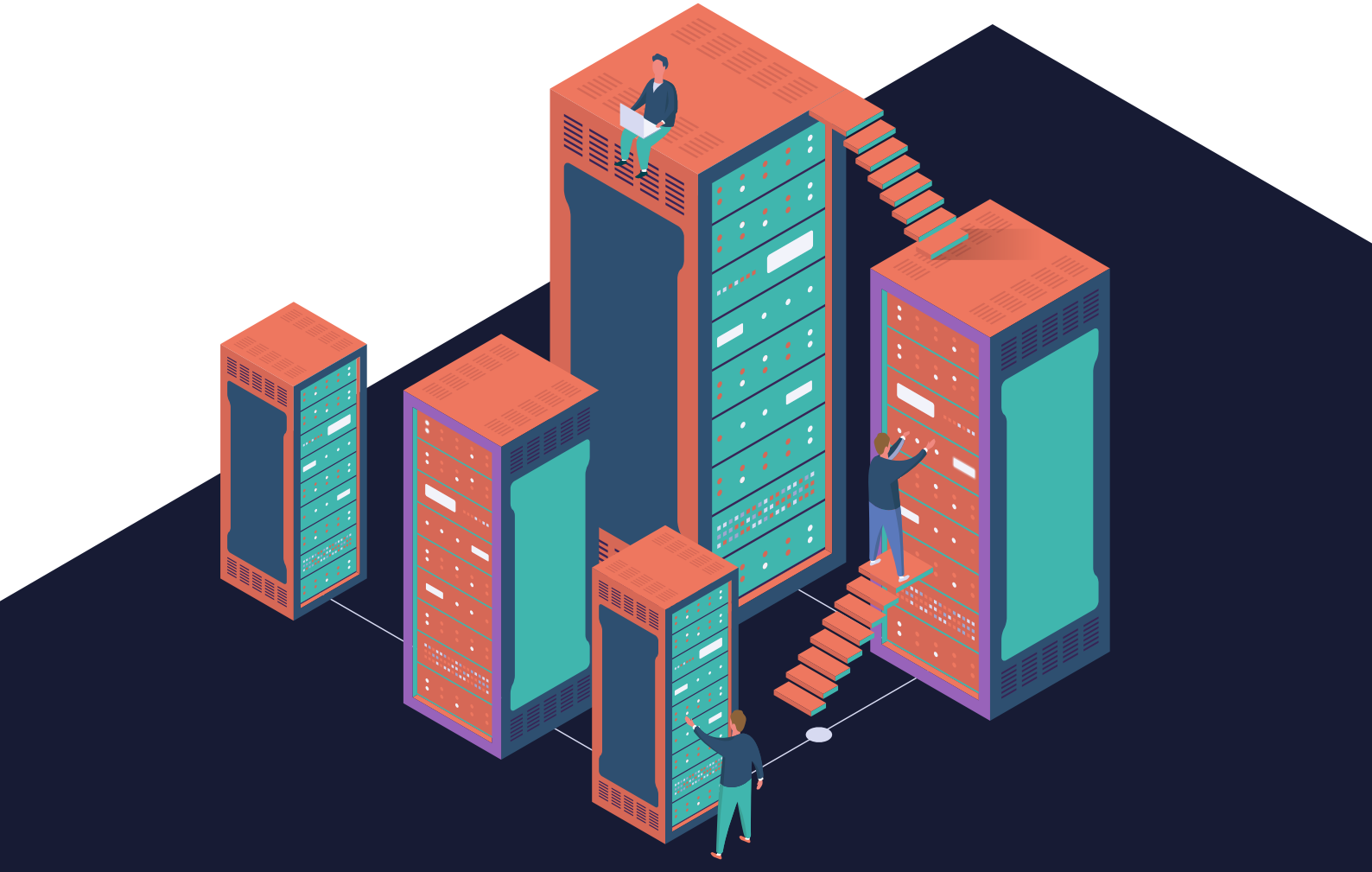
The failure of critical equipment, such as a local server outage, can cause major disruption. For this reason, server hardware should have built-in redundancy features such as:

- RAID - an array of hard disks acting as a single logical unit that ensures no loss of data should one or more disks fail
- Two or more power supplies
- Spare network ports
- Network devices that make it possible for issues to be diagnosed even when the server is offline or being powered up or down (e.g. Dell iDRAC).
- Spare network cards that support multiple or redundant network connections.

Critical devices should be protected by a UPS (uninterruptible power supply) which supplies backup battery power to devices for minutes or even hours if there is an outage and shuts down servers cleanly in an extended outage. The UPS will also regulate power to protect devices in the event of power surges and dropouts which could otherwise cause damage to equipment.

Warranties should be maintained for critical networking equipment such as servers and firewalls; these are typically available from all major vendors for up to five years and enable parts to be replaced within four hours in the event of a failure. Warranties may also be available beyond the standard terms via third-party providers.

You may also decide to keep network spares, such as pre-configured firewalls and switches, at your primary or secondary locations so you can quickly swap out a failed device. Another option is to deploy redundant servers locally, using replication technology, so that if one server fails your organisation can rapidly switch to the failover server. Finally, retaining spare workstations which can be swapped out quickly for key operations is also advisable.



Alternate locations

Home Working

Home working has become an essential business requirement following the Covid-19 pandemic. As a result, connectivity to the office via a VPN using remote desktop technology, is now standard for accessing on premise networks. Where private cloud solutions apply, users can continue operating seamlessly from home, while public cloud services may provide some or all of the functionality needed to work remotely.

In the event of an outage at the main office, your DR strategy may include having the ability to get secondary disaster recovery or backup locations up and running fast. These locations are categorised in IT terms as hot, cold, or warm sites.

Hot Sites

A hot site is a fully functional back-up data centre service equipped with all the hardware, software and network connectivity needed to perform near real-time backup or replication. Up and running continuously, critical production workloads can be failed over in a matter of minutes.

Warm Sites

A warm site has some or all of the IT equipment found in a typical primary data centre, such as software, hardware and network connectivity. Not ready for immediate switch over, organisations must first introduce customer data and possibly install additional equipment. Which means that unlike a hot site, recovery will be delayed while data is retrieved from a remote backup site.

Cold Sites

Featuring basic utilities and infrastructure to support IT, but no actual pre-installed technology, cold sites can take days or even weeks to set up properly. The lowest cost option of all, your organisation is essentially renting space without any equipment. Which means that in the event of a disaster, you'll need to migrate servers and make them functional in order to take on the workload of your primary site.

IT Business Continuity

Considering how the organisation will continue to operate in the event of a disaster before full recovery is achieved is critical.

The goal here is to minimise business downtime, which will involve a combination of technologies - particularly replication.

Business continuity solutions typically involve failover to a secondary data centre. This backup operational mode automatically switches to a standby server, database, or network if the primary system fails.

Failover may involve replication to a single virtual machine or entire site, and can be to on premise devices such as a backup network storage device (NAS) or to off-site locations.

Following failover, a failback phase is initiated where the original network services are recovered, and data which has been updated since the outage are merged back to the primary network.

The DR planning process

Creating a Disaster Recovery Plan may seem like an onerous and time consuming task, but it is an activity that will repay your business significantly in the event of a disaster. Involving senior managers and all key company stakeholders, the DR planning process entails a full assessment of current capabilities against your DR requirements, an analysis of what measures are required to bridge any gaps, and an action plan. This should include how the business continues to operate until system are fully recovered.

The main considerations for a DR plan include:

- Recovery Time Objective (RTO) – the duration of time and a service level within which business processes must be restored after a disaster to avoid the unacceptable consequences associated with a break in continuity.
- Recovery Point Objective (RPO) – the maximum acceptable amount of data loss an application can undergo before causing measurable harm to the business.
- IT Business Continuity – a critical part of the plan defining how the business will continue to operate until system are fully recovered..

For example, if a server is backed up once a day at 11.00 pm and was destroyed the following day at 6 pm, then a full working day's data would be lost; this would be considered when planning the RPO.

The DR planning process

The RPO should always balance business risk with cost; so, while a daily offsite backup represents an entry level cost solution, multiple daily backups would require greater investment but would also allow for several recovery points throughout the day.

The DR plan process and documentation should include:

- A detailed list of each business area and all related critical IT systems and services
- A Business Impact Analysis of possible failures by main causes and disaster scenarios
- An assessment of the required RTO and RPO for each business area
- A contingency plan for each function and related IT system
- Who owns DR planning for different business areas
- Key staff operational responsibilities
- Key actions for each business area
- Contact trees and communication flows
- Use of alternative sites and ‘war rooms’
- Third party contacts and communication plans
- IT Business Continuity measures
- Fail back plan to primary services once these are restored
- Post disaster actions and review process
- Training and testing plans
- Planning review schedule

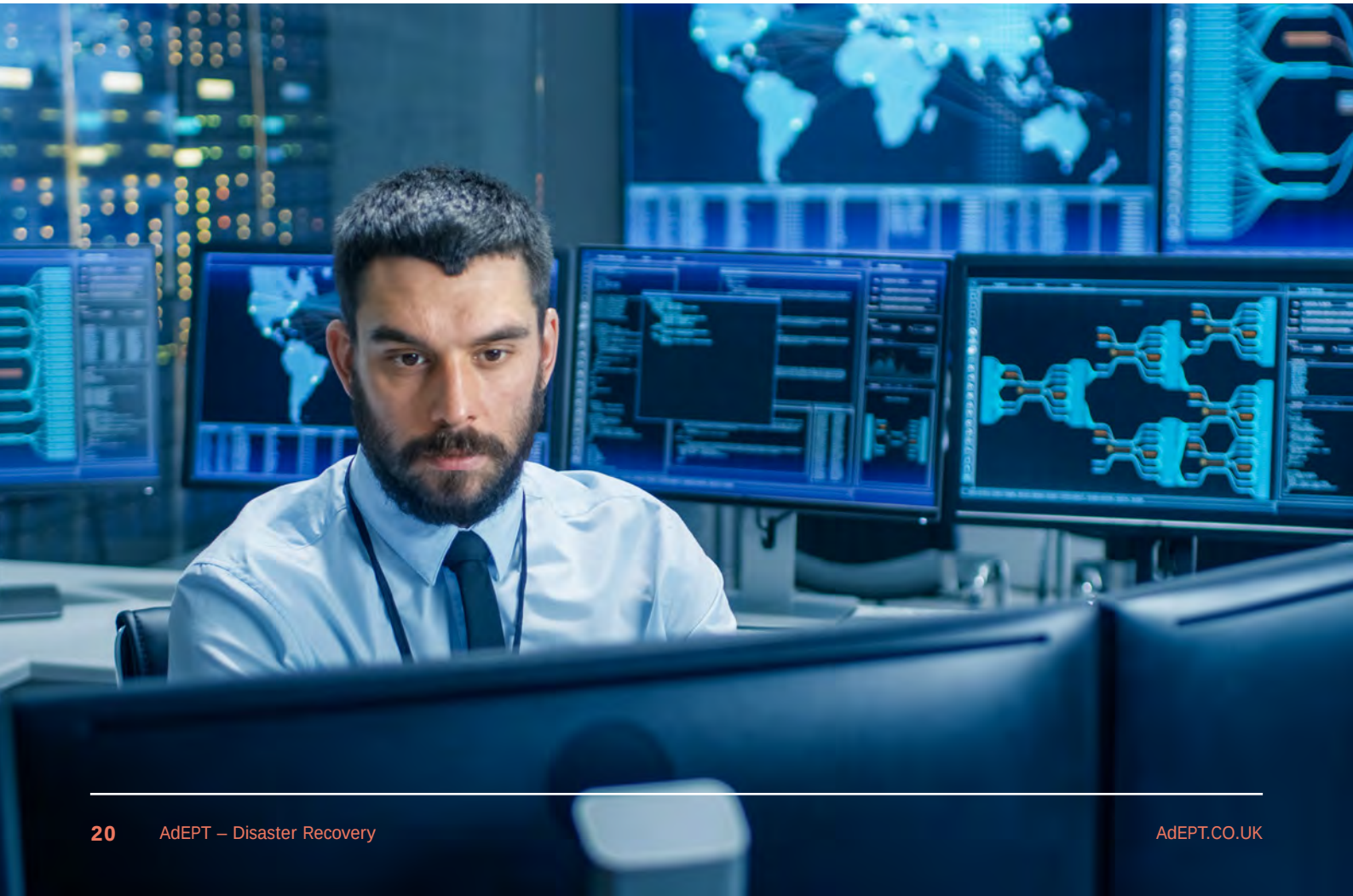
The DR Plan requires continual review as business needs evolve and systems change. It also requires a regular testing programme; for example, a quarterly dry run of potential DR scenarios.

AdEPT - Disaster Recovery, Business Continuity and Prevention

Today's modern businesses need to operate on a high availability basis, and most cannot afford long periods of downtime. Here at AdEPT, we offer best-in-class DR services you can rely on.

Experienced at helping businesses protect their day-to-day operations from downtime and loss of data, our Business Continuity services are designed to get you back up and running quickly and efficiently following a catastrophe. That includes providing guidance and services designed to prevent an event – such as multiple disk failures – from causing an unacceptable loss of data or productivity.

Alongside a combination of public and private / hybrid solutions that can be tailored to your specific requirements, we're also on hand to help with cloud readiness assessments. Plus, we can provide private hosting via Nebula, public cloud via multiple leading providers such as Azure and AWS, and advise on transforming IT delivered services to provide an optimal DR solution.



Take the test

To help you determine whether it's time we should be talking, why not take the following questionnaire to assess your current state of DR readiness.

Questionnaire:

- Do you have a DR Plan?
- Does the DR plan cover all your critical systems?
- Does the DR plan cover the main types of disaster scenario?
- Does the DR plan cover major time frames for disaster (e.g. 1 day / 1 week / 1 month)?
- Does the DR plan meet capacity requirements over the different time frames - for example 50% of staff to be operational in the first day, 75% by the end of the first week?
- Do you have an IT Business Continuity strategy so that your systems can continue to run in the event of a disaster until services are fully restored?
- Are the key stakeholders in your organisation aware of IT processes and actions in the event of a disaster?
- Do you review the DR Plan at least annually and have you reviewed this in the last 12 months?
- Do you regularly test your DR Plan under different scenarios?
- Are you satisfied that your IT systems meet the needs of your DR plan?

Glossary

Backup - a copy of a file, server or other item of data that is made in case the original is lost or damaged.

Backup Quota - the maximum amount of storage space available for backups, including all historical backups.

Backup Retention - a set of policies relating to the intervals and length of time backup archives are stored.

Business Continuity (IT) – services which allow access to IT systems during a disaster.

Business Continuity Planning – business focussed planning for recovery from potential threats to an organisation, covering both IT and non-IT systems.

DR Cold Site - office space with basic utilities such as power, and air conditioning, and communication equipment which can be used in the event of a disaster.

DR Hot site – a backup site with equipment set up with an organisation's current data and ready to operate from in the event of a disaster.

DR Warm Site - a backup site with equipment set up with the organisation's current data, ready to operate from in the event of a disaster.

Complex Firewalls – a firewall which allows a high level of configuration of network services and subscription-based protection features, such as anti-virus and packet inspection.

Disaster Recovery - the process of resuming normal operations following an unforeseen event by regaining access to data, hardware, software, networking, power, and connectivity in the shortest time possible.

Failover - a backup operational mode that automatically switches to a standby server, system, database, or network if the primary system fails.

Failback - the process of restoring operations to a primary machine or facility and data recorded by the backup facility during the duration of the crisis.

File backups – storing copies of critical files on a hard drive or auxiliary storage device to protect data in the event of a system failure or file corruption.

Firewall – a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules.

Image backups – an image or copy of the entire system, including the operating system.

IT Business Continuity – provision for continued access to IT systems during a disaster.

Local Backups – any backup where the storage medium is kept close at hand or connected through a local area network to the source being backed up.

NAS devices – a storage device attached to the network that allows storage and retrieval of data from a central location for authorised network users and clients.

Offsite backups – the replication of data to a server or media in a different geographic location to the primary server, which may be done via direct access over the Wide Area Network (WAN).

Private Cloud – on-premises computing services offered over the internet or a private internal network to selected users only.

Private hosted cloud –infrastructure and data centre services hosted by service providers who architect a solution to meet an organisation's specific needs, ensuring that the organisation is completely isolated from others.

Public Cloud – services provided via the internet on a pay-per-use model. Data for multiple organisations may reside on the same server.

Restore – the process of restoring backed up data and information to the original device.

Router – a networking device that forwards data packets between networks.

Server – a computer that provides data to other computers on the local area network (LAN, Wide Area Network (WAN) or over the internet).

Snapshot – a type of backup copy used to create the entire architectural instance/copy of an application, disk or system. It is used in backup processes to restore the system or disk of a particular device at a specific time. A snapshot backup can also be referred to as an image backup.

Switch –hardware that connects devices on a network by using packet switching to receive and forward data to the destination.

Call AdEPT today
to see how we can
liberate your business.

AdEPT

The Dorking Business Park
Station Rd, Dorking
Surrey RH4 1HJ

01306 873900
enquiries@adept.co.uk
www.adept.co.uk